УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА

ISSN 1857- 8691

ГОДИШЕН ЗБОРНИК 2012

YEARBOOK 2012

ГОДИНА 1 VOLUME I

GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“ – ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА

ГОДИШЕН ЗБОРНИК
2012
YEARBOOK
2012

ГОДИНА 1 МАРТ, 2013 VOLUME I

GOCE DELCEV UNIVERSITY – STIP
FACULTY OF COMPUTER SCIENCE

ГОДИШЕН ЗБОРНИК
ФАКУЛТЕТ ЗА ИНФОРМАТИКА
YEARBOOK
FACULTY OF COMPUTER SCIENCE

За издавачот:
Проф д-р Владо Гичев

Редакција и администрација
Универзитет „Гоце Делчев“-Штип
Факултет за информатика
ул. „Крсте Мисирков“ 10-А
п. фах 201, 2000 Штип
Р. Македонија

Address of the editorial office
Goce Delcev University – Stip
Faculty of Computer Science
Krste Misirkov 10-A
PO box 201, 2000 Štip,
R. of Macedonia

СОДРЖИНА
CONTENT

DEVELOPING CLOUD COMPUTING'S NOVEL COMPUTATIONAL METHODS FOR IMPROVING LONG-TERM WEATHER GLOBAL FORECAST

Zubov Dmytro
University for Information Science and Technology "St. Paul the Apostle"
dmytro.zubov@uist.edu.mk , dzubovcs@yahoo.com

Abstract:
Weather data mining methods and forecast algorithms have been of long standing interest. Recent research based on the global satellite data and special synergetic methods showed possibility of the long-term (up to half a year ahead) forecast with up to 10 % average mistake (standard is 20 %). Particularly, the average daily air temperature forecast's mistake is up to 6.5 % for Skopje Airport (half a year ahead). This approach is characterized by the final linear difference equations' simplicity and the high computational complexity of the above equations reasoning. The cloud computing web-site's prototype was developed (weatherforecast.tk). Main research proposals: improving the user interface based on 3D or/and ubiquitous computing technologies; developing new synergetic methods for the appropriate realization in the multithread cloud application, including the code and data parallelization; increase of the forecast parameters' quantity (e.g., precipitation). This paper main results are: precipitation's long-term (up to half a year ahead) forecast has very low quality now, and, therefore, it is not recommended for practice; the forecasting places' quantity is changed modifying the text file in the cloud application's package; the web-site http://weatherforecast.tk user interface was enhanced using 3D Chart diagram.

Keywords: cloud computing, inductive modeling, long-term average daily air temperature's forecast.

1 Introduction

Weather data mining methods and forecast algorithms have been of long standing interest because of high importance for noosphere. Recent research on the basis of the global satellite data and special synergetic methods showed possibility of the long-term (up to half a year ahead) forecast with up to 10 % average mistake (standard is 20 %). Particularly, the average daily air temperature forecast’s mistake is up to 6.5 % for Skopje Airport (half year ahead). This approach is characterized by the final linear difference equations’ simplicity and the high computational complexity of the above equations reasoning. The cloud computing web-site’s prototype was developed (URI – http://weatherforecast.tk/) on the basis of this know-how. Some details of the above approach can be found in the papers which can be downloaded free against http://weatherforecast.tk/.

1.1 Previous results’ analysis

There is currently no completed long-term weather forecast system. Several approaches for long term and short term weather forecasts have been suggested in [1, 2, 4]. However, precise forecast of the weather conforming to localised environment conditions is fraught with difficulties due to computational complexity of long-term forecasts requiring computing grid and/or clouds to compute the forecast values in reference points using the classical inductive analogue method for more than 80 % forecast quality at the average [3]. The problem focusing on enhancement in quality of the long- and short-term forecasts of weather processes, therefore, has drawn considerable attention [1]-[11]. As may be seen in [1]-[3] and Internet resources [7]-[9] that rise to this situation can be attributed to weather processes and noosphere interplay. It is well known that classical hydrodynamic equations are used for continuous modelling of these events. But, this approach depends on the variables variation (the theory catastrophe’s known effect). In addition, discrete modelling is applied on the basis of analogue complexing algorithm [4]. Yet, experts note that the forecasts’ quality (up to 80 % at the average) and forward (up to two weeks mainly) are not enough nowadays. A feature-specific forecasting method for high-impact weather events that takes advantage of high-resolution numerical weather prediction models and spatial forecast verification methodology was proposed in [11]. An application of this method to the prediction of a severe convective storm event was given only. But, the idea of the high-impact weather events’ usage is considered is very effective. Furthermore, the standard software and hardware combined solutions with user-friendly interface have not been developed as yet.

1.2 Organization of the paper

Paper includes three main parts: average daily air temperature’s long-term forecast model’s synthesis, software’s brief description, daily precipitation’s correlation analysis.

This paper’s structure is based on the main prospects of the developing cloud computing’s novel computational methods for improving of the long-term weather global forecast:

1. Improving the user interface of the web-site http://weatherforecast.tk. Particularly, 3D user interface or/and ubiquitous computing technology are planned for realization.
2. Developing new synergetic methods for the appropriate realization in the multithread cloud application, including the code and data parallelization for the continuous updating of the mathematical models’ structures, increase of the forecasting places’ quantity, and up-to-date weather forecast.
3. Increase of the forecast parameters’ quantity. As may be seen in http://weatherforecast.tk/, the average daily air temperature’s long-term forecast was realized only. Precipitation is next very important factor for forecasting.

The research plan can be formulated as (1st stage can be done in parallel):

1.a. Developing the user interface on the basis of 3D or/and ubiquitous computing technology.

1.b. Air temperature and precipitation’ global data mining and classification.

2. Increase of the forecast places’ quantity (the average daily air temperature parameter). Developing cloud computing multithread application’s prototype which includes the separate treads for the computationally complicated models (3) reasoning (models (3) are discussed below).
3. Developing the forecasting models for the precipitation’ long-term forecast.
4. Developing cloud computing multithread application (web-role) on the basis of Microsoft Windows Azure for long-term weather global forecast (the precipitation and the average daily air temperature parameters).

In addition, the scientific problem of the two-level hierarchical criterial system’s creation for the inductive forecasting method is proposed for solution optionally (as may be seen below, one criterion (4) is in use only).

The above mentioned cloud computing technology’s usage is grounded on the basis of Microsoft Windows Azure Educator Grant which one was received by the University for Information Science and Technology "St. Paul the Apostle".

Expected outcomes of this research include:

1. New up-to-date user interface of the web-site http://weatherforecast.tk on the basis of 3D or/and ubiquitous computing technology.
2. Advanced cloud software based on the code and data parallelization, which one allows to generate new, more effective global forecasting models on-line.
3. New forecasting models for different meteorological data (precipitation at least).

2 The average daily air temperature's long-term forecast model's synthesis

67 places took part in the correlation analysis initially (names were written according to the www7.ncdc.noaa.gov; places were chosen with 2 criterion: one country – one representative place; time series have to be continuous from 1st January, 1973): Nwso Agana, Aarhus Lufthavn, Abbeville, Aeropuerto Pettiros, Amman Airport, Amsterdam AP Schiph, Annaba, Ashgabat Keshi, Athinai al Helliniko, Auckland Airport, Bangkok Metropolis, Beijing, Ben-Guron International Airport, Beograd-Surcin, Bogota-Eldorado, Brasilia-Aeroporto, Bratislava-Letisko, Bruxelles National, Bucuresti INMH-Bane, Budapest-Ferihegy I, Busan, Cairo Airport, Canberra Airport, Caracas-Maiquetia, Damascus International Airport, Geneve-Cointrin, Gibraltar, Guernsey Airport, Helsinki-Vantaa, Hengchun, Jersey Airport, Kiev, Kingston-Norman Man, Kisinev, Kwajalein-Bucholza, La Paz-Alto, Lima-Callao Airport, Lisbon, London, Luqa, Luxembourg, Minsk, Moscow, Nassau Airport New, New Delhi-Safdarjun, Noumea-Nlle-Calledo, Nuuk, Oslo-Gardermoen, Paphos Airport, Praha-Libus, Rabat-Sale, Rarotonga, Reykjavik, Riga, Roma-Ciampino, Skopje Airport, Tallin-Harku, Tashkent, Tokyo, Torshavn, Tripoli, Tunis-Carthage, Ulaanbaatar, Vaduz, Warszawa-Okecie, Washington National, Wien-Hohe Warte. Data was downloaded in as the text files against www7.ncdc.noaa.gov (USA National Environmental Satellite, Data, and Information Services).

20 time series were selected as the most correlated to Skopje Airport with half-year (approximately) delay (correlation function is normalized and centralized):

0. Skopje Airport (delay 181, autocorrelation function's value -0.8327425 97188605).

1. Aeropuerto Pettiros (delay 187, correlation function's value 0.6230456 98552278).
2. Ashgabat Keshi (delay 184, correlation function's value -0.8516412838 20963).

3. Auckland Airport (delay 175, correlation function’s value 0.725715828 489775).
4. Canberra Airport (delay 182, correlation function’s value 0.7988013098 32135).
5. Gibraltar (delay 164, correlation function’s value -0.823452379725064).
6. Guernsey Airport (delay 163, correlation function’s value -0.7828445577 22741).
7. Jersey Airport (delay 167, correlation function’s value -0.78219805049 1036).
8. Lisbon (delay 165, correlation function’s value -0.761637258660198).
9. London (delay 174, correlation function’s value -0.781332533443968).
10. Nassau Airport New (delay 165, correlation function’s value -0.7676340 36673984).
11. New Delhi-Safdarjun (delay 199, correlation function’s value -0.84031 2570729328).
12. Noumea-Nlle-Calledo (delay 166, correlation function’s value 0.782559778633274).
13. Nuuk (delay 168, correlation function’s value -0.740870261967304).
14. Paphos Airport (delay 166, correlation function’s value -0.858819 233109924).
15. Rabat-Sale (delay 165, correlation function’s value -0.7843430 51359234).
16. Reykjavik (delay 172, correlation function’s value -0,73488389 2104582).
17. Tashkent (delay 183, correlation function’s value -0.833431861928644).
18. Tokyo (delay 168, correlation function’s value -0.855582219493774).
19. Washington National (delay 179, correlation function’s value -0.837 538640603375).

Average daily air temperature’s long-term forecast model has next linear structures:

$$\frac{X[i]}{\max\{X[i]\}} = k_0 + k_1 \frac{X_{j_1}[i]}{\max\{X_{j_1}[i]\}}, \tag{1}$$

$$\frac{X[i]}{\max\{X[i]\}} = k_0 + k_1 \frac{X_{j_1}[i]}{\max\{X_{j_1}[i]\}} + k_2 \left.\frac{X_{j_2}[i]}{\max\{X_{j_2}[i]\}}\right|_{j_2 \neq j_1}, \tag{2}$$

$$\frac{X[i]}{\max\{X[i]\}} = k_0 + k_1 \frac{X_{j_1}[i]}{\max\{X_{j_1}[i]\}} + k_2 \left.\frac{X_{j_2}[i]}{\max\{X_{j_2}[i]\}}\right|_{j_2 \neq j_1} + k_3 \left.\frac{X_{j_3}[i]}{\max\{X_{j_3}[i]\}}\right|_{\substack{j_3 \neq j_1 \\ j_3 \neq j_2}}, \tag{3}$$

where *X*[*i*] – air temperature data; *i* – data position's number in time series, *i*=1, 2, 3, ..., 14198 (July19, 1973 – June 1, 2012); $X_{j_1}[i], X_{j_2}[i], X_{j_3}[i]$ – biased (with appropriate delay) time series for the appropriate places; *k*k_0, k_1, k_2, k_3 = [-2;+2] – weighting coefficients (this range allows to find model with physical meaning); j_1, j_2, j_3=0,1,2,...,20 – number of the place in the above list. The main task is to find weighting coefficients k_0, k_1, k_2, k_3. We will use combinatorial (step is equal to 0.01) inductive modelling with next criterion (minimum of the regularity plus displacement):

$$\alpha_1 \frac{\sum\limits_{\substack{i=1\\ i\in B_1}}^{13680} \left| X^*[i] - X[i] \right|}{6840 \max\{X[i]\}} + \alpha_2 \frac{\sum\limits_{\substack{i=1\\ i\in B_2}}^{13680} \left| X^*[i] - X[i] \right|}{6840 \max\{X[i]\}} + \alpha_3 \frac{\left| \sum\limits_{\substack{i=1\\ i\in B_1}}^{13680} \left| X^*[i] - X[i] \right| - \sum\limits_{\substack{i=1\\ i\in B_2}}^{13680} \left| X^*[i] - X[i] \right| \right|}{6840 \max\{X[i]\}} \to \min$$

, (4)

where |.| – absolute value, B_1 – first learning sample (odd numbers); B_2 – second learning sample (even numbers); *X**[*i*] – forecast values; $\alpha_1 = \alpha_2 = 1, \alpha_3 = 10$ – criteria's weighting coefficients.

Thus, a formula (1) has next view (temperature measures Fahrenheit degrees):

$$X^*[i] = 92.6\left(1.08 - 0.8\frac{X_2[i]}{100.8}\right). \tag{5}$$

A criterion (4) has next view on the learning sample (*i*=1, 2, ..., 13680):

0.0726133559941771 + 0.0726451595651796 +
+ 10 · | 0.0726133559941771 – 0.0726451595651796 | = 0,14557655 1269382

A criterion (4) has next view on the training sample (*i*=13681, 13682, ..., 14198):

0.0696785289719569 + 0.0671852780183542 +
+ 10 · | 0.0696785289719569 – 0.0671852780183542| = 0.16179631 6526338

A formula (2) has next view:

$$X^*[i] = 92.6\left(1.29 - 0.49\frac{X_2[i]}{100.8} - 0.54\frac{X_{11}[i]}{103.7}\right). \qquad (6)$$

A criterion (4) has next view on the learning sample:

0.0648588883227404 + 0.0649056479360714 +
+ 10 · | 0.0648588883227404 – 0.0649056479360714 | = 0.13023213 2392122

A criterion (4) has next view on the training sample (*i*=13681, 13682, ..., 14198):

0.0638972281191006 + 0.0630384066284932 +
+ 10 · | 0.0638972281191006 - 0.0630384066284932 | = 0.13552384 9653668

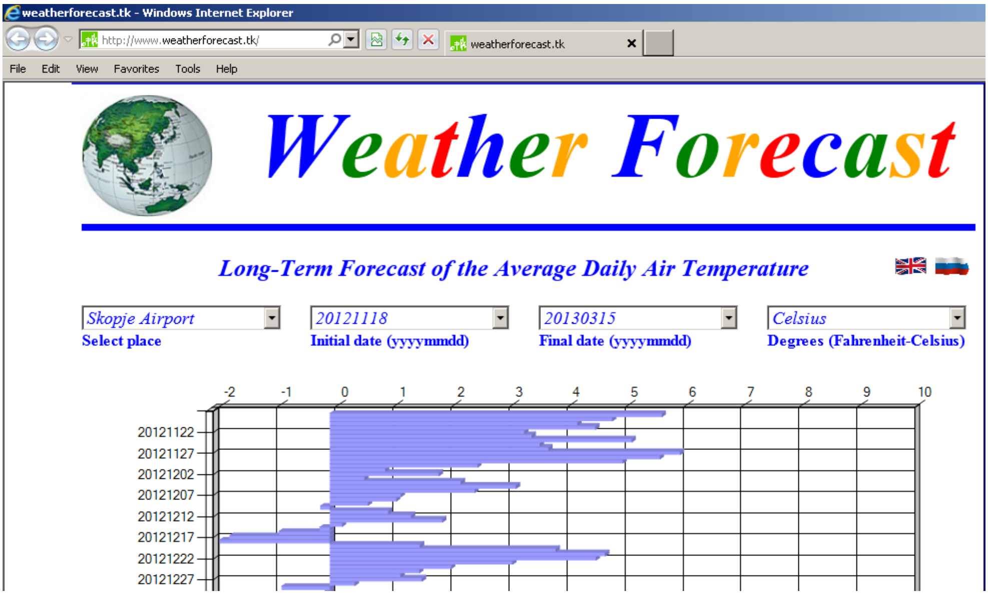
It is clear that criteria's values are identical. Results' analysis shows that forecast model (6) is more precise than (5). I.e., we have the average daily air temperature forecast's mistake up to 6.5 % for Skopje Airport (half year ahead).

Model (3) is not discussed because of the high computational complexity (the main development perspectives in the multithread cloud application). E.g., model (2) calculation time is 2 days approximately on the basis of Intel® Core™ i5 processor.

The similar results were achieved for Beijing, China (mistake is up to 6.2 %), Kiev, Ukraine (up to 9.5 %), Moscow, Russia (up to 8.7 %), Tokyo, Japan (up to 5.7 %), and Washington National Airport, USA (up to 7 %). The forecasting places' quantity can be increased modifying the text file "CF.txt" in the cloud application's package.

3 Software's brief description

Web-site http://www.weatherforecast.tk/ was developed on the basis of ASP.NET technology initially, and, then, was moved to Microsoft Windows Azure web-role (C# is programming language). Web-site's screenshot is shown in Figure 1. User can choose place, date, and degree regime (Fahrenheit or Celsius) for forecast.



Long-Term Forecast of the Average Daily Air Temperature

Select place: Skopje Airport
Initial date (yyyymmdd): 20121118
Final date (yyyymmdd): 20130315
Degrees (Fahrenheit-Celsius): Celsius

Figure 1 Web-site http://www.weatherforecast.tk/ screenshot

In praesenti, web-site code was improved. Firstly, it was speeded up using the partial-page update (UpdatePanel Control). Secondly, Chart Control's XmlDataSource file exception was handled using the set of the one-type files – file's title is changed in a loop. Thirdly, user interface was enhanced using 3D Chart diagram.

4 Skopje Airport daily precipitation's correlation analysis

Precipitation is a second important parameter in long-term weather forecast. Unfortunately, Skopje Airport daily precipitation's correlation analysis shows the practical inexpediency because of the low value of the correlation functions (up to 0.1 %; the pairs precipitation – precipitation and precipitation – temperature were considered). The similar results were achieved when the decade precipitation's correlation analysis is discussed [5]. I.e., the precipitation's long-term (up to half a year ahead) forecast has very low quality now, and, therefore, it is not recommended for practice.

5 Conclusion

In this paper, the cloud computing's novel computational methods for improving long-term weather global forecast were developed:

1. Precipitation's long-term (up to half a year ahead) forecast has very low quality now, and, therefore, it is not recommended for practice.

2. The forecasting places' quantity is changed modifying the text file "CF.txt" in the cloud application's package.
3. The web-site http://weatherforecast.tk user interface was enhanced using 3D Chart diagram.

At the same time, the main prospects for future research are following: the user interface based on the ubiquitous computing technology; developing new synergetic methods for the appropriate realization in the multithread cloud application, including the data parallelization for the continuous updating of the mathematical models' structures.

References

1. G.C. Onwubolu, P. Buryan, S. Garimella, V. Ramachandran, V. Buadromo, A. Abraham (2007): *Self-organizing Data Mining for Weather Forecasting*. IADIS European Conference Data Ming, pp. 81-88.
2. A.S. Cofino, J.M. Gutierrez (2003): *Implementation of Data Mining Techniques for Meteorological Applications, Realizing Teracomputing.* Ed. by W. Zwieflhofer and N. Kreitz, World Scientific Publishing Company, pp. 215-240.
3. D. Zubov, Y. Vlasov, M. Grigorenko (2008): *Method of the Decade Air's Temperature Long-Range Prognosis with Robust Inductive Models and Analogue Principle*. 2nd Int. Conf. on Inductive Modeling, Kyiv, Ukraine, Sept. 15-19, 2008, pp. 263-266.
4. G. Ivakhnenko (2008): *Short-Term Process Forecasting by Analogues Complexing GMDH Algorithm*. 2nd Int. Conf. on Inductive Modelling, Kyiv, Ukraine, Sept. 15-19, 2008, pp. 241-245.
5. D.A. Zubov, Y.N. Vlasov (2004): *Long-term Forecasting of the Air Average Temperature and Atmospheric Precipitations on the Linear Auto Regression Model and Maximal Error's Minimisation Criterion Basis*. Proceedings of Scientists of East Ukrainian National University named V.Dahl, Lugansk, Ukraine, pp. 40-49.
6. D. Zubov (2011): *Development of Web Application Structure for Weather Inductive Forecasting*. 4th International Workshop on Inductive Modelling (ICIM'2011), Kyiv, Ukraine, July 4-11, 2011, Kyiv, 2011, pp.123-127.
7. *Outline of the Operational Numerical Weather Prediction at the Japan Meteorological Agency*. It was read on November 18, 2012. http://wind.geophys.tohoku.ac.jp/~sakai/lab/JMA.pdf
8. Handbook – *Use a Radio Spectrum for Meteorology*. [Online]. It was read on November 18, 2012. http://www.docstoc. com/docs/24344415/ HANDBOOK---Use-of-Radio-Spectrum-for-Meteorology

9. *Basic principles for the Weather Forecast Estimations and Calculations*. It was read on November 18, 2012. www.dvgu.ru/meteo/book /Synoptic/Glava_16.pdf
10. *WeatherXML Developers Kit*. It was read on November 18, 2012. http://www.weather.ua/services/xml/
11. Jacob R. Carley, Benjamin R. J. Schwedler, Michael E. Baldwin, Robert J. Trapp, John Kwiatkowski, Jeffrey Logsdon, Steven J. Weiss (2011): *A Proposed Model-Based Methodology for Feature-Specific Prediction for High-Impact Weather*. Weather and Forecasting Journal 26:2, pp. 243-249.

PERVASIVE ALERT SYSTEM FOR FALL DETECTION BASED ON MOBILE PHONES

Kire Serafimov[1], Natasa Koceska[2,*]

[1]Faculty of Computer Science, University Goce Delcev – Stip; kire.10470@student.ugd.edu.mk
*[2]Faculty of Computer Science, University Goce Delcev – Stip; natasa.koceska@ugd.edu.mk**

Abstract:
Falls are an everyday potential health hazards that all of us are exposed to. A fall can cause injuries or hurt people especially the elderly. Critical injuries provoked by falls are among the major causes of hospitalization in elderly persons, diminishing their quality of life and often resulting in a rapid decline in functionality or death. Rapid response can improve the patients outcome, but this is often lacking when the injured person lives alone and the nature of the injury complicates calling for help. This paper presents pervasive alert system for fall detection using common commercially available Android-based smart phone with an integrated tri-axial accelerometer. The focus of this research was developing the most successful algorithm for detecting falls and distinguishing them from non-falls. Hybrid algorithm concentrating on acceleration magnitude and angle change was developed for fall detection. We implement a prototype system on the Android phone and conduct experiments to evaluate its performances on real-world falls. Experimental results show that the system achieves strong detection performance and power efficiency.

Keywords: tri-axial accelerometer, acceleration magnitude, angle change, angular velocity, elderly.

6 Introduction

Fall is a major care and cost burden to the health and social services worldwide [1, 2]. Falls and fall-induces injury are more often among the elderly people due to their stability problems and fragile bones. Although most falls produce no serious consequence, 5–10% of community-dwelling older adults who fall each year do sustain serious injuries such as fractures, head injuries or serious laceration, that reduce mobility and increase the risk of premature death [3], [4]. Besides the physical injuries the falls can also elicit dramatic psychological consequences such as decreased independence [5] and increased fear of falling [6], [7]. This can lead to an avoidance of activity that can bring about a pattern of deterioration, social isolation and decreased quality of life [8], [9].

Treatment of the injuries and complications associated with falls costs the U.S. over 20 billion dollars annually [10]. This situation deteriorates as the elderly population surges. According to the scientific reports from the World Health Organization (WHO) during the next 3 to 4 decades, there will be a very significant increase (about 175%) in the number of elderly persons, particularly the older aged. Moreover, there will be large increases in the numbers of some very vulnerable groups, such as the oldest old living alone, especially women; elderly racial minorities living alone and with no living children; and unmarried elderly persons with no living children or siblings. With the population aging, both the number of falls and the costs to treat fall injuries are likely to increase.

Falls may be very risky or even fatal especially for old people living alone. Indeed, major concerns for these adults include the risks associated with falling and whether there will be someone there to help them in case of an emergency. There is therefore a demand and need for an automatic pervasive fall detection system in which a patient can summon help even if they are unconscious or unable to get up after the fall.

In order to find falls effectively and timely, many fall detection methods have been developed and shown their well performance [11], [12], [13], [14]. The current fall detection methods can be basically classified in three types: acoustic based, video based and wearable sensor based system. The acoustic based system means detecting a fall via the analyzing on the audio signals. This is achieved by having a device, usually implanted in the floor, monitor sound and other vibrations. In generally, this method is not very precise, and is used as an assistant way to the other methods [15], [16]. The video based system means capturing the images of human movement via one or several cameras, mounted in fixed locations, and then determining whether there is a fall occurred based on the variations of some image features [17], [18], [19], [20]. The wearable sensor based system means embedding some micro sensors into clothes, to monitor the human activities in realtime, and find the occurrence of a fall based on the changes of some movement parameters [21], [22], [23]. As long as a person wear such a clothes, he will be monitored anywhere.

The major problem with existing systems is that they require some application specific hardware or software design, which increases the cost and sometimes require a training period for the users. The main objective of this work is to design pervasive alert system for fall detection using common commercially available Android-based smart phone with an integrated tri-axial accelerometer. Our system eliminates the middle man call centre service and therefore the extra monthly fee. It offers a manual cancellation button in the event of a false alarm or minor fall that the user was able to recover from. Another advantage of our system is that it allows mobility beyond the range of the house. Our device also offers a wide range of selectable alert methods should the user be hearing-impaired, seeing-impaired or otherwise.

7 System design and architecture

To be able to detect falls, the device first has to be able to sense motion and the different measurable qualities involved with motion. Sensing in the device begins with a digital tri-axis accelerometer, which measures acceleration along the three coordinate axes. Using the data acquired, the algorithm should be able to distinguishing falls from non-falls.

Upon identifying a fall, the device initiates a continuous audible, tactile, and visual warning. The user is then given a window of time (20 seconds) in which to cancel the alert in the instance that the fall is not serious and the user is able to regain their composure on their own. If left un-cancelled, the fall is considered serious and an alert is sent out.

Accelerometer provides the acceleration readings in directions of x-, y-, and z-axis. Accelerations in these directions are represented by Ax, Ay and Az, respectively. For generality, we assume the directions of x-, y-, and z-axis decided by the posture of the phone. The x-axis has positive direction toward the right side of the device, the y-axis has positive direction toward the top of the device and the z-axis has positive direction toward the front of the device. Vector A_T represents the total acceleration of the phone body. Its amplitude can be obtained by Eq. 1.

$$|A_T| = \sqrt{|A_x|^2 + |A_y|^2 + |A_z|^2} \qquad (1)$$

A mobile phone’s orientation can be determined by yaw, pitch, roll values that are denoted as θx, θy and θz, respectively. We can further obtain the amplitude of Av, the acceleration at the absolute vertical direction, from Eq. 2.

$|A_v| = |A_x*\sin\theta_z + A_y*\sin\theta_y – A_z*\cos\theta_y*\cos\theta_z|$ (2)

We consider that a fall starts with a short free fall period, which is characterized by the acceleration magnitude (Eq. 1) decreasing significantly below the 1G threshold. The impact of the body on the ground causes a large spike in acceleration. The tests have shown that the minimum value for the upper threshold is around 2.6G. After the impact there is a period when the person may struggle to regain composure. After that, if the person is seriously injured in the fall he usually remains on the ground for a period of time. In this period of time the acceleration magnitude returns to a normal level. Also there is a notable change in the smartphone’s orientation before and after the fall.

The algorithm monitors the acceleration magnitude of the mobile device to check if the acceleration magnitude breaks the predefined upper threshold, which is an indicator of a possible fall. If the upper threshold is broken, then the algorithm waits up to 20 seconds for the acceleration magnitude to return to a relatively normal level. If the magnitude doesn’t return to normal after 20 seconds it is assumed that the large spike in acceleration was caused by some other daily activity, like jogging or biking. On the other side, if the magnitude returns to normal level in less than 20 seconds then it is assumed that the person has potentially stopped struggling and is immobilized after the fall. Then the algorithm checks to see if the person’s orientation has changed. If that is true, then a fall is detected.

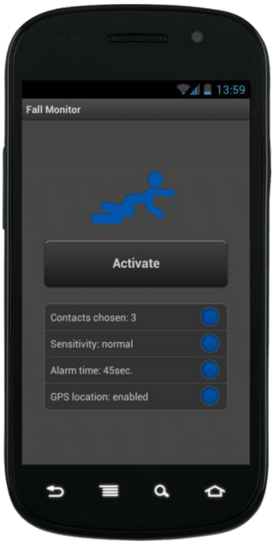
To determine the change in the person’s position we are using the vectors of gravity. The algorithm uses two readings of the force of gravity: the vector of gravity recorded 1.5 seconds before the detection of a large spike in acceleration and the vector of gravity recorded after the fall, when the acceleration returns to normal level. The angle between these two vectors is calculated and if it’s in the range between 0.98 and 1.87 radians then a fall is detected.

To determine the detection of falls, it has to circumvent the so-called false positives, which can range from a jump, going down/up stairs or even sitting in a chair. In order to circumvent these obstacles, the system was tested and evaluated under several situations. After detailed analysis of the collected data, the threshold value was defined.

This algorithm only uses the angle of change in the gravity regarding the phone’s position, and not the actual position of the phone in the moment when the person lies on the ground after the fall. Because of this, there is no restriction for the phone to be in a certain orientation. The algorithm works well regardless of the smartphone's position, i.e. it doesn't matter whether the smartphone can is placed horizontally, vertically or in some other position in the pocket; with the screen towards the body or against, or even if it is placed upside down.

3 Experimental evaluation and results

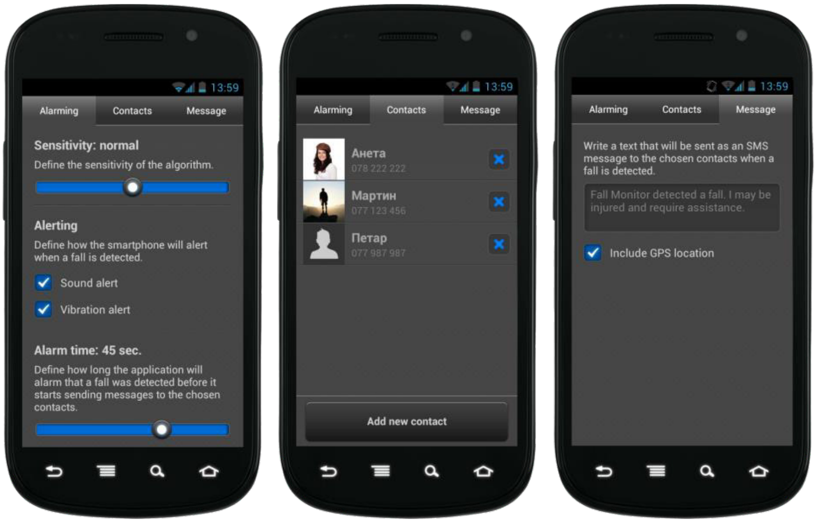
To evaluate the proposed methodology we have developed an application called Fall Monitor (Figure 1 and 2).



Fall Monitor

Contacts chosen: 3
Sensitivity: normal
Alarm time: 45sec.
GPS location: enabled

Figure 1 Main application interface



Sensitivity: normal
Define the sensitivity of the algorithm.

Alerting
Define how the smartphone will alert when a fall is detected.
☑ Sound alert
☑ Vibration alert

Alarm time: 45 sec.
Define how long the application will alarm that a fall was detected before it starts sending messages to the chosen contacts.

Анета 078 222 222
Мартин 077 123 456
Петар 077 987 987

Write a text that will be sent as an SMS message to the chosen contacts when a fall is detected.
Fall Monitor detected a fall. I may be injured and require assistance.
☑ Include GPS location

Figure 2 Screen of the application for alerting contacts, application settings and alerting message setting

For the evaluation purposes 20 persons aged between 24 and 37 were equipped with the mobile phone fixed with elastic band on their waist. They were asked to perform 20 times the following several activities: lying down, getting up (from the bed), sitting on chair, getting up from the chair, walking, running, climbing stairs, going down stairs. Each of the test subjects was asked to simulate 40 times various situations of falling (from stand position, pushed down, slipping, falling forward, falling backward, falling aside, from the chair etc.).

The overall results for each activity for all test subjects are presented in the Table 1.

Table 1 Results from the experimental fall detection using a confusion matrix with various activities

Activity	Fall detected		Number of trials	Percentage of correct action recognition
	Yes	**No**		
Falling	796	4	800	99,50%
Lying down on the bed	21	379	400	94,75%
Getting up from the bed	7	393	400	98,25%
Sitting on chair	9	391	400	97,75%
Getting up from the chair	2	398	400	99,50%
Walking	12	388	400	97,00%
Running	47	353	400	88,25%
Climbing stairs	22	378	400	94,50%
Going down stairs	23	377	400	94,25%

To make the application operable during a longer period of time, four steps are taken to reduce power consumption: (1) the monitoring daemon runs in the background while other components of the program halt; (2) the sampling frequency can be adjusted; (3) the pattern matching process is launched only after daemon-collected data exceeds the preset threshold; and (4) hardware such as the screen is activated only when necessary.

4 Conclusion

The main contributions of this paper are the following:

- We propose utilizing mobile phones as the platform for pervasive fall detection system development using mobile phones to integrate comprehensive fall detection and emergency communication.
- We design an algorithm for fall detection systems using mobile phones. It is an acceleration-based detection approach whose only requirement is that a mobile phone has an accelerometer.
- We design and implement a pervasive fall detection system, on the mobile phone-based platform to conduct fall detection. It has few false positives and false negatives; it is available in both indoor and outdoor environment; it is user-friendly, and it requires no extra hardware and service cost. It is also lightweight and power-efficient.
- We conduct experiments to evaluate detection accuracy. The experimental results show that our detection system achieves good performance in terms of low false negative and low false positive in fall detections.

This system is applicable not only to elderly but also to healthy individuals performing various activities walking, running, climbing, cycling, rolling, etc. experiencing falls due to various causes such as: unexpected health problems, inattention, dangerous environment, car accidents, attacks, etc.

Референци (References)

1. Annekenny R, O'Shea D. *Falls and syncope in elderly patients*. Clin Geriatric Med 2002;18:xiii-xiv.
2. Scuffam P, Chaplin S, Legood R. *Incidence and costs of unintentional falls in older people in the United Kingdom*. J Epidemiol Community Health 2003;57:740-4.
3. Tinetti ME, Doucette J, Claus E, Marottoli R (1995) *Risk factors for serious injury during falls by older persons in the community*. J Am Geriatr Soc 43: 1214–1221.
4. Sadigh S, Reimers A, Andersson R, Laflamme L (2004) *Falls and Fall-Related Injuries Among the Elderly: A Survey of Residential-Care Facilities in a Swedish Municipality*. Journal of Community Health 29: 129–140.
5. Ryynanen OP, Kivela SL, Honkanen R, Laippala P (1992) *Falls and Lying Helpless in the Elderly*. Z Gerontology 25: 278–282.

6. Spice CL, Morotti W, George S, Dent THS, Rose J, et al. (2009) *The Winchester falls project: a randomised controlled trial of secondary prevention of falls in older people*. Age and Ageing 38: 33–40.
7. Vellas BJ, Wayne SJ, Romero LJ, Baumgartner RN, Garry PJ (1997) *Fear of falling and restriction of mobility in elderly fallers*. Age and Ageing 26: 189–193.
8. Mann R, Birks Y, Hall J, Torgerson D, Watt I (2006) *Exploring the relationship between fear of falling and neuroticism: a cross-sectional study in community-dwelling women over 70*. Age and Ageing 35: 143–147.
9. Delbaere K, Crombez G, Vanderstraeten G, Willems T, Cambier D (2004) *Fear-related avoidance of activities, falls and physical frailty. A prospective community-based cohort study*. Age and Ageing 33: 368–373.
10. American Academy of Orthopaedic Surgeons, “*Don’t let a fall be your last trip: Who is at risk?*,” Your Orthopaedic Connection, AAOS, July 2007.
11. Lin, C.-W., et al., *Compressed-Domain Fall Incident Detection for Intelligent Home Surveillance*. Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2005, 2005: p. 2781-3784.
12. Nait-Charif, H. and S.J. McKenna, *Activity Summarisation and Fall Detection in a Supportive Home Environment*. Proceedings of the 17th International Conference on Pattern Recognition (ICPR04), 2004.
13. M.Prado, J. Reina-Tosina, and L.Roa, *Distributed intelligent architecture for falling detection and physical activity analysis in the elderly*. Proceedings of the Second Joint EMBS/BMES Conference, 2002: p. 1910-1911.
14. Zhang, T., et al., *Fall Detection by Wearable Sensor and One-Class SVM Algorithm*. Lecture Notes in Control and Information Science, 2006. 345: p. 858-863.
15. Majd Alwan, Prabhu Jude Rajendran, Steve Kell, David Mack, Siddharth Dalal, Matt Wolfe, and Robin Felder. *A smart and passive floor-vibration based fall detector for elderly.*
16. Mihail Popescu, Yun Li, Marjorie Skubic, and Marilyn Rantz. *Anacoustic fall detector system that uses sound height information to reduce the false alarm rate*. 30th Annual International IEEE EMBS Conference, August 2008.
17. Tracy Lee and Alex Mihailidis. *An intelligent emergency response system: preliminary development and testing of automated fall detection*. Journal of Telemedicine and Telecare, 11(4):194–198, 2005.

18. Shaou-Gang Miaou, Pei-Hsu Sung, and Chia-Yuan Huang. *A customized human fall detection system using omni-camera images and personal information* p.39–41. Proceedings of the 1st Distributed Diagnosis and Home Healthcare (D2H2) Conference, April 2006.
19. Caroline Rougier and Jean Meunier. *Fall detection using 3d head trajectory extracted from a single camera video sequence*. The First International Workshop on Video Processing for Security June 7-9, 2006 Quebec City, Canada
20. Hammadi Nait-Charif and Stephen J. McKenna. *Activity summarisation and fall detection in a supportive home environment*. 2004.
21. K Doughty, R Lewis, and A McIntosh. *The design of a practical and reliable fall detector for community and institutional telecare*. Journal of Telemedicine and Telecare, 6(1):150–154, 2000.
22. Thomas Riisgaard Hansen, J. Mikael Eklund, Jonthan Sprinkle, Ruzena Bajcsy, and Shankar Sastry. *Using smart sensors and a camera phone to detect and verify the fall of elderly persons*. European Medicine, Biology and Engineering Conference (EMBEC 2005), November 2005.
23. G Williams, K Doughty, K Cameron, and D.A. Bradley. *A smart fall and activity monitor for telecare applications*, volume 30, pages 1151–1154. Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 1998.

ESTABLISHEMENT OF A HEALTHCARE INFORMATION SYSTEM

Ass. Prof. Alexandar Kostadinovski, Faculty of Economics, "Goce Delchev University " - Stip, aleksandar.kostadinovski@ugd.edu.mk;
Ass. Prof. Drasko Atanasoski, Faculty of Tourism and Business Logistics, "Goce Delchev University-Stip, drasko.atanasoski@ugd.edu.mk

Abstract

Having healthcare information on a disposal which is reliable and timely is a base for starting up any action on the healthcare system. But often, especially in developing countries, such information is not available, because these are traits of insufficient investment in data collection system, their analyses, understanding and usage. As a result, managers in these countries are not able to identify problems and needs, also to monitor progress and assess the impact of interventions which appear as a condition to make decisions related to health policy and the design of programs and allocations of resources which are based on evidence.

Introduction

The ultimate goal of the Healthcare information system is to unable various stakeholders in the healthcare system in order to make transparent decisions based on evidence. The performances of Healthcare information system should not only be calculated on the basis of quality of the produced data, but on the evidence for continued usage of such data as well; all of this in order to improve the performances of the healthcare system and health status among population. Improving the Healthcare information systems in terms of data availability, quality and their application often require interventions that indicate a wide range of possible determinants of performance. Lafond and Field proposed a classification of these determinants divided into three categories: technical, organizational and behavioral determinants[1]. These determinants are explained in a triple or prismatic framework shown in Figure 1.

[1] Lafond A, Field R: The Prism: introducing an analytical framework for understanding performance of routine Healthcare information systems in developing countries. Eastern Cape Province, South Africa, 2003

Components of the healthcare system

Healthcare information system can be illustrated through terms of its inputs (resources), processes (selection of indicators and data sources; collection and data management) and outputs (product information and dissemination and use of information). As of the aforementioned it can be concluded that the Healthcare information system is consisted of the following 6 componenents.[2]

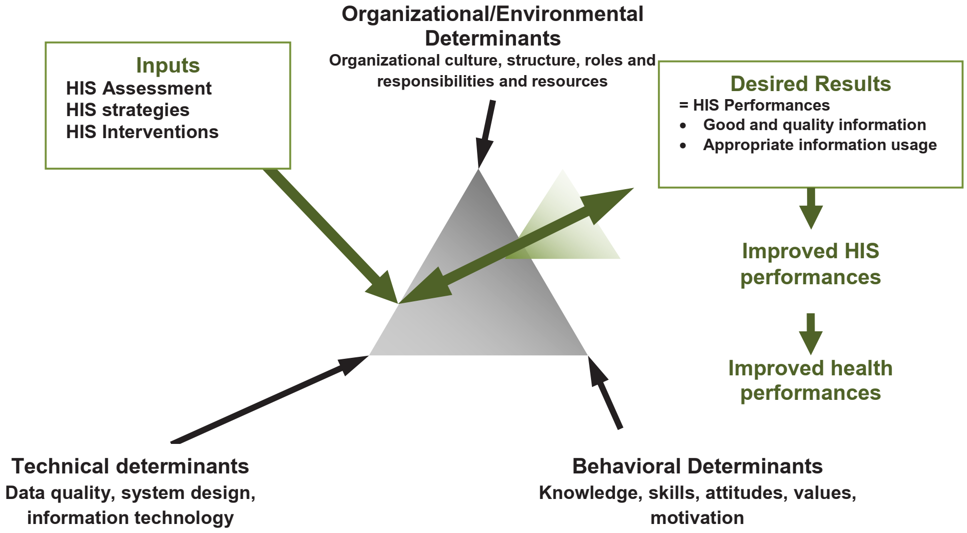

Organizational/Environmental Determinants
Organizational culture, structure, roles and responsibilities and resources
Inputs
HIS Assessment
HIS strategies
HIS Interventions
Desired Results
= HIS Performances
• Good and quality information
• Appropriate information usage
Improved HIS performances
Improved health performances
Technical determinants
Data quality, system design, information technology
Behavioral Determinants
Knowledge, skills, attitudes, values, motivation

Figure 1: Prismatic framework for comprehenstion of HIS performance

Resources of the healthcare information system. During operation of the HIS there are certain prerequisites that should be fulfilled. It is about legal, regulatory and planning frameworks in order to ensure a fully functioning of HIS and availability of resources for health information necessities, including human potential, logistical support, information and communication technologies and the coordinating mechanisms in terms of and between those 6 components.

[2] World Health Organization: Health metrics network: Framework and standards for the development of country healthcare information systems, WHO 2006, pg. 19

Information policies. This refers to a legal and regulatory context within which the application of the health information is generated, which is actually an essential element because it allows the establishment of mechanisms to ensure availability, exchange, quality and sharing data. The existence of a legal and policy framework which is consistent with international standards enhances confidence in the integrity of the results. Financial resources. Not enough evidence is to determine the required level of investments in order to ensure sustainable healthcare information system, bur ir can be expected to vary according the overall level of development of the concerned country. The annual expenses for a complete healthcare information system were estimated to a range between 0.53- 2.99 USD per capita[3].

Human resources. Improvements of the healthcare information system cannot be achieved if a proper attention is not paid to the training, development, reward and career growth of staff at all levels. Numerous skilled epidemiologists, statisticians and demographers are needed on a national level in order to monitor the quality of data and to ensure proper analysis. At a peripheral level, health information staff should be responsible for collecting, reporting and data analysis.

Information and communication technology. Information technology can affect the improvement of the quality of data collected and communication technology can improve the timeliness, analysis and information usage. This indicates to the need to adopt a clear policy of data management, which would also point out the issues of privacy and confidentiality. Ideally, at a national and sub-national level, health managers should have access to the information infrastructure that includes computers, email and internet access. National and regional statistical units should be equipped with transport and communication equipment in order to enable timely collection and compilation of data on sub-national level.

Coordination and leadership. It is necessary to establish a committee that would have constituted the key interest groups from the country's health and statistical sectors. He should be responsible for development and maintenance of healthcare information system and to ensure that information is shared between programs and institutions.

[3] Stansfield SK et al: Information to improve decision making for health. Pg. 20

1. Indicators. Healthcare information system is not restrictively limited to the health sector, at the same time, there is a strong connection between this system and the information systems in the other sectors. HIS should provide information that would meet wide range of needs, from the data for delivery of services to individual customers, statistical data for planning and management of health services and measurements relevant to health policy formulation and evaluation.

Some essential health indicators in the assessment of changes in the three main areas are required (figure 2): *determinants of health, healthcare system and health status*.

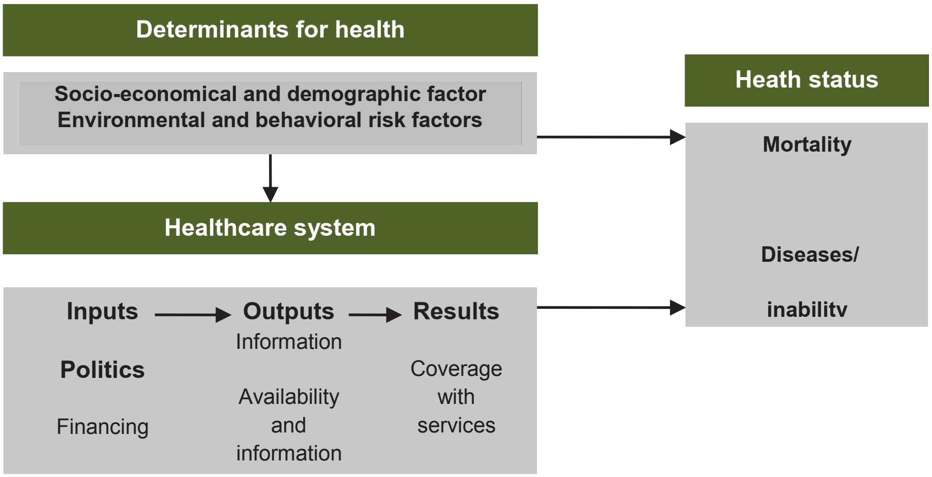


Figure 2: Measuring areas of healthcare information systems

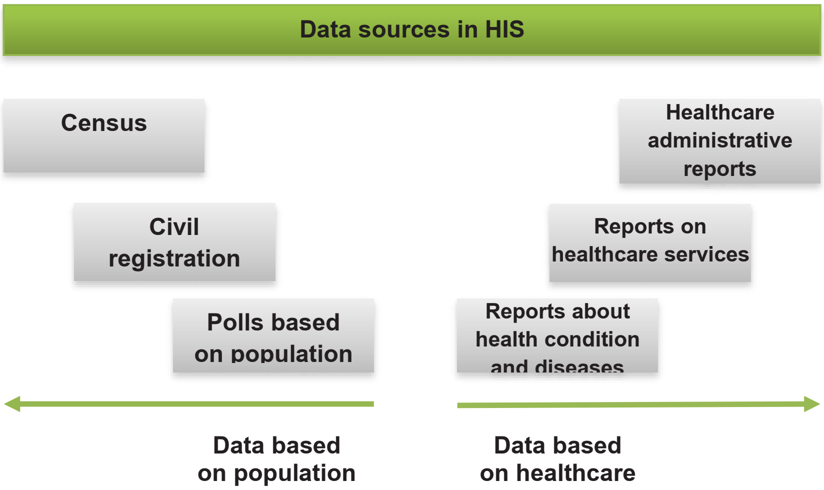
(Source: World Health Organization: Health metrics network: Framework and standards for the development of country Healthcare information systems, WHO, 2006, p. 23).

It is important to make a rational selection of the minimum set of core health indicators. In recent WHO publications standard definitions and points of measurements related to 40 core indicators could be found[4]. Health indicators should be valid, reliable, specific, sensitive and feasible to measurements.

[4] World Health Statistics 2005. Geneva, World Health Organization, 2005.

They also need to be relevant or useful for decision making at the level of data that is collected or where necessity for data at higher levels is quite clear.

2. Data sources. The selection of the most appropriate data source depends on the required information, the effectiveness and convenience methods, human and technical capacity required for data collection, management and dissemination of data, as well as the financial and time constraints. All healthcare information systems of the countries should be based on a set of core data sources. Sources of data, as seen from figure 3, can be divided into two broad categories: those that generate data concerning the population as a whole (population-based sources) and those that generate data for operations related to health services (based sources of health services).[5]


Data sources in HIS
Census
Civil registration
Polls based on population
Healthcare administrative reports
Reports on healthcare services
Reports about health condition and diseases
Data based on population
Data based on healthcare

[5] World Health Organization: cited, pg.26

Census				●
Life's statistics	●			●
Polls	●	●	●	●
Reports on heath status	●		●	●
Reports on services	●		●	
Administrative reports		●		

Table 1: Data sources for indicators according to regions

3. Data management. Data management involves a set of procedures applied during collection, storage, analysis and distribution of data (figure 4).

Figure 3: Data sources into a comprehensive healthcare information system

(Source: World Health Organization: Health metrics network: Framework and standards for the development of country Healthcare information systems, WHO, 2006, p. 27)

Every important health indicator should be associated with one or more appropriate data sources. Sometimes there is only one method of data collection, but it happens very often that different data sources can be used in generating similar indicators. In such a situation, all the circumstances should be taken into account, in order to make decisions about the most appropriate data sources (Table 1).

	Health status	**Healthcare system**		**Determinants**
		Inputs and outputs	**Results (benefits)**	

The collection of accurate and complete data is a fundamental prerequisite and a basic of data management plan. The tool used for this purpose is the so-called metadata dictionary. Metadata dictionary strictly defines the data elements and their usage in indicators. It specifies the method of collecting data, periodicity, and measurement techniques used methods of assessment and possible inconsistencies in the data. It is a critical element in ensuring the quality and transparency of data.

Integrated data storage offers many significant benefits. Integrated data from various sources could perform the best application of complementarity and data synergy. Developing data warehouse and metadata dictionary becomes possible to create an integrated healthcare information system.

The analysis and presentation of data should improve their usage of local or district level where they could acquire the most significant impact on the delivery of health services. Data repository provides instantaneous feedback of information to the institution or district level. At the national level, the data warehouse provides adequate central position where all data are available for analysis, evaluation and research, which in turn has an impact on decisions related to policy, planning and management.

The distribution of data at all levels within the country, beginning from the authorities as well as international partners, is eased owing to the data repository. It should be designed with a web internet network and is connected with the appropriate access control. A significant tool in the management of information is the electronic documentation center where all relevant outputs of the country are accumulated.

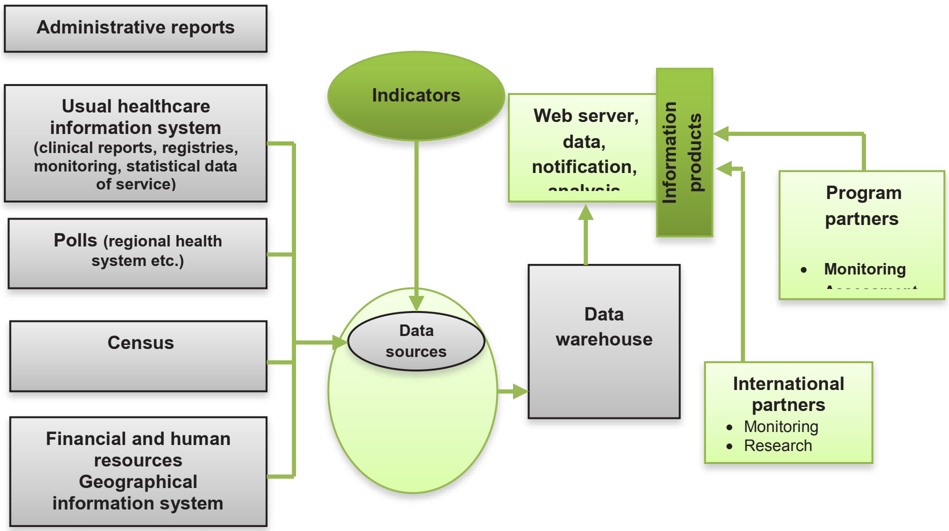

Administrative reports
Usual healthcare information system (clinical reports, registries, monitoring, statistical data of service)
Polls (regional health system etc.)
Census
Financial and human resources Geographical information system
Indicators
Data sources
Data warehouse
Web server, data, notification,
Information products
Program partners
Monitoring
International partners
Monitoring
Research

Figure 4: Data management

HIS should ensure that the data is intercepting the standards of reliability, transparency and completeness.

4. Information products. As previously discussed HIS data where pointed out as in the form of *products*. However, the data represent only raw products. Appearing as such, they have a minor value until they are refined, controlled, organized and analyzed. At this stage the data becomes *information*. Information should be displayed in front of the staff and the public. As with this information system and the quality of its information is gradually improving through cyclical processes of learning. Such necessity arouses because individual information has limited value until it is integrated with other information and therefore be evaluated through issues facing the healthcare system. At this level, information becomes *evidence*, which as such is used for making local decisions within the system.

(Source: World Health Organization: Health metrics network: Framework and standards for the development of country Healthcare information systems, WHO 2006, pg. 39)

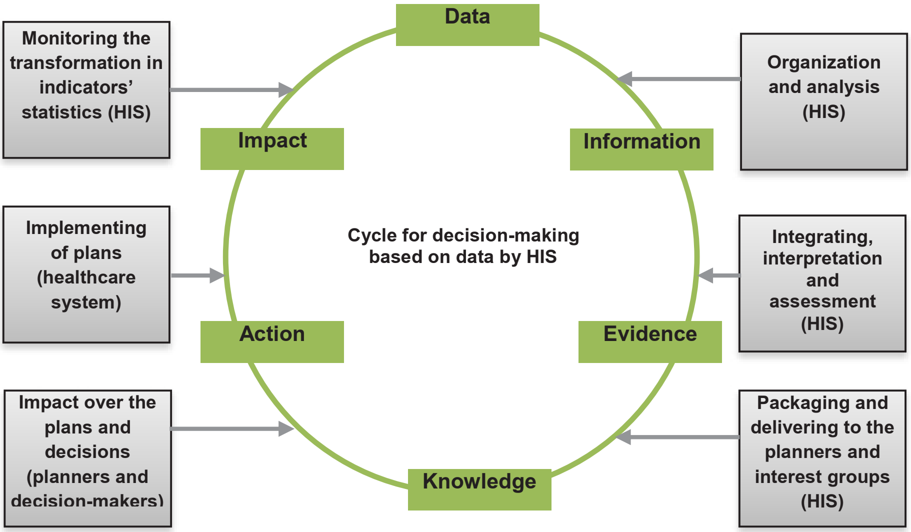

Data
Monitoring the transformation in indicators' statistics (HIS)
Organization and analysis (HIS)
Impact
Information
Implementing of plans (healthcare system)
Cycle for decision-making based on data by HIS
Integrating, interpretation and assessment (HIS)
Action
Evidence
Impact over the plans and decisions (planners and decision-makers)
Packaging and delivering to the planners and interest groups (HIS)
Knowledge

Figure 5: Relation of data impact over healthcare system

As of the data's movement towards higher levels of the healthcare system through data repositories at these levels, they are synthesizing and triangulating (comparing) with other sources and further on compiling into statistical data which is useful for more thorough analyses and comparison within the healthcare system. The synthesis of the evidence is not yet sufficient until they pack up, communicate and deliver to the management in a form that changes their understanding of issues and needs. At this level, the evidence becomes *knowledge.* Once knowledge is applied, it is logical to expect that through the planning process it could easily result in *action* or change, which in turn has an *impact* to the indicators. Such impact should be measurable through changes of statistics indicators data.

5. Dispersion and usage. Information is used at different levels within the healthcare system through the processes of managing healthcare services, healthcare system management, planning, advocacy and policy

(Source: World Health Organization: Health metrics network: Framework and standards for the development of country Healthcare information systems, WHO 2006, pg. 44) development. Information dissemination should be planned in accordance with the very own characteristics of each user, in which the utmost effective packaging and communication channel for transmitting information should be selected. Time transfer of information should be carefully planned, in order to fully coincide with the planning cycle and the needs of users. Communication experts can be considered as of a great assistance in packaging information for different audiences.

Conclusion

Healthcare information systems include complex processes and relations that go beyond the responsibility of any single government agency. The development of healthcare information systems need to respond to the needs and requirements of different institutions within the comprehensive plan, using the approach of cooperation rather than individual consideration of only one entity. In the context of health sector reforms and decentralization, healthcare systems are managed to the level of service delivery. Such transfer of functions from central to peripheral levels generates new information needs and requires in-depth restructuring of information systems altering of requirements for data collection, processing, analyzing and understanding them as well. Standardization and quality information are the main challenges in the implementation of health sector reform, which is an issue that should be raised from the central level.

References:

1. Lafond A, Field R (2003): The Prism: introducing an analytical framework for understanding performance of routine Healthcare information systems in developing countries. Eastern Cape Province, South Africa.
2. Stansfield SK et al (2004): Information to improve decision making for health.
3. World Health Organization (2005): World Health Statistics, Geneva.
4. World Health Organization (2006): Health metrics network: Framework and standards for the development of country Healthcare information systems, WHO.

TIME COMPLEXITY IMPROVEMENT OF THE FIRST PROCESSING STAGE OF THE INTELLIGENT CLUSTERING

Done Stojanov[1,*], Cveta Martinovska[2]

[1]Faculty of Computer Science, University ,,Goce Delcev”-Stip
done.stojanov@ugd.edu.mk
[2]Faculty of Computer Science, University ,,Goce Delcev”-Stip
cveta.martinovska@ugd.edu.mk
** Done Stojanov, e - mail: (done.stojanov@ugd.edu.mk)*

Abstract.
A new approach for data clustering is presented. IC clustering [1] initial processing stage is changed, so that the interval between the smallest and the largest radius-vector is divided into k equal sub-intervals. Each sub-interval is associated to a cluster. Depending on which sub-interval a radius-vector belongs, it is initially distributed within a cluster, associated with that sub-interval.

Key words: data clustering, radius-vectors, IC clustering, intervals.

1. Introduction

Since the second half of the 20th century, several techniques for data clustering have been proposed. The oldest one, but commonly used technique for data clustering is the k-means [2] algorithm, based on initial selection of k,k<n random objects (centroids) of object set of size n. The remaining n-k objects, which are not selected as centroids, are distributed within the closest clusters. Initially, each centroid represents a cluster. When a cluster is changed, cluster's center is also changed. Centers no further change implies appropriate data distribution.

PAM (Partitioning Around Medoids) [4] as opposed to the k-means algorithm, effectively handles extreme values (data outliers), which can easily disrupt the overall data distribution. Central objects within clusters (medoids) are used. Medoids are swapped only if that would result with a better data clustering.

CLARA [3] is basically PAM clustering, applied to a part (set of samples) of the object set. The result is not always the optimal one. CLARANS [5] searches graph data structure. Nodes medoids are replaced by nodes non-medoids, if that would reduce the clustering cost.

IC clustering [1] calculates the radius-vector for each object of object set of size n. During the first processing stage, the set of radius-vectors is sorted in ascending order, and then divided into k subsets of approximately equal size, where each subset initially represents a cluster. Next, radius-vectors being closer to the neighboring clusters are moved from one cluster into another. This is repeated until clusters no further change, when all objects are properly partitioned. Finally radius-vector clusters are transformed into object clusters, with properly partitioned objects.

In this paper, IC clustering is changed. Each radius-vector initially is partitioned within a cluster, determined by a sub-interval to which the radius-vector belongs, what in the worst case takes *O(nk)* processing time, where n is the size of the object set, k is the number of clusters, k<n. Certainly *O(nk)<O(n^2)*, where *O (n^2)* is the time required to sort a set of size n, what implies improved time complexity of the first processing stage of the IC clustering.

2. Preliminaries

If a set of n objects $O=\{o_1,o_2,\dots o_{n-1},o_n\}$ is given, where each object is represented with m attributes (properties), $o_i=(p_{i,1},p_{i,2},\dots,p_{i,m-1},p_{i,m})$, objects should be properly partitioned in $k, k<n$ clusters, where similar objects share a common cluster. There is no empty cluster.

3. Methodology

For each object o_i, a radius-vector $R_i = \sqrt{\sum_{k=1}^{m} p_{i,k}^2}, 1 \le i \le n$ is calculated. Memory keeps n data pairs $(i, R_i), 1 \le i \le n$, tracking object's position i in the object set O, where R_i is the radius-vector corresponding to the object at position i.

From the set of radius-vectors $R = \{R_1, R_2, ..., R_{n-1}, R_n\}$, the smallest and the largest radius-vector are chosen, $R_{\min} = \min\{R_1, R_2, ..., R_{n-1}, R_n\}$, $R_{\max} = \max\{R_1, R_2, ..., R_{n-1}, R_n\}$. The interval $[R_{\min}, R_{\max}]$ is divided into k equal subintervals, starting from s_1 up to s_k. A radius-vector R_i, such as $R_i \in s_j, 1 \le i \le n, 1 \le j \le k$ is satisfied, initially is partitioned in cluster c_j.

$$s_1 : [R_{\min}, R_{\min} + \frac{1}{k}(R_{\max} - R_{\min}))$$

$$s_2 : [R_{\min} + \frac{1}{k}(R_{\max} - R_{\min}), R_{\min} + \frac{2}{k}(R_{\max} - R_{\min}))$$

.....

$$s_{k-1} : [R_{\min} + \frac{k-2}{k}(R_{\max} - R_{\min}), R_{\min} + \frac{k-1}{k}(R_{\max} - R_{\min}))$$

$$s_k : [R_{\min} + \frac{k-1}{k}(R_{\max} - R_{\min}), R_{\min} + \frac{k}{k}(R_{\max} - R_{\min})]$$

Since the data distribution is initiall, some of the radius-vectors might be inappropriately partitioned. The mean values for each two neighboring clusters c_j and $c_{j+1}, 1 \le j \le k-1$, are calculated according (1) , where $|c_j|$ is the number of elements in cluster c_j. A radius-vector $R_i \in c_j$, for which $|R_i - mc_{j+1}| < |R_i - mc_j|$ is satisfied, is moved from cluster c_j in cluster c_{j+1}. Thus radius-vector $R_i \in c_{j+1}$, for which $|R_i - mc_j| < |R_i - mc_{j+1}|$ is satisfied, is moved from cluster c_{j+1} in cluster c_j. When a radius-vector is moved from one cluster into another, clusters' structure and clusters' mean values are changed, recalculating clusters' new mean values mc_j and mc_{j+1}. Objects are moved from one cluster into another neighboring cluster, until clusters' structure no further change, when all radius-vectors will be properly partitioned. Using data pairs (i, R_i) information, each radius-vector R_i is transformed into object o_i , $1 \le i \le n$. Thus clusters of radius-vectors $c_j, 1 \le j \le k$, are transformed into object clusters $oc_j, 1 \le j \le k$, having each object $o_i, 1 \le i \le n$ from the object set O properly partitioned in object cluster $oc_j, 1 \le j \le k$.

$$mc_j = \frac{\sum R_i \in c_j}{|c_j|}, 1 \le j \le k \qquad (1)$$

4. Algorithm

Algorithm 1 Improved IC: Intelligent Clustering

Input: set of objects $O=\{o_1,o_2,\ldots,o_{n-1},o_n\}$
Output: k clusters of objects oc_j, 1<=j<=k

```
for each object $o_i$ which belongs to the object set O{
calculate its radius-vector $R_i$;
store data pair (i,$R_i$) in the memory;
}
find the smallest radius-vector $R_{min}=min\{R_1,R_2,\ldots,R_{n-1},R_n\}$;
find the largest radius-vector $R_{max}=max\{R_1,R_2,\ldots,R_{n-1},R_n\}$;
determine sub-intervals $s_j$, 1<=j<=k;
i=1;
j=1;
while(i<=n){
while(j<=k){
if($R_i$ belongs to sub-interval $s_j$){
add $R_i$ in cluster $c_j$;
break while(j<=k) loop;
}
j++;
}
i++;
}
calculate centers of clusters $mc_j$, 1<=j<=k;
LOOP: j=1;
  while(j<=k-1){
  for each $R_i$ which belongs to cluster $c_j$
  if (|$R_i$-$mc_{j+1}$|<|$R_i$-$mc_j$|){
  move $R_i$ from cluster $c_j$ in cluster $c_{j+1}$;
  calculate clusters' new mean values $mc_j$ and $mc_{j+1}$;
   }
   for each $R_i$ which belongs to cluster $c_{j+1}$
   if (|$R_i$-$mc_j$|<|$R_i$-$mc_{j+1}$|){
```

```
   move $R_i$ from cluster $c_{j+1}$ in cluster $c_j$;
   calculate clusters' new mean values $mc_j$ and $mc_{j+1}$;
   }
   j++;
   }
go to LOOP while at least one $mc_j$ is changing;
transform radius-vector clusters $c_j$ into object clusters $oc_j$, 1<=j<=k;
```

5. An Example

Set of objects $O=\{(3,4),(5.7,5.9),(6,5.7),(6.1,5.8),(5.8,5.9),(4.5,4.9),(4.6,5),(7,7),(4,4),(8,6)\}$ should be partitioned in three clusters. According to the methodology being presented, for each object at position i a radius-vector $R_i, 1 \le i \le 10$ is calculated, Table 1. Memory keeps ten data pairs $(i,R_i), 1 \le i \le 10$, Table 2.

Table 1 Objects' radius-vectors

Object	(3,4)	(5.7,5.9)	(6,5.7)	(6.1,5.8)	(5.8,5.9)	(4.5,4.9)	(4.6,5)	(7,7)	(4,4)	(8,6)
Radius-vector	5	8.204	8.276	8.417	8.273	6.653	6.794	9.899	5.657	10

Table 2 Data pairs (i,R_i)

Data pairs
(1,5)
(2,8.204)
(3,8.276)
(4,8.417)
(5,8.273)
(6,6.653)
(7,6.794)
(8,9.899)
(9,5.657)
(10,10)

Once the smallest and the largest radius-vector have been found, $R_{\min} = 5, R_{\max} = 10$ intervals s_1, s_2 and s_3 can be determined.

$$s_1 : \left[5{,}5 + 1 \times \frac{(10-5)}{3}\right) = \left[5, \frac{20}{3}\right) = [5{,}6.667)$$

$$s_2 : \left[\frac{20}{3}{,}5 + 2 \times \frac{(10-5)}{3}\right) = \left[\frac{20}{2}, \frac{25}{3}\right) = [6.667{,}8.333)$$

$$s_3 : \left[\frac{25}{3}{,}5 + 3 \times \frac{(10-5)}{3}\right] = \left[\frac{25}{3}, \frac{30}{3}\right] = [8.333{,}10]$$

Distributing radius-vector $R_i, 1 \le i \le 10$ in cluster $c_j, 1 \le j \le 3$ is permitted, only if R_i belongs to the interval $s_j, 1 \le j \le 3$.

Cluster c_1: {5,6.653,5.657}, mean value $mc_1 = \frac{17.31}{3} = 5.77$

Cluster c_2: {8.204,8.276,8.273,6.794}, mean value $mc_2 = \frac{31.547}{4} = 7.887$

Cluster c_3: {8.417,9.899,10}, mean value $mc_3 = \frac{28{,}316}{3} = 9.439$

A check for radius-vectors $R_i \in c_1$, being cluster c_2 less distanced than cluster c_1, is conducted, Table 3.

Table 3 Calculating the distances between cluster c$_1$ radius-vectors and cluster c$_1$ and c$_2$ mean values

Radius-vector	Distance from cluster c$_1$	Distance from cluster c$_2$
5	|5-5.77|=0.77	|5-7.887|=2.887
6.653	|6.653-5.77|=0.883	|6.653-7.887|=1.234
5.657	|5.657-5.77|=0.113	|5.657-7.887|=2.23

According Table 3, there is no cluster c_1 radius-vector, being closer to cluster c_2 than cluster c_1, what indicates appropriate radius-vector distribution in cluster c_1.

A check for radius-vectors $R_i \in c_2$, being closer to cluster c_1 than cluster c_2, has also to be conducted, Table 4.

Table 4 Calculating the distances between cluster c$_2$ radius-vectors and cluster c$_1$ and c$_2$ mean values

Radius-vector	Distance from cluster c$_2$	Distance from cluster c$_1$
8.204	|8.204-7.887|=0.317	|8.204-5.77|=2.434
8.276	|8.276-7.887|=0.389	|8.276-5.77|=2.506

8.273	|8.273-7.887|=0.386	|8.273-5.77|=2.503
6.794	**|6.794-7.887|=1.093**	**|6.794-5.77|=1.024**

Considering Table 4 distance results, it can be denoted that radius-vector 6.794 is cluster c_1 less distanced than cluster c_2, where was initially distributed. In this case, radius-vector 6.794 is moved from cluster c_2 in cluster c_1. Since cluster c_1 and cluster c_2 structure has been changed, cluster c_1 and cluster c_2 new mean values are calculated.

Cluster c_1 : {5,6.653,5.657,6.794}, mean value $mc_1 = \frac{24.104}{4} = 6.026$

Cluster c_2 : {8.204,8.276,8.273}, mean value $mc_2 = \frac{24.753}{3} = 8.251$

Cluster c_3 : {8.417,9.899,10}, mean value $mc_3 = \frac{28,316}{3} = 9.439$

Distance results between cluster c_2 radius-vectors and cluster c_3 and cluster c_2 mean values are given in Table 5.

Table 5 Calculating the distances between cluster c_2 radius-vectors and cluster c_2 and c_3 mean values

Radius-vector	**Distance from cluster c_2**	**Distance from cluster c_3**
8.204	|8.204-8.251|=0.047	|8.204-9.439|=1.235
8.276	|8.276-8.251|=0.025	|8.276-9.439|=1.163
8.273	|8.273-8.251|=0.022	|8.273-9.439|=1.166

Table 5 distance results clearly show that there is no cluster c_2 radius-vector being closer to cluster c_3 than cluster c_2, where from can be concluded that cluster c_2 radius-vectors are properly partitioned.

At the end has to be checked whether exist cluster c_3 radius-vectors being cluster c_2 less distanced than cluster c_3, Table 6.

Table 6 Calculating the distances between cluster c_3 radius-vectors and cluster c_2 and c_3 mean values

Radius-vector	**Distance from cluster c_3**	**Distance from cluster c_2**
8.417	**|8.417-9.439|=1.022**	**|8.417-8.251|=0.166**
9.899	|9.899-9.439|=0.46	|9.899-8.251|=1.648
10	|10-9.439|=0.561	|10-8.251|=1.749

Once again, radius-vector being partitioned in one cluster is closer to the neighboring cluster. Cluster c_3 radius-vector 8.417 is cluster c_2 less distanced than cluster c_3 , resulting with rearrangement of radius-vector 8.417, being moved from cluster c_3 in cluster c_2. Since cluster c_2 and cluster c_3 structure is changed, clusters' new mean values mc_2 and mc_3 are calculated.

Cluster c_1 : {5,6.653,5.657,6.794}, mean value $mc_1 = \frac{24.104}{4} = 6.026$

Cluster c_2 : {8.204,8.276,8.273,8.417}, mean value $mc_2 = \frac{33.17}{4} = 8.293$

Cluster c_3 : {9.899,10}, mean value $mc_3 = \frac{19{,}899}{2} = 9.950$

Repeating this procedure from the beginning, no structure change of a cluster is recorded, where from a conclusion for clusters' no further structure change can be deduced.

Using data pairs $(i, R_i), 1 \le i \le 10$, each radius-vector is transformed into object from the object set O. Thus radius-vector clusters are transformed into object clusters, having all objects properly partitioned.

Object cluster oc_1 : {(3,4),(4.5,4.9),(4,4),(4.6,5)}

Object cluster oc_2 : {(5.7,5.9),(6,5.7),(5.8,5.9),(6.1,5.8)}

Object cluster oc_3 : {(7,7),(8,6)}

Conclusion

A new data clustering technique is presented. Each object is represented with a radius-vector. Instead of sorting a set of radius-vectors of size n (Intelligent Clustering initial processing stage [1]), the interval between the smallest and the largest radius-vector is divided in k equal sub-intervals. Depending on which sub-interval a radius-vector belongs, it is distributed within a particular cluster. Radius-vectors being less distanced to the neighboring clusters are rearranged, moving them from one cluster into another. That is repeated until clusters' structure no further change, when all radius-vectors are properly partitioned. Finally clusters of radius-vectors are transformed into clusters of objects, having all objects appropriately partitioned.

References

1. D. Stojanov (2012): *IC: Intelligent Clustering, a new time efficient data partitioning methodology*. International Journal of Computer Science and Information Technologies 3(5), pp. 5065-5067.
2. J. MacQueen (1967): *Some Methods for classification and Analysis of Multivariate Observations*. In Proc. of 5th Berkeley Symposium on Mathematical Statistics and Probability, pp. 281-297.
3. L. Kaufman and P. Rousseeuw (1990): *Finding Groups in Data, An Introduction to Cluster Analysis*, 99th Edition. Willey-Interscience.
4. L. Kaufman and P. Rousseeuw (1987): *Clustering by means of medoids*. In Statistical Data Analysis Based on the L1 Norm, pp. 405-416.
5. R. Ng and J. Han (1994): *Efficient and effective clustering methods for spatial data mining*. In Proc. of the 20th VLDB Conference, pp. 144–155.

MOODLE AS A TEACHING TOOLS IN MATHEMATICS-CASE STUDY IN UNIVERSITY “GOCE DELCEV” STIP

Tatjana Atanasova Pacemska, Sanja Pacemska, Biljana Zlatanovska
tatjana.pacemska@ugd.edu.mk,sanja.pacemska@ugd.edu.mk,
biljana.zlatanovska@ugd.edu.mk
University "Goce Delcev" Stip, Macedonia

Abstract:
During recent years, the teaching process at the University "Goce Delcev" Stip has been changing by usage of the e-learning methods. This paper compares the achievements of students in Math 1who use Moodle as a teaching tool with those who does not. Achievements of students are treated in the statistical program SPSS 17. We can conclude how e-learning impacts on the success of the students based on the results obtained.

Keywords: level of achievements, data analysis, teaching methods, Moodle

Introduction

During recent years, e-learning platforms are becoming increasingly sophisticated by showing potential as an effective way of improving the learning process. Numerous e-learning platforms exist; some require paying for access to enter the software, while others do not. The following are in the first category: WebCT, Blackboard, and TopClasse; Moodle, Ilias, and Claroline are free.[3,8] They are considered open-source software.

In the first years of the establishment and functioning of the University "Goce Delcev", the Republic of Macedonia, the teaching process in math courses was mostly realized by classical verbal text methods:

- Curriculum was presented to the students with a well-known and proven method (blackboard-chalk);
- Students recorded observations on the same classes, and they later served as a guide in the learning process;
- At the beginning of the course, the students received a list of literature needed, that partly could be found in the bookstore and library, but the most of it should have be found by themselves, because at that time the main source of learning for the students were the notes taken at the consultation classes with the teachers and the assistants.

With the development of the University and the efforts of all employees to make it modern higher educational institution in which teaching process will follow modern methods, an imminent need for change was to implement e-learning as a modern platform that functions in several Universities in Europe and the world. The university had a desire to make a connection between the art of the lectures and the exercises with the power and strength of the new IT technology, involving the generation and transfer of knowledge through the use of information and communication technology (ICT in teaching). E-learning as a method combines modern methods of learning with the management of knowledge and offers better ways to evaluate it.[7] We got a virtual learning tool which supports the usual learning. The teachers at the Department of Mathematics and Statistics adapted this way of working relatively quickly as a way of acquiring modern education which includes motivation, communication, efficiency and technology.

Context of the research problem (technology supported learning, advantages and disadvantages)

New technologies (the Internet, in particular) provide faculty with the tools for teaching–learning including the web-based applications known as e-learning Platforms. E-learning platforms have transformed the ways professors teach and students learn.[6] This transition has made it possible for students to take part in the learning process, while the role of the teacher is that of “conductor”, orchestrating and guiding students their education.[4] Within this framework, University professors have had to modify the subjects and methodology involved in teaching/learning. Students must actively collaborate in learning, participating and collaborating with their teachers.

In the process of realization of math courses, we approach to the application of e-learning method developed in the following way:

- we created electronic courses, which are attached lectures and exercises as basic learning materials, supplementary materials, scripts, a collection of exercises, electronic books, and anything else that can help the student in the learning process. The courses make it possible to attach papers and homework. All information related to the subject is in the form of news, announcements, events, and results, the students get appropriate courses. The knowledge check can be done by organizing short tests and quizzes. On the courses there is a calendar with planned activities given;
- speed of communication between teachers, collaborators and students increased through the use of tools for collaboration and communication, setting up discussion forums etc..;
- the courses provide checking and evaluation of some students skills.[1,2]

In the process of transformation of teaching, we observed the following benefits:

- the materials, as well as electronic books, were available to students at any time and free of charge. Before this, students were not always able to obtain the recommended titles given by teachers and assistants;
- the students are not forced to "take" notes at lectures and exercises and can become active participants in the teaching process;
- in the learning process communication with other participants is possible without having physically meet them which saved time and money.

In this process, we met some difficulties in the following nature:

- e-learning user requires specific knowledge and skills in using the computer. Without basic computer literacy, e-learning would be hindered. It is necessary to possess adequate computer equipment, because the slightest technical problem will affect the student's concentration;
- E-learning requires students' greater responsibility. They themselves have to estimate, how much time they need for learning certain contents, to motivate themselves, which can lead to poor progress in the learning process.

The interest of the participants in the process of conversion of math is the measurement of student achievement in math final exams and it is compared to those achievements by way of teaching process.

Research Methodology

Mathematics 1 of Computer Science at the University “Goce Delcev”, the Republic of Macedonia is taught in the first semester. In academic years 2010/2011 and 2011/2012 part of the teaching process makes use of the electronic course in Math 1.

We analyzed the level of achievement of students in the February exam for 2009/2010, when the teaching process was realized with classical verbal text method and for 2010/2011, 2011/2012, when the teaching process was supported by e-learning.

[8] The data processing is done in the statistical package SPSS17.[5]

Analysis of research results

Table 1 shows the success of students achieved in the academic year 2009/2010.

Table 1: The achievements of students in February exam for generation of 2009/2010

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
passed	54	45,8	45,8	45,8
failed	64	54,2	54,2	100,0
total	118	100.0	100.0	

The course of math 1 in the winter semester of 2009/2010 year was attended by 118 students. From Table 1, it can be seen that 45.8% of students passed the exam in February, while 54.2% have not passed. A more detailed analysis of the achievement of students who passed the exam is given in Table 2:

Table 2: Results of students who passed in February examination period for generation 2009/2010

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	6	32	50.0	50.0	50.0
	7	15	23.4	23.4	73.4
	8	9	14.1	14.1	87.5
	9	5	7.8	7.8	95.3
	10	3	4.7	4.7	100.0
	Total	64	100.0	100.0	

From the given results it can be seen that more than 50% of the students who passed the exam passed it with grade 6. Only 4.7% of the passed students received grade 10. The average success achieved in academic year 2009/2010 in math 1 for February exam is 6.94.

Table 3: Measures of central tendency for the achievement of students for February exam for generation 2009/2010

N	Valid	64
	Missing	0
Mean		6,94
Median		6,50
Mode		6
Std. Deviation		1,180
Variance		1,393

For the academic year 2010/2011 for February exam, the data are shown in Table 4.

Table 4: The achievements of the students for February exam for generation 2010/2011

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
passed	72	56,7	56,7	56,7
failed	55	43,3	43,3	100,0
total	127	100.0	100.0	

The results show that of the 127 students who claimed exam in math 1, 56.7% of students passed the exam. More of students passed the exam this year than the previous one.

The success of passed students is given in the following table:

Table 5: The achieved of students, who passed for February exam for generation 2010/2011

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	6	38	69.1	69.1	69.1
	7	7	12.7	12.7	81.8
	8	6	10.9	10.9	92.7
	9	2	3.6	3.6	96.4
	10	2	3.6	3.6	100.0
	Total	55	100.0	100.0	

80% of students passed the exam with a grade 6 or 7, while only 3.6% passed with grade 10. Passed students' average performance is 6.60, which is very close to the average success last year.

Table 6: Measures of central tendency for the achievement of students in February examination period for generation 2009/2010

N	Valid	55
	Missing	
Mean		6,60
Median		6,00
Mode		6
Std. Deviation		1,065
Variance		1,133

In the academic year 2011/2012 students in math 1 achieved the following results:

Table 7: The achievements of the students for February exam for generation 2011/2012

	Frequency	Percent age	Valid Percentag e	Cumulative Percentage
passed	67	51,5	51,5	51,5
failed	63	48,5	48,5	100,0
total	130	100,0	100,0	

Table 8: Achieved success of students who passed for February exam for generation 2011/2012

		Frequency	Percent age	Valid Percentag e	Cumulative Percentage
Valid	6	24	35.8	35.8	35.8
	7	18	26.9	26.9	62.7
	8	15	22.4	22.4	85.1
	9	7	10.4	10.4	95.5
	10	3	4.5	4.5	100.0
	Total	67	100.0	100.0	

51.5% of students passed the math 1 in February exam session. 15% of passed students won grades 9 and 10. The number of students who received a minimum grade for passing the exam reduced. Average performance achieved was 7.21 In Table 9, we have the best average grade.

Table 9: Measures of central tendency for the achievement of students for February exam for generation 2011/2012

N	Valid	67
	Missing	0
Mean		7,21
Median		7,00
Mode		6
Std. Deviation		1,175
Variance		1,380

The success we are achieving with students in the three years of study in the February examination period is changed. From the analyzes it can be seen that in the academic year 2010/2011 the success of students reduces, a large percentage (69.1%) of students received a grade 6. Next year this percentage drops to 35.8%, but at the expense of increasing the number of students who received 7 or 8. The last academic year 2011/2012 achieved the best results in terms of the number of passed students, and obtained higher average performance grade.

From the analyses previously made, we can conclude that the percentage of passed students is increasing, and the average success of the students who passed the exam increases. It is shown in the following charts:

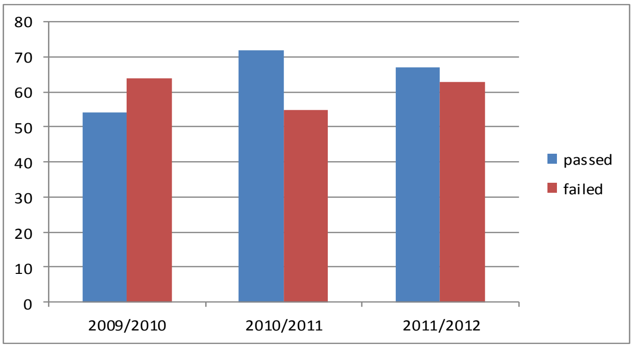


Figure 1: The results of generations of students for February exam

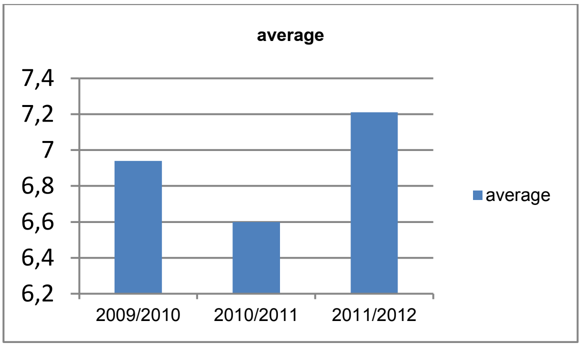


Figure 2: Average success of generations of students who passed for February exam

Figures 1 and 2 show that the academic year 2010/2011 is the year that reduces the number of passed students who passed the year with students' average performance. It is the period when the more intensive use of e-learning is applied in the learning process. In this period, teachers and students needed the time and training to use e-learning tools. But later the results were already visible. The achievement of students in math 1 has increased. In order to determine whether the dependence of the students' success achieved in three academic years 2009/2010, 2010/2011 and 2011/2012 and the way of implementation of the curriculum is connected we use the hypothesis:

H_0: There is a statistically significant difference between the success that students achieve, and the way of implementing the curriculum, opposed to the alternative hypothesis:

H_1: There is no statistically significant difference between the students' success and the way of learning curricula.

However, Pearson χ^2 test is used.

Evaluation of student achievement in two consecutive academic years:

Table 10: Test χ^2 for teaching 2009/2010-2010/2011

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	86.210[a]	1	.000
Continuity correction	82.714	1	.000
N of Valid Cases	118		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 20.59.

b. Computed only for a 2x2 table

Table 11: Test χ^2 for teaching 2010/2011-2011/2012

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	62.414[a]	1	.000
Continuity correction	59.512	1	.000
N of Valid Cases	127		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 20.59.

b. Computed only for a 2x2 table

Table 12: Test χ^2 for teaching 2009/2010-2011/2012

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	75.786[a]	1	.000
Continuity correction	72.574	1	.000
N of Valid Cases	118		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 20.59.

b. Computed only for a 2x2 table

In all three tests the hypothesis Pearson test value is obtained Asymp. Sig = 0.000. This means that there is a statistically significant difference between the success students achieve and the way they realize the curricula.

Conclusion The results of students achieved in math 1 may not be the best but they show a tendency for improvement. Our findings are confirmed, the application of e-learning as a method of realization of math leads to improved student achievement. Teaching becomes dynamic, and therefore more interesting for monitoring by students. Students can increase their learning skills using IT. Those using the Moodle platform regularly throughout the school year seem to get better grades than those who rarely or never use it. However, to implement e-learning environments, students' acceptance of this technology is a very important issue.

In summary, this research contributes to the field of e-learning platforms acceptance because it provides insight on factors that contribute to intention to adopt this technology. The findings point out specific actions by faculty that can improve student experience with Moodle and identify other actions that appear to have no effect. These results could be used to direct Universities toward successful paths for supporting communication between teachers and students using Moodle. Further research might investigate the importance of influences such as individual differences, prior experience, level of educations, different countries and the role of technology in Universities in the context of predictors of perceived ease of use and usefulness. More broadly, future research should seek to further extend models of technology acceptance to encompass other important theoretical construct in education.

References

1. A. Bergeren, D. Burgos, J.M. Fontana, D. Hinkelman, V. Hung, A. Hursh(2005) *Practical and pedagogical issues for teacher adoption of IMS learning design standards in Moodle.* LMS Journal of Interactive Media in Education
2. A. Ciudad *Teaching innovation and use of the ICT in the teaching-learning process within the new framework of the EHEA, by jeans of Moodle platform* American Journal of Business Education, 3 (13) (2010), pp. 13–19
3. C. Romero, S. Ventura, E. García(2008)*Data mining in course management systems: Moodle case study and tutorial .*Computers & Education, 51, pp. 368–384
4. G. Fillion, M. Limayem, T. Laferrière, R. Mantha(2007) *Integrating ICT into higher education: a study of onsite vs online students' perceptions.* Academy of Educational Leadership Journal, 11 (2), pp. 45–72
5. S.Pacemska, S.Jakimovic, T.A.Pacemska (2011)„ Efekti od koristenje na programskiot paket GeoGebra vo temata „Funkcija.Proporcionalnost "vo VII oddelenie od osumgodisnoto osnovno obrazovanie, VI Megunaroden Balkanski kongres za obrazovanie i nauka "Sovremeno opstesvo i ", 30.09-1.10. 2011, Ohrid
6. T.Escobar-Rodriguez,P.Monge-Lozano(2012)*The acceptance of Moodle technology by business administration students.* Computer&Education, Vol58,Issue4,pp.1085-1093T.
7. T. Teo, J. Noyes (2011*) An assessment of the influence of perceived enjoyment and attitude on the intention to use technology among pre-service teachers: a structural equation modelling approach.* Computer & Education, 57, pp. 1645–1653
8. T. Martin, A. Serrano(2009) *The role of new technologies in the learning process: Moodle as a teaching tool in Physics.* Computer & Education, 52, pp. 35–44

TOURISM RECOMMENDATION SYSTEMS: ANALYTICAL APPROACH

Biljana PETREVSKA[6]
Marija PUPINOSKA GOGOVA[7]
Zoran STAMENOV[8]

Abstract: Since tourism generates numerous positive impacts, each country is interested in its development. The base for increasing the number of tourists lies in capability to meet their preferences, which is not a trouble-free process, particularly in times of ever-changing environment. The tourist's behavior has changed dramatically specifically to the way how they search for information in the Web as the leading source. The paper argues the importance of introducing tourism recommendation systems, particularly in small and tourism developing countries as Macedonia. Moreover, it makes an attempt to justify the necessity of designing tourism recommenders in order to assist the tourists to identify their holiday in more sophisticated way.

Key words: Tourism; Recommendation systems; Tourists' preferences.

1. Introduction

Tourism has emerged as one of the major industries in the world economy by benefiting numerous sectors. Thus, each country insists in developing it and making a profit from its variety of impacts. Everyone is interested in increasing the number of visitors since it serves as a source of economic growth. In 2011, the international tourism continued to grow, despite an increasingly uncertain global economy, political changes and natural disasters around the world. The international tourist arrivals reached a record 982 million, an increase of 4.6% compared to previous year, while receipts grew by 3.8% to €740 bn (UNWTO, 2012: 7). With growth forecast to continue in 2012, although at a slightly slower rate of between 3% and 4%, international tourism will hit a major milestone in 2012: one billion international tourists. The one billionth tourist is expected to travel sometime in December 2012 (UNWTO, 2012: 8).

However, attracting bigger number tourists is not a trouble-free process, particularly in times of ever-changing travel preferences. Despite the variety of options regarding tourist destination or attraction, tourists frequently are not capable to cope with such a huge volume of choice. So, they need advice

[6] PhD, Assistant Professor, "Goce Delcev" University, Faculty of Tourism and Business Logistics, Stip, Macedonia, biljana.petrevska@ugd.edu.mk

[7] Professor of Computer science, "Bratstvo Edinstvo" - Ohrid, Macedonia, mpg@hotmail.com

[8] Sales specialist, Info-Kod - Skopje, Macedonia, stamenov.zoran@gmail.com

about where to go and what to see. In a tourism domain, recommendations may indicate cities to go to, places to visit, attractions to see, events to participate in, travel plans, road maps, options for hotels, air companies, etc. Such scope of work very often is not a trivial task. In this respect, recommenders assist tourists by facilitating personal selection and prevent them from being overwhelmed by a stream of superfluous data that are unrelated to their interest, location, and knowledge of a place. So, it is much easier for tourists to access the information they need thus resulting in shorter lead-time for bookings, making last-minute decisions and generally, tailoring their own packages from a suite of options. Solution is seen in developing recommenders in tourism domain.

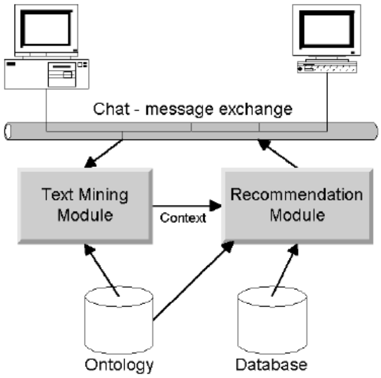
Generally, the contribution of this paper lies in the fact that gives an overview of necessity for developing recommendation systems in tourism. Moreover, it may serve as a starting thinking point for making attempts for introducing tourism recommenders in Macedonia. Finally, the paper may alarm the relevant tourism-actors in Macedonia, that the time has changed and that on-line experience has shifted from searching and consuming to creating, connecting and exchanging.

The remainder of the paper is organised in several sections. After the introductory part, the section 2 provides a brief overview of developing recommendation systems in tourism. Section 3 presents a snapshot on theoretical and empirical literature. Section 4 is rich on facts at glance towards the necessity of developing tourism recommenders in Macedonia. The most interesting conclusions and future challenges are presented in Section 5 which is the final part of the paper.

2. Recommendation systems in tourism

Tourism is an interesting phenomenon particularly for recommendation purposes. Being detected as the only way out in assisting tourists and travelers to identify their ideal holiday, recommenders offer personalization of information delivery to each traveler, together with travel history. Yet, the advanced tourist information systems must offer more than just relatively static information about sights and places. Over the past two decades a noteworthy transformation was made from just passive searching and surfing to creating content, collaborating and connecting. In this respect, the Web became the leading source of information particularly important in times of increased number of competitors in tourism market. The way out is detected in application of recommenders as a promising way to differentiate a site from competitors.

Generally, recommendations may be made to a tourist by software, as in a multimedia totem, an ATM device, or in a Web site, or by a human intermediary (e.g., the travel agent) who will receive information from a decision support system (Figure 1). However, the most successful results may be expected by applying collaborative filtering and content-based filtering (Figure 2). Based on conversational approaches, such recommenders are promising in tourism, meaning that the user is giving opportunity to choose a quantum of tourist items with regards to personal preferences.



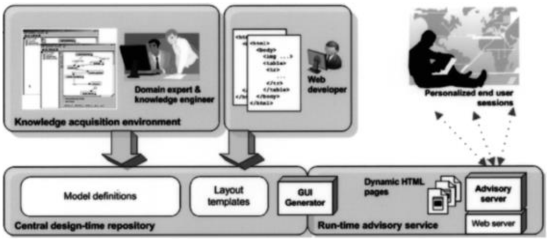

Domain expert & knowledge engineer
Knowledge acquisition environment
Web developer
Personalized end user sessions
Model definitions
Layout templates
GUI Generator
Central design-time repository
Dynamic HTML pages
Advisory server
Web server
Run-time advisory service

Figure 2 (Jannach *et al*., 2009: 145)

Figure 1. Architecture of decision support system (Loh *et al*., 2004: 159)

It is more than obvious that whether a potential tourist will be interested in a certain item depends on his preferences. Although may sound fragile, but the vast majority of today's tourists know exactly what they are looking for. Yet, they are very demanding and have complex, multi-layered desires and needs. Today's so called "postmodern tourists" have specific interests and individual motives which results in tailored made tourist products according to their particular preferences. They are often high experienced in travelling and demand perfect tourism products rather than standardized ones. Consequently, they take much more active role in producing diversified tourism products with shorter life cycles enabled by increased usage of ICT.

Many researchers were interested in identifying tourists' needs, expectations and behavior. Hence, numerous papers discuss tourist roles in order to define their considerable variations. In mostly, the behavior is related to specific demographic and background characteristics emphasizing the life course as the leading component for investigating tourist role preferences. Yet, attention should be paid to a variety of social structures and processes, including psychological needs and lifecourse stage.

3. Literature review

One may argue the inevitable relationship between tourists and information. Moreover, it is a widely-recognized fact that information and decision-making have become the foundation of world economy (Wang, 2008). Due to tourism essentiality, recommenders applied in tourism have been a field of study since the very beginnings of artificial intelligence. There is a large body of literature regarding the significance and effectiveness of applying the recommenders in tourism, travelling and hospitality. It is a matter of identifying a class of intelligent applications that offer recommendations to travelers, generally as a response to their queries. They mostly leverage in-built logical reasoning capability or algorithmic computational schemes to deliver their recommendation functionality. Thus, recommenders are an attempt to mathematically model and technically reproduce the process of recommendations in the real world.

Numerous researchers made efforts in their introducing. In this respect, the need for developing intelligent recommenders which can provide a list of items that fulfill as many requirements as possible is elaborated (Mirzadeh *et al.*, 2004; McSherry, 2005; Jannach, 2006). Also, a recommender dealing with a case-based reasoning is introduced in order to help tourist in defining a travel plan (Ricci & Werthner, 2002; Wallace *et al.*, 2003). Yet, as the most promising recommenders in tourism domain are the knowledge-based and conversational approaches (Ricci *et al.*, 2002; Thomson *et al.*, 2004). The knowledge-filtering, constraint-based and casebased approaches are further engaged for recommendation (Kazienko & Kolodziejski, 2006; Ricci & Missier, 2004; Zanker *et al.*, 2008). Additionally, the recommenders based on text mining techniques between travel agent and customer through a private Web chat may easily find an application (Loh *et al.*, 2004).

Furthermore, we refer to some late research that brought more sophisticated outcomes, like: introducing a personalized tourist information provider as a combination of an event-based system and a location-based service applied to a mobile environment (Hinze *et al.*, 2009); Investigation on sources and formats of online travel reviews and recommendations as a third-party opinions in assisting travelers in their decision making during trip planning (Zhang *et al.*, 2009); Findings regarding development of a web site in order to enable Internet users to locate their own preferred travel destinations according to their landscape preferences (Goossen *et al.*, 2009); Selecting the destination from a few exceptions (Niaraki & Kim, 2009; Charou *et al.*, 2010); Usage of orienteering problem and its extensions to model tourist trip planning problem (Vansteenwegen & Wouter, 2011); and similar. It is evidently that the research area is extending resulting in improved dependability of recommendations by certain semantic representation of social attributes of destinations (Daramola *et al*., 2010).

4. Necessity of developing tourism recommender in Macedonia

Macedonia identified tourism as a strategic priority for national economic development (Government of Macedonia, 2009). Up-to-date, tourism in Macedonia has accomplished an average growth of 4.64%, GDP share is 1.7% and it incorporates 3.1% of total workforce. Additionally, in the frames of services, tourism inflows are the second biggest item (just a little bit lower compared to the inflows of transport services), which is 1.3 times higher than the inflows of business services and 2.4 times larger than communication services inflows. Such condition indicates high potential to increase tourism effects in economic activity of Macedonia.

Furthermore, forecasts regarding tourism development in Macedonia are very optimistic. Namely, according to estimations by 2021 it is expected that direct contribution of tourism to GDP will reach to 1.6 % thus bringing revenue of €170 million according to constant 2011 prices; total contribution of tourism to GDP will rise to 6.0%; visitor exports will generate €76 million and investments in tourism will reach the level of €76 million representing 2.8% of total investments. Additionally, it is expected that number of employees that indirectly support tourism industry in Macedonia will rise to 35000 jobs representing 5.4% of total workforce (WTTC, 2011: 3)

With regards to international tourism demand in Macedonia, the upward trend is expected to continue in the next period (Petrevska, 2012). This optimistic view is supplemented additionally with the fact that the number of user ratings is permanently increasing by 15% monthly growth rate. Supportive and not surprising is another fact noting an upward trend of web portal users which complements the positive general conclusion referring tourism income in Macedonia. The average tourism consumption of €50 per day (WTTC, 2010) is anticipated to note an increase of one third of a euro, which may be misinterpreted as insignificant to national economy. However, on long-term horizon based on these projections the tourism contribution to the GDP may note an increase of more than 1%.

However, budget expenditures allocated for tourism promotion in Macedonia are very modest. Yet, the budget is constantly increasing yearly, from approximately €100000 in 2005, to €130000 in 2012 (Government of Macedonia, 2012). In the other hand, being ranked low on the list of the most attractive destinations for travel and tourism, illustrates the need for tourism improvement. Namely, Macedonia was ranked as 83rd out of 130 countries in 2008 (Blanke & Chiesa, 2009) with a slight improvement in 2011 being ranked at 76th place out of 139 countries (Blanke & Chiesa, 2011). It is worth noting that majority of countries in the region are significantly better ranked: Slovenia - 33rd place, Croatia - 34th place, Montenegro - 36th place, Bulgaria - 48th place and Albania - 71st place. From neighboring countries, only Serbia, and Bosnia and Herzegovina are ranked lower than Macedonia.

In order to strengthen tourism competitiveness of Macedonia, the first national web tourism portal (www.exploringmacedonia.com) was created in 2005 as a public-private partnership between an international donor and the Ministry of economy. In this regard, several other private initiatives act as additional tourism portals, thus supporting country’s tourism profile, like: www.go2macedonia.com, www.simplymacedonia.com, www.macedonia lovesyou.com, www.macedonia-timeless.com etc. Despite the existence of variety and most probably, sufficient number of web-portals that promote Macedonia as attractive tourist destination, so far none of them act as tourism recommender. Moreover, Table 1 supports the noted conclusion by giving a glance of poor visits to particular sites referred by search engines in a three-month period. Surprisingly, the both web-portals labeled as national are placed at the bottom of the table.

Table 1. Traffic statistics for selected web-sites

Web-site	Traffic rank
www.macedonialovesyou.com	18.824.372
www.simplymacedonia.com	14.670.989
www.go2macedonia.com	14.010.522
www.macedonia-timeless.com	1.690.753
www.exploringmacedonia.com	1.360.389

Source: Authors’ note based on www.alexa.com

The forth mentioned advantages produced by recommenders fully justify the urgency and necessity of their design in Macedonia. Specifically lead from the fact that they assist tourists and visitors in planning and creating their trip and holiday in more sophisticated way.

5. Conclusion

Based on fact that tourism is defined as one of the most economically-oriented industries in the world, it enhances and strengthens national economies. With regards to Macedonia, tourism is identified as an industry which might contribute to: enhancing foreign export demand for domestic goods and services, generating foreign currency earnings, new employment opportunities within the country, repaying the foreign debt, increasing the national income etc. Additionally, it is worth noticing that travel and tourism economy in each country incorporates broad spectrum of tourism-oriented activities and results with multiplicative impacts.

The paper presented an analytical approach of positive results in developing tourism recommendation systems, thus emphasizing the necessity for their introduction in Macedonia. Tourism recommenders may serve as a guideline for tourists and travelers in the line of identifying ideal trip and holiday. So, development of such software module may generally contribute to increasing the awareness of tourist destination that is capable of fulfilling travelers' preferences, and respectfully in raising net tourism income.

Furthermore, a successful launch of a web-based recommender at national level is in the line of supporting the economy through improvement of tourism supply in more qualitative manner. Since such portal will indicate the motives, preferences and reasons for traveling to Macedonia, it might be of high importance to all key-tourism actors in the process of identifying measures and implementing activities necessary for creating comprehensive tourism policy. Finally, the paper may alarm the relevant tourism-actors in Macedonia, that the time has changed and that on-line experience has shifted from searching and consuming to creating, connecting and exchanging.

References

Blanke, J. & Chiesa, T. (2009). *The Travel & Tourism Competitiveness Report 2009: Managing in a Time of Turbulence.* Geneva: World Economic Forum.

Blanke, J. & Chiesa, T. (2011). *The Travel & Tourism Competitiveness Report 2011: Beyond the Downturn.* Geneva: World Economic Forum.

Charou, E., Kabassi, K., Martinis, A. and Stefouli, M. (2010). Integrating multimedia GIS technologies in a recommendation system for geo-tourism. In: Tsihrintzis G A and Jain L C (eds.). Multimedia Services in Intelligent Environment 2010. Springen-Verlag Berlin, 63-74.

Daramola, O. J., Adigun, M. O., Ayo, C. K. and Olugbara, O. O. (2010). Improving the dependability of destination recommendations using information on social aspects. *Tourismos: an International Multidisciplinary Journal of Tourism*, 5(1), 13-34.

Goossen, M., Meeuwsen, H., Franke, J. and Kuyper, M. (2009). My Ideal Tourism Destination: Personalized Destination Recommendation System Combining Individual Preferences and GIS Data. *Journal of Information Technology & Tourism*, 11(1), 17-30.

Government of the Republic of Macedonia (2009). National Strategy on Tourism Development 2009-2013, Skopje.

Government of the Republic of Macedonia, Ministry of Economy. (2012). *Program for Tourism Promotion and Support for 2012,* Skopje.

Hinze, A., Voisard, A. and Buchanan, G. (2009). TIP: Personalizing Information Delivery in a Tourist Information System. *Journal of Information Technology & Tourism*, 11(3), 247-264.

Jannach, D. (2006). Finding preferred query relaxations in content-based recommenders. IEEE Intelligent Systems Conference, Westminster, UK, 355-360.

Jannach, D., Zanker, M. and Fuchs, M. (2009). Constraint-based recommendation in tourism: a multi-perspective case study. *Information Technology and Tourism*, 11, 139-155.

Niaraki, A. S. and Kim, K. (2009). Ontology based personalized route planning system using a multicriteria decision making approach. *Expert Systems with Applications,* 36, 2250-2259.

Kazienko, P. and Kolodziejski, P. (2006). Personalized Integration Recommendation Methods for E-commerce. *International Journal of Computer & Applications*, 3(3), 12-26.

Loh, S., Lorenzi, F., Saldaña, R. and Licthnow, D. (2004). A Tourism Recommender System Based on Collaboration and Text Analysis. *Information Technology & Tourism*, 6, 157-165.

Mirzadeh, N., Ricci, F. and Bansal, M. (2004). Supporting user query relaxation in a recommender system. 5th International Conference on E-Commerce and Web Technologies, Zaragoza, Spain, 31-40.

McSherry, D. (2005). Retrieval failure and recovery in recommender systems. *Artificial Intelligence Review*, 24, 319-338.

Petrevska, B. (2012). Forecasting International Tourism Demand: the Evidence of Macedonia, *UTMS Journal of Economics,* 3(1), 45-55.

Ricci, F. and Del Missier, F. (2004). Supporting Travel Decision Making through Personalized Recommendation. In: Clare-Marie K, Jan B and John K (eds.), Designing Personalized User Experiences for e-Commerce, 2004, Kluwer Academic Publisher, 221-251.

Ricci, F. and Werthner, H. (2002). Case base querying for travel planning recommendation. *Information Technology & Tourism*, 4(3/4): 215-226.

Ricci, F., Arslan, B., Mirzadeh, N. and Venturini, A. (2002). ITR: A case-based travel advisory system. 6th European Conference on Advances in Case-Based Reasoning, 613-627.

Thompson, C., Göker, M. and Langley, P. (2004). A personalized system for conversational recommendations. *Journal of Artificial Intelligence Research*, 21, 393-428.

UNWTO (2012). *Annual Report 2011*, WTO, Madrid.

Vansteenwegen, P. and Wouter, S. (2001). Trip Planning Functionalities: State of the Art and Future. *Information Technology & Tourism*, 12(4), 305-315.

Wallace, M., Maglogiannis, I., Karpouzis, K., Kormentzas, G. and Kollias, S. (2003). Intelligent one stop-shop travel recommendations using an adaptive neural network and clustering of history. *Information Technology & Tourism,* 6, 181-193.

Wang, J. (2008). Improving decision-making practices through information filtering. *International Journal of Information and Decision Sciences*, 1(1), 1-4.

WTTC (2011). Travel & Tourism Economic Impact - Macedonia 2011.

WTTC (2010). Travel & Tourism Economic Impact - Macedonia 2010.

Zanker, M., Fuchs, M., Höpken, W., Tuta, M. and Müller, N. (2008). Evaluating Recommender Systems in Tourism - A Case Study from Austria. In: P. O'Connor (ed). Information and Communication Technologies in Tourism, Proceedings ENTER 2008, Springer, 24-34.

Zhang, L., Pan, B., Smith, W. and Li, X. (2009). Travelers’ Use of Online Reviews and Recommendations: A Qualitative Study. *Journal of Information Technology & Tourism,* 11(2), 157-167.

CLOUD COMPUTING APPLICATION FOR WATER RESOURCES MODELING AND OPTIMIZATION

Blagoj Delipetrev[1]

[1]Faculty of Computer Science, University "Goce Delcev" 2000 Shtip, Republic of Macedonia, blagoj.delipetrev@ugd.edu.mk

Abstract: Modeling and optimization of water resources is complex multidisciplinary collaborative task suitable for development of a cloud computing application. The presented application for water resources modeling and optimization is built on three latest advancements in computer science and technology: Cloud Computing, Service Oriented Architecture and web Geographic Information Systems. The cloud computing application have three tiers: (1) database tier capable of storing all relevant data and information (including geospatial information) (2) middle tier that support multiple data sources and provide platform for building specialized web services and (3) web services tier. The web service tier contains three web services (1) for geospatial data management, (2) for water resources modeling and (3) water resources optimization. The cloud computing application for water resource modeling and optimization advantages over previous solutions are: accessible from everywhere, available all the time, scalable, interoperable, distributed and ultimate collaboration platform. The application web address is www.delipetrov.com/his/.

Keywords: Cloud computing, GIS, modeling, optimization, water resources.

8 Introduction

Water is one of the most valuable human resources. Population growth, higher livings standards, industry, power production, food production are the main factors for continuous increase of water demand. These factors together with climate change put additional pressure on water managers demanding efficient and optimal distribution of water resources between all users and functions. New tools and methods are needed for development of integrated water management systems. These water management systems will include stakeholders, users and functions into one integrated platform addressing technical, economical, social and ecological aspects.

Water managers nowadays use sophisticated decision support systems for integrated water management. Core component of these systems is water resources modeling and optimization. Water resources modeling and optimization is usually performed by computer models of the real world. In the last decade advances in ICT (Information and Communication Technologies) significantly improved water resources modeling and optimization leading to improved management of engineering, economic, social, ecological, hydrological and institutional aspects of complex multifunctional water systems. These contribute to improved design, implementation, management and knowledge of the water systems.

Existing water modeling systems are usually available as stand-alone applications, frequently relying on GIS (Geographic Information Systems) that provide the framework for management and integration of all geo-spatial data [1]. Recent advances demonstrate transition to web-based applications, using similar GIS frameworks [2]. There are successful examples of open source water modelling solutions [3], while other solutions are combination of open source and commercial software components, creating web services for distributed and interoperable hydro information system [4].

The main objective in the presented research is to create cloud computing application for water resources modelling and optimization that is internet based and only a web browser is required to use it. The cloud application is conceived to contain all necessary data and information concerning water resources and to provide a platform for development of specialized web services. Additional application objectives are: (1) available from everywhere, (2) accessible all the time, (3) flexible for adding additional web services and components, (4) interoperable, (5) designed to operate in distributed computer environment, (6) based on open source software and (7) can be simultaneously used by multiple users that are geographically dispersed, therefore enabling web-based collaborative environment.

The presented cloud computing application for water resources modeling and optimization satisfies all previously specified objectives. This application is one of the most feasible solutions for future development of integrated water modeling systems where all data, services and processing are carried out on one common platform enabling integrated management of the physical system in question that addresses various economic, social, ecological and other objectives. The cloud application presented here have three web services:

1. Web service for geospatial data management.
2. Web service for water resources modeling.
3. Web service for water resources optimization.

The cloud application is developed using several programming languages (JavaScript, AJAX, PhP), additional applications (GeoServer, PostgreSQL, PosgGIS), libraries (OpenLayers), geospatial standards protocols (WMS, WFS, WFS-T) and others additional components. All components and software packages used in the application development are open source. The system design and components allow easy upgrade, interoperability, distribution and scalability.

The cloud application for water resources modeling is designed to work in private cloud architecture e.g. its compliance isn't tested on any current cloud provider. Main idea in cloud computing is to use the service without knowing (or caring) about the infrastructure being what this application does.

9 Main concept and technologies

The three main concepts and technologies for the development of cloud application for water resources modelling and optimization are: (1) Cloud Computing, (2) Service Oriented Architecture (SOA), (3) web GIS.

Cloud computing is the latest ICT trend. The core concept of cloud computing is “only a web browser is needed” while everything else is in the cloud. Data, models and software reside in the cloud and are available “on demand” anytime and everywhere. Only internet connection and browser is needed to use the system. This concept is analogous to the electricity grid where we just plug in our devices and use them without understanding the infrastructure behind. Cloud computing [5] also creates new possibilities and advantages for companies and users. This is demonstrated by the fact that the largest IT companies like Apple, Google, Facebook, Microsoft, and Amazon are heavily investing in their cloud computing facilities.

Service Oriented Architecture (SOA) [6] defines a group of rules for design, development, integration and implementation of information systems. The key idea behind SOA is how to integrate and connect various information system components. SOA define components interfaces and communications protocols using messages in XML (eXtensible Markup Language) format. SOA enables previously developed components and applications, various programming languages and different platforms to be joined into one integral solution.

Third and crucial concept used in this application is web GIS. GIS provides integration framework for modelling in any domain with geospatial information (water, climate, population, etc.). Almost all water resources information's are geospatial in nature. Latest standards and tools of Web GIS allow development of fully distributed web applications, making the Internet as the new medium for using these systems [7]. The presented cloud application is successful demonstration of the latest web GIS technologies and standards.

10 Architecture of the cloud application

The cloud application architecture is based on SOA and presented on Figure 1. The arrows in this figure represent communication between the different web services, as they have been introduced earlier. The three different web services, together with the technologies and components used for their implementation are explained in the following sections.

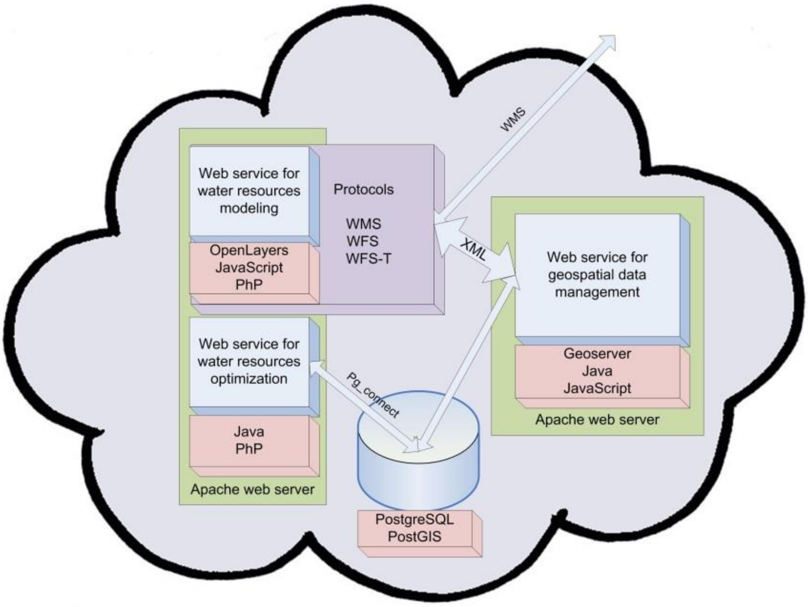


Figure 1 Architecture of the cloud application for water resources modeling and optimization

3.1 Web service for geospatial data management

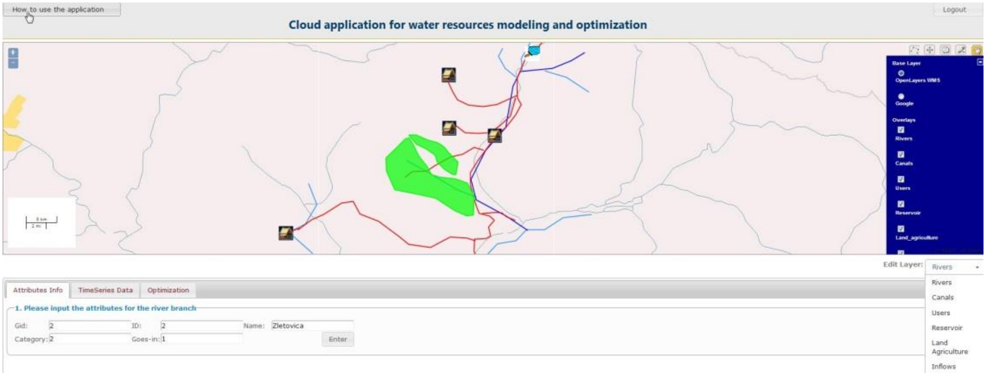
The web service for geospatial data management is composed of two main components: web application GeoServer and relational database HMak created in PostgreSQL and PostGIS. The relational database HMak stores relevant water resources related data (river network, canals, towns, cities, irrigation fields, etc.) as well as data for the web service for water resources modeling and the web service for water resources optimization.

GeoServer is a middle component that can connect to mutiple data sources and provide data to other components using Open Geospatial Consortium (OGC) standard protocols (WMS, WFS, WFS-T). GeoServer abstracts data sources and provides data access platform for various web services. In the current implementation, the web service for water resources modelling is connected to GeoServer using WFS-T protocol. WFS-T protocol is based of XML messages and operate asynchronous or “on demand”.

3.2 Web service for water resources modeling

The web service for water resources modeling is created using OpenLayers library and prototype code of the programing languages JavaScript, AJAX and PhP. The web service geospatial capabilities are enabled by OpenLayers library that support OGC standards (WMS, WFS, WFS-T, etc.). The web service gives possibility to draw, edit, delete or modify vector geospatial data online. In the current implementation, the web service is connected over WMS to Google map servers and Open map servers and uses these layers as background maps. The web service through WFS-T connects to the GeoServer and indirectly with the HMak database. HMak database stores six geospatial vector layers: rivers, canals, users, reservoirs, inflow and agricultural areas. For each layer attribute tables are defined and stored, together with the geospatial data, same as in GIS. The web service provides a toolbar for operations with geospatial objects from the six vector layers and creating the water resources model shown on figure 2. Moreover, the web service provides the interface to enter attributes data to the objects. When a geospatial objects is selected, JavaScript code is activated that reads attributes data from HMak and fills the data under the tab “Attribute Info”. Users can change this data and store it back to HMak. In the current demonstrator implementation attribute data is still relatively simple but the possibilities for extending every object with additional information are possible.

An example model representation using the web service was developed, by entering rivers, canals, reservoir, users, and agriculture areas, as shown on figure 2. Together with the geospatial data, sample attribute data was provided for every object.



Cloud application for water resources modeling and optimization

1. Please input the attributes for the river branch

Gid: 2 ID: 2 Name: Zletovica
Category: 2 Goes-in: 1

Edit Layer: Rivers

Figure 2 River basin model created with the service for WRM

3.3 Web service for water resources optimization

The web service for water resources optimization is composed of the prototype Dynamic Programming (DP) application developed in Java and the appropriate web interface. This application is based on the dynamic programming algorithm provided in [8] for calculating optimal reservoir operation that simultaneously satisfies the objectives for flood control, downstream water demand and recreation on the lake reservoir. The application works with 5 input tables: reservoir inflow, total demand, upper flood limit, lower recreation limit and reservoir discretization shown in table 1. Timestep is denoted with TS in table 1. The weight factors in tables Demand, Flood and Recreation describe the relative importance of satisfying the three objectives.

Table 2 Input tables of the web service for water resources optimization

Inflow	Demand	Flood	Recreation	Reservoir Discretization
Integer:TS Double: Inflow	Integer:TS Double: Demand	Integer:TS Double:Flood Double:Weight	Integer:TS Double:Recreation Double:Weight	Double:Discretization

The web service has web interface for entering data, performing basic data quality checks and uploading of the data into HMak database. The execution starts the dynamic programming (DP) algorithm, which uses the uploaded data and provides the results on a separate web page. Application result is optimal reservoir operation in terms of reservoir releases.

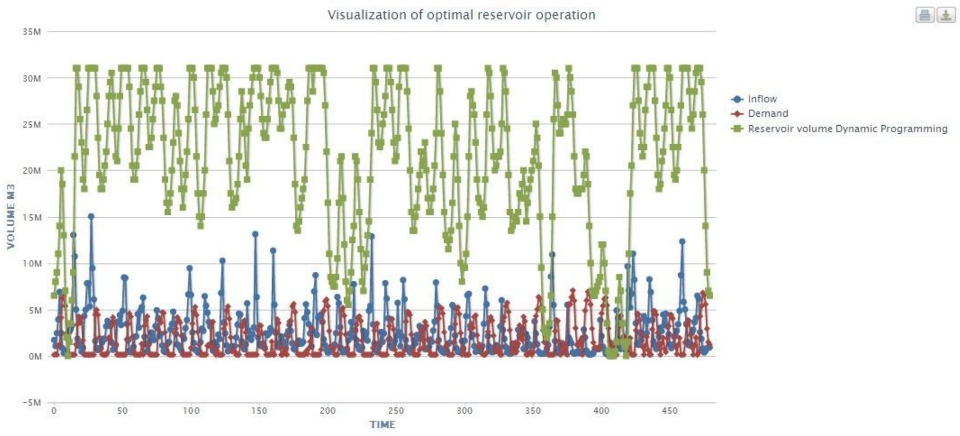


Figure 3 Visualization of optimal reservoir operation

This service is started by selecting a reservoir object from the main working window. The execution of the application loads the data from HMak, runs the DP algorithm and provides the results. Such results are shown on figure 3 where reservoir inflow, total demand and optimal reservoir operation curve are plotted together. The idea of including this service is not to present state of the art optimization algorithm or hard mathematical background which can be found in [8], but instead to demonstrate that cloud computing platform can facilitate different programming languages and components.

4. Discussion

The development of the application demonstrates the possibilities of ICT for creation of integrated cloud solution for water resources modelling and optimization. The main goal of using only web browser for operating the application is accomplished. The presented cloud application is web based, accessible and available all the time and from everywhere. The current implementation of the system is on one physical server with one relational database HMak, one GeoServer instance, and two apache web servers on which three services are working. The system components and technologies provide seamless scalability, interoperability and can work in distributed environment. GeoServer can connect to several distributed relational database and other types of data sources. The source code of the cloud application can connect to more instances of GeoServer, which can be distributed on many physical servers. This demonstrates the power of the presented solution to work in heterogeneous server environments and the opportunity to adjust hardware and software resources based on the workload. The cloud application SOA increases the flexibility to add additional web services or upgrading the existing ones. The service for optimizing water resources demonstrates how different applications (using different programing languages) can be connected to the existing services and integrated into cloud application.

The current cloud application is open to everyone, and anyone with internet connection can use the web services. Geographically dispersed users using only a web browser can jointly model the water system, draw rivers, enter attributes, run optimization and view results. This is the ultimate collaborative environment that provides same interface, data and users working windows. Each user action is processed by the cloud application and presented immediately in the web service where all other users can see it. Example for this is if one user is entering (drawing) rivers other can enter canals and with each refresh of the web browser can actually monitor the overall progress and jointly develop the water model. All services, data and modes are accessible to users at every time and everywhere. Additionally, future cloud application development can create different working environments for different user categories, such as decision makers, water managers and the general public. These working environments would be based on different services, capabilities and data access. Important advantage of the presented solution is that all services will be based on one common platform.

There are several possibilities for upgrading and improvement of the existing services. The service for water resources modelling can be upgraded with adding new layers and creation of quality attributes tables. The most important part is development of a computational framework that will create an intelligent system, connect different objects and define dependencies between them. Example for this is when a river enters a reservoir the river discharge to be added to the reservoir storage and update the reservoir level. These extensions can lead to the development of a full-fledged water resources modelling system as a cloud application. The service for water resources optimization can be improved by including additional algorithms based on other optimization techniques (reinforcement learning, stochastic dynamic programming etc.) or by improving the existing one with adding additional input information.

5. Conclusion

The shifting of desktop applications, information, and processing power to the cloud has started. Future applications, software and services will be increasingly cloud oriented. The developed cloud application for water resources modelling and optimization is a pioneer in future integrated water management application. The software components and the web services presented in the article demonstrate that there are software and technologies to develop a robust and complex cloud application. Important to notice is that cloud application is build using open source system components and prototype code. Advantages of the presented application are its availability, accessibility, flexibility, scalability, interoperability included in the design and software components. Further development of the application can also include various water related data, population growth, urbanization, climate variations, etc., as they are needed for analysing and solving particular water resources management problems. The platform for development of such applications is already created and future applications will be additional services or modules of the existing cloud application.

References

1. B. Delipetrev, D. Mihajlov, M. Delipetrev and T. Delipetrov (2010): *Model of the Hydro-Information System of the Republic of Macedonia*, Journal of Computing and Information Technology, 18(2), 201-204.
2. M. Rao, G. Fan, J. Thomas, G. Cherian, V. Chudiwale and M. Awawdeh (2007): *A web-based GIS Decision Support System for managing and planning USDA's Conservation Reserve Program (CRP).* Environmental Modelling & Software*,* Vol. 22, No. 9, pp. 1270-1280.
3. J. Y. Choi, B. A. Engel and R. L.Farnsworth (2005): *Web-based GIS and spatial decision support system for watershed management*. Journal of Hydroinformatics, Vol. 7, No. 3, pp. 165-174.
4. J. Horak, A. Orlik and J. Stromsky (2008): *Web services for distributed and interoperable hydro-information systems.* Hydrology and Earth System Sciences, Vol. 12, No. 2, pp. 635-644.
5. M. Armburst, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin and I. Stoica (2009): *Above the clouds: A berkeley view of cloud computing.* EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28.
6. T. Erl (2005): *Service-oriented architecture: concepts, technology, and design*, Prentice Hall PTR.
7. M.G. Tait (2005): *Implementing geoportals: applications of distributed GIS,* Computers, Environment and Urban Systems, Vol. 29, No. 1, pp. 33-47.
8. D.P. Loucks and E. Van Beek (2005): *Water Resources Systems Planning and Management: An Introduction to Methods, Models and Applications*. Paris: UNESCO.

IMPROVING THE SECURITY OF CLOUD-BASED ERP SYSTEMS

Gjorgji Gicev[1], Ivana Atanasova[2] and Jovan Pehcevski[3]

[1]*Artisoft, Skopje, Macedonia, george.gicev@artisoft.net*
[2]*Artisoft, Skopje, Macedonia, ivana.atanasova@artisoft.net*
[3]*Faculty of Informatics, EURM, Skopje, Macedonia, jovan.pehcevski@eurm.edu.mk*

Abstract: Enterprise resource planning (ERP) systems integrate internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, customer relationship management, etc. ERP systems automate this activity with an integrated software application.The architecture of the software facilitates transparent integration of modules, providing consistent flow of information between all functions within the enterprise. ERP popularity has rapidly increased in the last few years and they are starting to be used by all types of businesses. In this regard, the ERP is becoming a system with high vulnerability and confidentiality in which security is critical for the system to operate. Recent studies show that many ERP vendors have already integrated some kind of security solutions, which may work well internally. However, in an open environment, one needs more advanced and innovative technological approaches to secure an ERP system.

In this paper, we evaluate how and to what extent one can improve the security of an ERP system by implementing a set of security measures addressing the current top security threats. The paper evaluates the effects and provides conclusions on the applied security measures using ArtAIIS – Artisoft’s cloud-based, web-enabled software-as-a-service ERP system.

Keywords: Security measures, cloud ERP, web security, security framework.

11 Introduction

Information technology has been making huge impact on the civilization especially in the last two decades. Tremendous achievements in the micro technology made computers extremely fast and cheap, which triggered rapid development in all segments of everyday life. World Wide Web Technology combined with affordable workstations and fast networks caused explosion of networked people, institutions and businesses. As never before, we are witnessing a true globalization of the world in all segments. We do not have information flow anymore. Information is everywhere instantly from the moment it originates. But as always, good things also come with drawbacks. Leaving everything on the net allows for someone to harm or take opportunity to hack, steal or destroy the information or the system. Accordingly, we continually build security blocks, measures, procedures, and protocols in order to defend our systems from external and also internal attacks.
Today, we can say that Internet addiction leads humanity to a level where a small break in any of these services is having serious impact on our daily work as would for example electricity brake down. Civilization is networked as never before. We became de facto global village. But this networking is bringing huge possibilities for everybody, including those who want to harm the positive trends. The bigger the network is, the bigger the threat is, and the bigger the security vulnerability is. This is why implementation of security measures on application software, in our case web application software is an interesting area and topic for discussion.

Recent studies show huge, even extremely, increased number of users of Internet services. According to Internet World Stats, on December 31 2011, the number of Internet users was over 2 billion

.

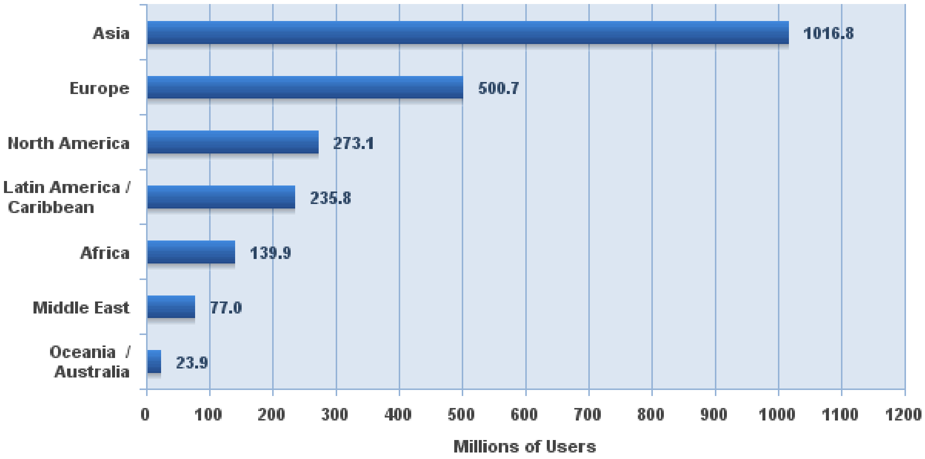


Fig.1.1 Analysis of the number of Internet users (web sites and web applications) according to Internet World Stats, 2011

Because of the technology globalization, ERP systems have started to appear as a necessity not solely for large companies but also for small and medium businesses [1]. This sent ERP system utilization to the sky. However, according to Dhilloni [2], information security in the ERP solutions has traditionally been an afterthought. Because of businesses' increased dependence on information, security is being considered proactively. On the other hand, the process of security implementation in ERP system is a long and everlasting process. The great popularity of integrated ERP system solutions, today more than ever, lead to the need of a solid security framework in order to set the base minimum when it comes to ERP security. This framework should only be used as a starting point in the process of securing and fortifying an existing ERP system.

In this paper we evaluate how and to what extent one can improve the security of an ERP system by implementing a set of security measures addressing the top current web application threats in the world.

12 Existing security frameworks to ERP systems

Security in ERP solutions requires grasping a wider approach and concept where security measures will involve people, network, host and application security [6]. In this regard, we have analyzed existing security frameworks which include all aspects of security in an ERP system.

We note, however, that both, the Security framework for an ERP system [4] and the Security framework for ERP in cloud [3] have not gone into much detail as far as the technology component is concerned.

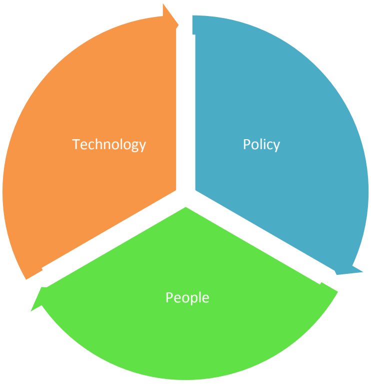


Fig. 2.1 Components of the Security framework for ERP system[1]

According to Marnewick [4], the weakest link in an ERP system is still its users, as open gateways to the information stored and obtained through the system. User behavior is still unpredictable and it represents an issue that must be addressed in the stages before starting to use the ERP system. The most important stages are:

- Policies and procedures – for explicit control and management of user behavior;
- Risk analysis – to increase the level of security to the assets of greatest value to the business; and
- Awareness – users need to become aware of the security threats and risks of their behavior.

The technology component also involves the following elements [4]:

- Identification & Authentication – ensuring that the system is accessed by legitimate, authorized users;
- Authorization – restriction of the access rights and actions of the user in the system;
- Confidentiality – only authorized users can see and use specific data;
- Integrity – only authorized users can modify specific data;
- Non – repudiation - a transaction which took place must have a continuity information in the system in order to undoubtedly prove its existence and the user who initiated it;
- Availability – the system must be available 24/7 for business continuity; and
- Auditing –requires a risk-based systems review supported by detailed checklists and practical experience in designing controls.

13 Improving the cloud-based ERP security

The main goal of this paper is to contribute to the technology component of the existing security frameworks to ERP systems. In this section, we propose, implement and evaluate a set of security measures for an ERP system in the cloud [3]. We use the ArtAIIS ERP system – a product of the company Artisoft - which is web-enabled and offered as a service (SaaS) on a cloud platform.

3.1 Security threats

When considering the technology component of the system, it is necessary to include and analyze different types of threats and attacks which are current and recurrent.
According to the list of Top 10 threats of web application software OWASP [5], the number one threat is the *SQL Injection attack*, immediately followed by the *XSS attack*. In this paper, we focus only on the top 5 threats of web application software, as from our experience these are identified as the most occurring threats in the ERP industry. They are described as follows.

1. *XSS scripting* - represents a type of injection problem, where harmful script is inserted into seemingly reliable website. XSS attack occurs when an attacker uses a web application to send malicious code, usually in the form of a browser - script to another user of the application.
2. *SQL injection* - SQL injection attack exploits weaknesses in the validation of input parameters in the web application to execute commands and activities in the database.
3. *Cookie replay* - takes user authentication cookie through software to monitor traffic and performs its replay for obtaining access to the application under a false identity.
4. *Session replay* - With special software to scan and monitor network traffic, the attacker can intercept the user’s session token and it can be used to pass authentication.
5. *Cookie, query and form field manipulation* - Attacker can easily perform manipulation and modification of the query string parameters that are passed via HTTP GET from the client to the server as they are visible in the URL. There are numerous tools that allow the attacker to modify a cookie that is stored in memory. This type of attack is performed in order to gain access to a particular application or web site. Values of HTML form fields are sent in clear format via HTTP POST Protocol. This applies to

visible and hidden form fields. These fields can be modified very easily and they can skip the validation procedures.

3.2 Security measures

The proposed security measures we consider [7, 8, 9] are shown in Table 1.

Table1. Proposed security measures for extending the technology component of an existing security framework for ERP system [7, 8, 9].

Threat	Measures
XSS Scripting	• Full validation of user input parameters.The application must verify that the input query strings, form fields, and cookies are valid for the application. The approach that works here is to treat all input parameters as harmful. • Usage of HTMLEncode() or URLEncode() functions. In this way, the code that performs harmful scripts is transformed into harmless HTML.
SQL Injection	• Full validation of user input parameters.The application must verify that the input query strings, form fields, and cookies are valid for the application. The approach that works here is to treat all input parameters as harmful. • Procedure and query parameterization. Provides the value of parameters that are not treated as executive code. In this way, the incoming user parameters cannot contain other types of data than those defined for the type parameter. • Least privilege rule. To access the database to be used user orders with minimal privileges to perform the required actions on the data.
Cookie replay	• SSL. Use SSL encrypted communication channel each time when an authentication cookie is transmitted. • Cookie timeout. Use cookie timeout value to force re-authentication after expiration of the specified time interval. This measure does not

	prevent replay attacks but shortens the time frame in which such an attack can be carried out.
Session replay	• Re-authentication. Re-authentication before performing a critical operation is sufficient protection from this attack. • Session timeout. Session expiration process should be fully respected, including all cookies and tokens. • Remember me. Creating the option "Remember me" in order to allow the user not to store any information for the client session on his computer.
Cookie manipulation	• Cookie encryption or protection using HMAC
Query manipulation	• Session identifier. Use a session identifier to identify the client and keep the session data in the server state warehouse. • HTTP POST. Select HTTP POST instead of GET for submission of forms • Encryption. Encryption of query string parameters
Form field manipulation	• Session identifier. Instead of using hidden fields, those values should be stored in session identifiers that are safely protected in the server’s state warehouse.

3.3 Experimental methodology

The validity of the proposed security measures, described in subsection 3.2, was evaluated in two phases:

- Phase I - the ERP solution is tested in the current state to detect existing weaknesses and vulnerabilities; and
- Phase II - the ERP solution is tested with the same security tools for vulnerabilities after the proposed security measures have been applied.

The analysis is made using the following security tools:

- NetSparker – powerful scanner of vulnerabilities of web applications, which performs crawling, attacks and detection of vulnerabilities, regardless of platform or operating system. NetSparker is the only tool that allows false-positive testing with a built-in exploitation engine which confirms the detected weaknesses.

- Acunetix- web application auto scanner more like a black-box tool. Acunetix provides full scanner, crawler and search reports, as well as huge database security checks for all server platforms

- WebCruiser –effective and powerful tool that allows detailed analysis of websites and web applications. The tool offers a weakness scanner as well as numerous safety tests. WebCruiser is an automated SQL Injection, XPath Injection and XSS tool. In our paper Web Cruiser is used only for testing high level threats

According to the level of threat, the application tools detected weaknesses into three categories: High, Medium and Low level threat.

The ERP solution was evaluated in its current state, as offered on the SaaS platform of Artisoft. No additional protection measures existed aside from the initial security measures implemented when the solution was built.

3.4 Results and discussion

In Phase I the following top 3 results were obtained (shown in Table 2).

Table2. Top 3 detected weaknesses and threats by the security tools used to scan ArtAIIS ERP system in its current state

Application	**Weaknesses**
NetSparker	High: password is transmitted in its original form via HTTP Medium: autocomplete is enabled for sensitive data Medium: cookie not marked as HttpOnly
Acunetix	Medium: server admin page publicly available

WebCruiser	Medium: cookie not marked as HttpOnly Medium: unprotected username and password transmission High: six POST SQL INJECTION attacks and one XPath INJECTION.

The security measures from Table 1 were applied to the ERP solution ArtAIIS. Phase II consisted of reassessment of the ERP solution again after applying the security measures from Table 1. The summarized results are shown in Fig. 3.1

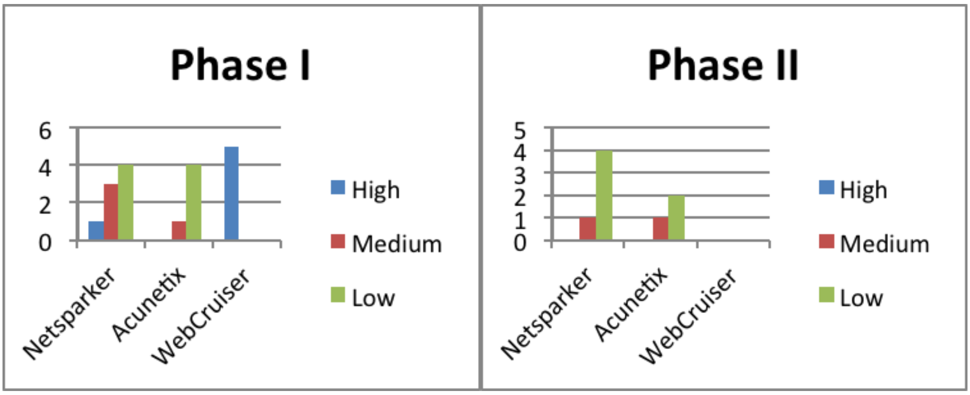


Fig. 3.1 Results from phase I and phase II analyses

5 Conclusions and future work

Results of our analysis show that, when even a small set of standard security measures are applied to a sample ERP software solution, one can greatly contribute to the security of the system. The results demonstrate that after the implementation of the set of security measures (shown in Table 1) the security scanner applications did not detect any high level threats and decreased the number of medium level threats. This substantially improved the overall security of the ERP system.

However, we must note that there is no recipe to complete security when it comes to ERP systems. The weakest element is still the people component where no security measures can guarantee the confidentiality level of the people of the company, regardless of the awareness and procedures that are put in place. As mentioned previously, security is an ongoing process where the security measures have to be tuned every time the system is updated. What matters even more, of course, is the price/performance ratio, meaning that security measures will always try to first comply with a higher performance ratio and then to advantage the security of the system.

In the future, this small set of security measures could be extended and reevaluated with different security scanner applications to confirm the effectiveness of the same in the ERP system architecture. There always should be balance between the price/performance ratio and the security level applied to the ERP system, since usability is directly connected to the performance of the system. In this way one would define a baseline set of security measures which will successfully increase the security of the ERP system while maintaining at the same time a satisfying level of performance. Nevertheless, critical and sensitive modules should always get a security base line measures applied regardless of the effect they have on the system performance, as data security and protection is the foundation of today's ERP web-based systems.

References

Book chapter:

[1] M. A. Rashid, L. Hossain and J. D. Patrick (2002): *Evolution of ERP Systems: A Historical Perspective, Chapter 01,* DOI: 10.4018/978-1-931777-06-3.ch001, IGI Global

Journal papers:

[2] G. Dhillion (2004): Guest Editorial: the challenge of managing information security. International Journal of Information Management. Volume 24. pp 3 – 4

[3] G. Fathima Haseen Raihana (2012): Cloud- ERP: A Solution model. IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No. 1

Proceedings:

[4] C. Marnewick and L. Labuschagne, (2006): *A Security framework for ERP Systems*, Academy for Information Technology, University of Johannesburg.

Web pages:

[5] OWASP, (2010): *The ten most critical Web application security risks (Top 10)*. The Open Web Application Security Project. Accessed on 18.04.2012

[6] C. Herberger – SCMagazine (2010): *Defense in depth: building a holistic security infrastructure,* Accessed on: Februray 2012, (http://www.scmagazine.com/defense-in-depth-building-a-holistic-security-infrastructure/article/190025/

[7] Microsoft (2005): *Prevent Cross-site scripting in ASP.NET,* Accessed on: February 2012. http://msdn.microsoft.com/en-us/library/ff649310.aspx

[8] Microsoft (2005): *Protect from SQL Injection in ASP.NET*, Accessed on: February 2012. http://msdn.microsoft.com/en-us/library/ms998271.aspx

[9] C-SharpCorner (2004): *How to secure your Web Applications*, Accessed on: February 2012. http://www.c-sharpcorner.com/UploadFile/krishvr/securewebapp11262005011914AM/securewebapp.aspx

USING OF THE MOORE-PENROSE INVERSE MATRIX IN IMAGE RESTORATION

Igor Stojanovic[1,*], Predrag Stanimirovic [2], Marko Miladinovic [2]

[1] Faculty of Computer Science, Goce Delcev University – Stip, igor.stojanovik@ugd.edu.mk
[2] Faculty of Sciences and Mathematics, University of Nis, Serbia, pecko@pmf.ni.ac.rs, markomiladinovic@gmail.com
** Igor Stojanovic, e-mail: igor.stojanovik@ugd.edu.mk*

Abstract: A method for digital image restoration, based on the Moore-Penrose inverse matrix, has many practical applications. We apply the method to remove blur in an image caused by uniform linear motion. This method assumes that linear motion corresponds to an integral number of pixels. Compared to other classical methods, this method attains higher values of the Improvement in Signal to Noise Ratio (ISNR) parameter and of the Peak Signal-to-Noise Ratio (PSNR), but a lower value of the Mean Square Error (MSE). We give an implementation in the MATLAB programming package.

Keywords: deblurring, image restoration, matrix equation, Moore-Penrose inverse matrix.

14 Introduction

Recording and presenting helpful information is the purpose of producing images. Yet, the recorded image is a degraded form of the initial scene as a result of flaws in the imaging and capturing process. Images are rather unclear in numerous applications such as satellite imaging, medical imaging, astronomical imaging or poor-quality family portraits. It is vital to many of the subsequent image processing tasks to neutralize these flaws. One should consider an extensive variety of different degradations for example blur, noise, geometrical degradations, illumination and color imperfections [1-3]. Blurring is a form of bandwidth reduction of an ideal image owing to the imperfect image formation process. It can be caused by relative motion between the camera and the original scene, or by an optical system that is out of focus. When aerial photographs are produced for remote sensing purposes, blurs are introduced by atmospheric turbulence, aberrations in the optical system, and relative motion between the camera and the ground. The field of image restoration is concerned with the reconstruction or estimation of the uncorrupted image from a blurred one. Essentially, it tries to perform an operation on the image that is the inverse of the imperfections in the image formation system. In the use of image restoration methods, the characteristics of the degrading system are assumed to be known a priori [4].

The method, based on Moore-Penrose inverse matrix, is applied for the removal of blur in an image caused by uniform linear motion. This method assumes that linear motion corresponds to an integral number of pixels. For comparison, we used two commonly used filters from the collection of least-squares filters, namely Wiener filter and the constrained least-squares filter [2]. Also we used in comparison the iterative nonlinear restoration based on the Lucy-Richardson algorithm [3].

This paper is organized as follows. In the second section we present process of image formation and problem formulation. In Section 3 we describe a method for the restoration of the blurred image. We observe certain enhancement in the parameters: *ISNR*, *PSNR* and *MSE*, compared with other standard methods for image restoration, which is confirmed by the numerical examples reported in the last section.

15 Modeling of the process of the image formation

We assume that the blurring function acts as a convolution kernel or point-spread function $h(n_1,n_2)$ and the image restoration methods that are described here fall under the class of linear spatially invariant restoration filters. It is also assumed that the statistical properties (mean and correlation function) of the image do not change spatially. Under these conditions the restoration process can be carried out by means of a linear filter of which the point-spread function (PSF) is spatially invariant. These modeling assumptions can be mathematically formulated as follows. If we denote by $f(n_1, n_2)$ the desired ideal spatially discrete image that does not contain any blur or noise, then the recorded image $g(n_1,n_2)$ is modeled as [2]:

$$\begin{aligned} g(n_1,n_2) &= h(n_1,n_2) * f(n_1,n_2) \\ &= \sum_{k_1=0}^{N-1}\sum_{k_2=0}^{M-1} h(k_1,k_2) f(n_1-k_1,n_2-k_2). \end{aligned} \tag{1}$$

The objective of the image restoration is to make an estimate $f(n_1,n_2)$ of the ideal image, under the assumption that only the degraded image $g(n_1,n_2)$ and the blurring function $h(n_1,n_2)$ are given. The problem can be summarized as follows: let H be a $m \times n$ real matrix. Equations of the form:

$$g = Hf, g \in \Re^m; f \in \Re^n; H \in \Re^{m\times n} \tag{2}$$

describe an underdetermined system of m simultaneous equations (one for each element of vector g) and $n = m + l - 1$ unknowns (one for each element of vector f). Here the index l indicates horizontal linear motion blur in pixels. The problem of restoring an image that has been blurred by uniform linear motion, usually results of camera panning or fast object motion can be expressed as, consists of solving the underdetermined system (2). A blurred image can be expressed as:

$$\begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ \vdots \\ g_n \end{bmatrix} = \begin{bmatrix} h_1 & \cdots & h_l & 0 & 0 & 0 & 0 \\ 0 & h_1 & \cdots & h_l & 0 & 0 & 0 \\ 0 & 0 & h_1 & \cdots & h_l & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & h_1 & \cdots & h_l \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ \vdots \\ f_m \end{bmatrix} \tag{3}$$

The elements of matrix H are defined as: $h_i = 1/l$ for i=1, 2,..., l. The objective is to estimate an original row per row f (contained in the vector f^T), given each row of a blurred g (contained in the vector g^T) and a priori knowledge of the degradation phenomenon H. We define the matrix F as the deterministic original image, its picture elements are F_{ij} for i=1,…, r and for j=1,…, n, the matrix G as the simulated blurred can be calculated as follows:

$$G_{ij} = \frac{1}{l}\sum_{k=0}^{l-1} F_{i,j+k}, i = 1,\cdots,r, j = 1,\cdots,m \tag{4}$$

with $n = m + l - 1$, where l is the linear motion blur in pixels. Equation (4) can be written in matrix form of the process of *horizontal* blurring as:

$$G = \left(HF^T\right)^T = FH^T \tag{5}$$

Since there is an infinite number of exact solutions for *f* or *F* in the sense that satisfy the equation $g = Hf$ or $G = FH^T$, an additional criterion that find a sharp restored matrix is required. The process of blurring with vertical motion is with the form:

$$g = Hf, g \in \Re^m; f \in \Re^r; H \in \Re^{m\times r} \tag{6}$$

where $r = m + l - 1$, and l is linear vertical motion blur in pixels. The matrix H is Toeplitz matrix as the matrix given in (3), but with other dimensions. The matrix form of the process of vertical blurring of the images is:

$$G = HF, G \in \Re^{m\times n}; H \in \Re^{m\times r}; F \in \Re^{r\times n} \tag{7}$$

16 Method for the image deblurring

The notion of Moore-Penrose inverse (generalized inverse) matrix of square or rectangular pattern is introduced by H. Moore in 1920 and again from R. Penrose in 1955, who was not aware of the work of Moore. Let *T* is real matrix with dimension $m \times n$ and $\Re(T)$ is the range of *T*. The relation of the form:

$$Tx = b, T \in R^{m\times n}, b \in R^m, \tag{8}$$

are obtained in the analysis and modeling of many practical problems. It is known that when *T* is a singular matrix, its unique Moore-Penrose inverse matrix is defined. In case when *T* is real matrix with dimension $m \times n$, Moore and Penrose proved that Moore-Penrose inverse matrix $T^\dagger$ is a unique matrix that satisfies the following four relations: $TT^\dagger T = T$, $T^\dagger TT^\dagger = T^\dagger$, $(TT^\dagger)^T = TT^\dagger$ and $(T^\dagger T)^T = T^\dagger T$.

We will use the following proposition from [5]:

Let $T \in R^{m\times n}, b \in R^m, b \notin \Re(T)$ and we have a relationship $Tx = b$, then we have $T^\dagger b = u$, where u is the minimal norm solution and $T^\dagger$ is the Moore-Penrose inverse matrix of *T*.

Since relation (2) has infinitely many exact solutions for *f*, we need an additional criterion for finding the necessary vector for restoration. The criterion that we use for the restoration of blurred image is the minimum distance between the measured data:

$$\min(\left\|\hat{f} - g\right\|), \tag{9}$$

where $\hat{f}$ are the first *m* elements of the unknown image *f*, which is necessary to restore, with the following constraint:

$$\left\|Hf - g\right\| = 0. \tag{10}$$

Following the above proposal, only one solution of the relation $g = Hf$ minimizes the norm $\|Hf - g\|$. If this solution is marked by $\hat{f}$, then for it is true:

$$\hat{f} = H^{\dagger}g \tag{11}$$

Taking into account the relations of horizontal blurring (2) and (5), and relation (11) solution for the restored image is:

$$\hat{F} = G(H^{T})^{\dagger} = G(H^{\dagger})^{T} \tag{12}$$

In the case of process of *vertical blurring* solution for the restored image, taking into account equations (6), (7) and (11), is:

$$\hat{F} = H^{\dagger}G \tag{13}$$

17 Numerical results

In this section we have tested the method based on Moore-Penrose inverse (generalized inverse) matrix (GIM method) of images and present numerical results and compare with two standard methods for image restoration called least-squares filters: Wiener filter and constrained least-squares filter and the iterative method called Lucy-Richardson algorithm. The experiments have been performed using Matlab programming language on an Intel(R) Core(TM) i5 CPU M430 @ 2.27 GHz 64/32-bit system with 4 GB of RAM memory running on the Windows 7 Ultimate Operating System.

In image restoration the improvement in quality of the restored image over the recorded blurred one is measured by the signal-to-noise ratio (*SNR*) improvement is defined as follows in decibels [6]:

$$\begin{aligned} ISNR &= SNR_{\hat{f}} - SNR_{g} \\ &= 10\log_{10}\left(\frac{\text{Variance of } g(n_1,n_2) - f(n_1,n_2)}{\text{Variance of } \hat{f}(n_1,n_2) - f(n_1,n_2)}\right) \end{aligned} \tag{14}$$

The simplest and most widely used full-reference quality metric is the mean squared error (*MSE*) [7], computed by averaging the squared intensity differences of restored and reference image pixels, along with the related quantity of peak signal-to-noise ratio (*PSNR*). The advantages of *MSE* and *PSNR* are that they are very fast and easy to implement. However, they simply and objectively quantify the error signal. With *PSNR* greater values indicate greater image similarity, while with *MSE* greater values indicate lower image similarity. Below *MSE*, *PSNR* are defined:

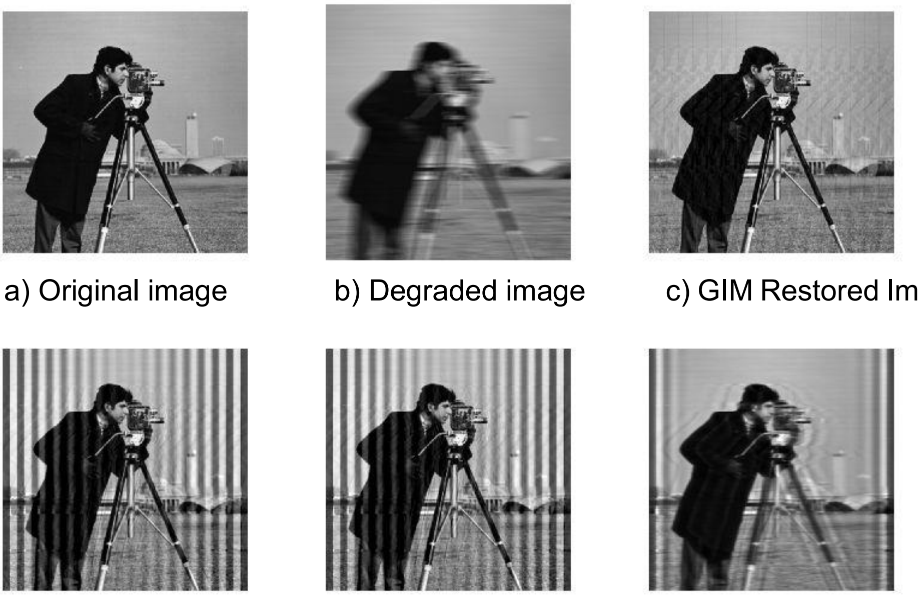
$$MSE = \frac{1}{rm}\sum_{i=1}^{r}\sum_{j=1}^{m}\left|f_{i,j} - \hat{f}_{i,j}\right|^{2} \tag{15}$$

$$PSNR = 20\log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right)(\text{dB}) \qquad (16)$$

where *MAX* is the maximum pixel value.

7.1 **Horizontal motion**

Figure 1, Original Image, shows such a deterministic original standard Matlab image Cameraman. Figure 1, Degraded Image, presents the degraded Cameraman image for *l*=30. Finally, from Figure, GIM Restored Image, Wiener Restored Image, Constrained LS Restored Image and Lucy-Richardson Restored Image, it is clearly seen that the details of the original image have been recovered. These figures demonstrate four different methods of restoration, method based on Moore-Penrose inverse, Wiener filter, Constrained least-squares (LS) filter, and Lucy-Richardson algorithm, respectively.



a) Original image b) Degraded image c) GIM Restored Image

d) Wiener Restored Image e) Constrained LS Restored Image f) Lucy-Richardson Restored Image

Figure 1 Restoration in simulated degraded Cameraman image for length of the horizontal blurring process, *l*=30

The difference in quality of restored images can hardly be seen by human eye. For this reason, the *ISNR*, *PSNR* and *MSE* have been chosen in order to compare the restored images. Fig. 2 – 4 shows the corresponding *ISNR*, *PSNR* and *MSE* values. The figures illustrate that the quality of the restoration is as satisfactory as the classical methods or better from them (*l*<100 pixels).

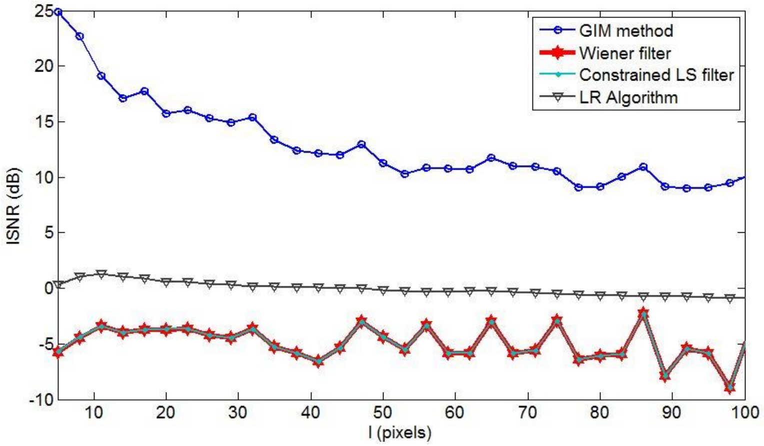


Figure 2 Improvement in signal-to-noise-ratio vs. length of the blurring process in pixels

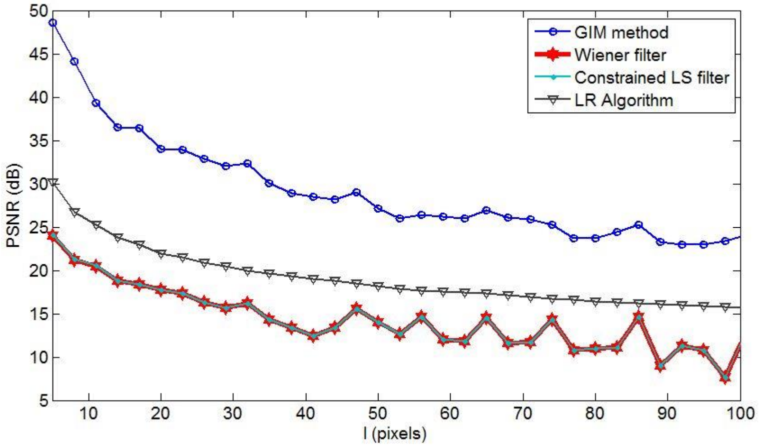


Figure 3 Peak signal-to-noise-ratio vs. length of the blurring process in pixels

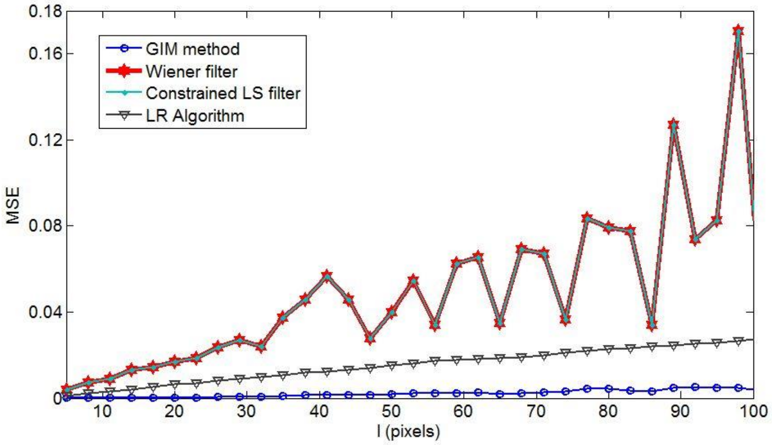
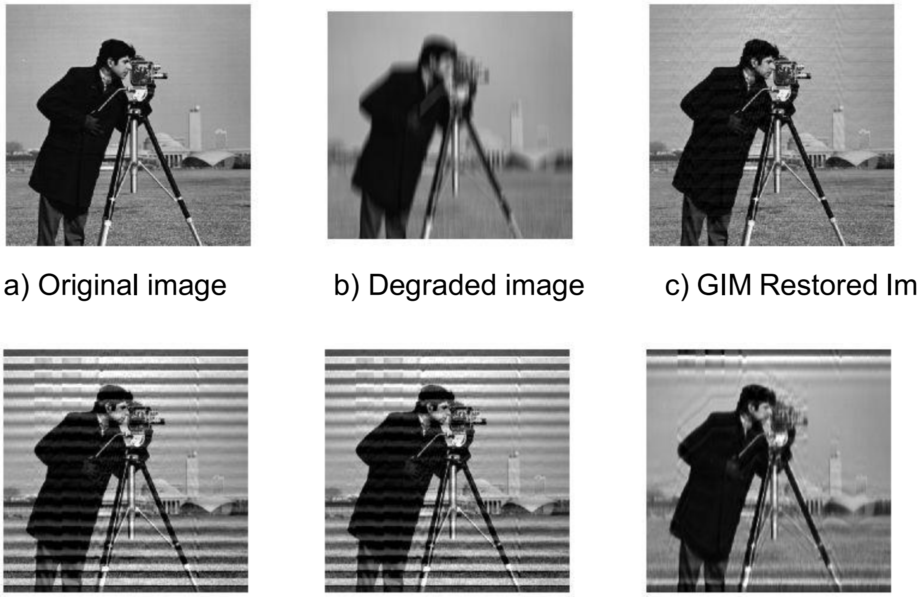


Figure 4 Mean squared error vs. length of the blurring process in pixels

7.2 **Vertical motion**

The results present in Fig. 5 – 8 refer when we have vertical blurring process.



a) Original image

b) Degraded image

c) GIM Restored Image

d) Wiener Restored Image

e) Constrained LS Restored Image

f) Lucy-Richardson Restored Image

Figure 5 Restoration in simulated degraded Cameraman image for length of the vertical blurring process, *l*=30

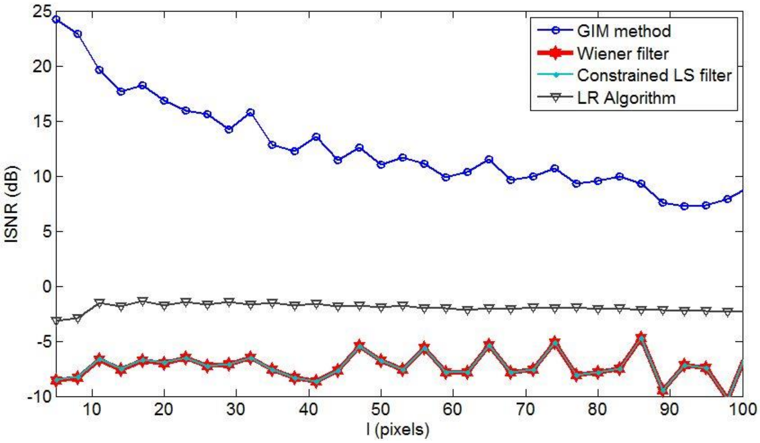


Figure 6 Improvement in signal-to-noise-ratio vs. length of the blurring process in pixels

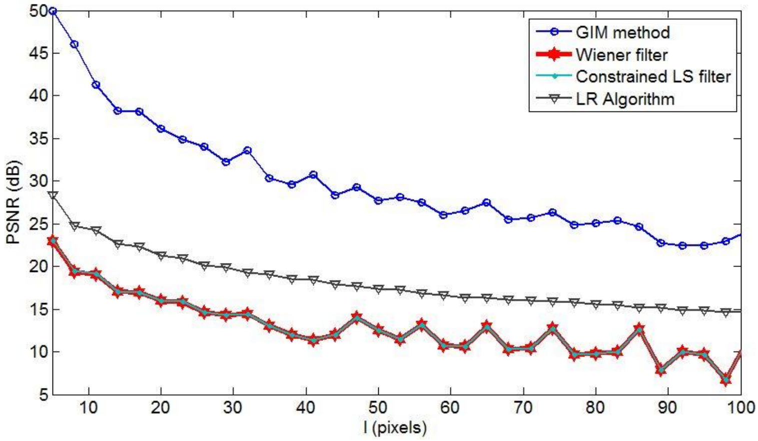


Figure 7 Peak signal-to-noise-ratio vs. length of the blurring process in pixels

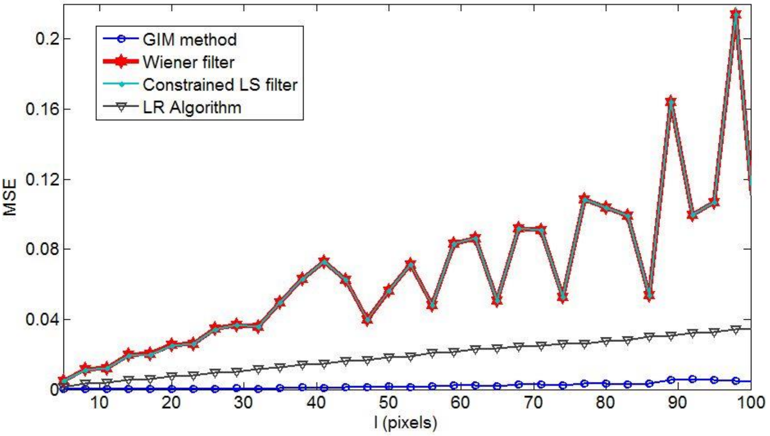


Figure 8 Mean squared error vs. length of the blurring process in pixels

18 Conclusion

We introduce a computational method, based on the Moore-Penrose inverse matrix, to restore an image that has been blurred by uniform linear motion. We are motivated by the problem of restoring blurry images via the well-developed mathematical methods and techniques based on Moore-Penrose inverse matrix in order to obtain an approximation of the original image. We present the results by comparing our method and that of the Wiener filter, Constrained least-squares filter and Lucy-Richardson algorithm, well-established methods used for fast recovery and restoration of high resolution images.

In the method we studied, the resolution of the restored image remains at a very high level, yet the *ISNR* is considerably higher while the computational efficiency is improved in comparison to other methods and techniques.

References

[1] J. Biemond, R. L. Lagendijk, and R. M. Mersereau (1990): *Iterative methods for image deblurring*. *Proc. IEEE*, 78(5), pp. 856–883.

[2] A. Bovik (2009): *The essential guide to the image processing*. Academic Press.

[3] R. C. Gonzalez, R. E. Woods (2002): *Digital Image Processing*, 2nd Edition. Prentice-Hall.

[4] I. Stojanovic, P. Stanimirovic and M. Miladinovic (2012): *Applying the Algorithm of Lagrange Multipliers in Digital Image Restoration*. FACTA UNIVERSITATIS, Series Mathematics and Informatics, ISSN 0352-9665, Vol. 27, No 1, pp. 41-54.

[5] S. Chountasis, V. N. Katsikis and D. Pappas (2009): *Applications of the Moore-Penrose Inverse in Digital Image Restoration*. Mathematical Problems in Engineering, Volume 2009.

[6] A. M. Eskicioglu and P. S. Fisher (1995): *Image Quality Measures and Their Performance.* IEEE Transactions on Communications, vol. 43, pp. 2959-2965.

[7] Z. Wang and A. C. Bovik (2009): *Mean Squared Error: Love It or Leave It? A New Look at Signal Fidelity Measures*. IEEE Signal Processing Magazine, vol. 26, no. 1, pp. 98-117.

THE INFLUENCE OF THE BUSINESS INTELLIGENCE ON THE BUSINESS PERFORMANCE MANAGEMENT

PhD Ljupco Davcev[1], Ana Ljubotenska[2]

1 Goce Delcev University, Faculty of Economics, Stip, Macedonia {ljupco.davcev@ugd.edu.mk}

2 Goce Delcev University, Faculty of Computer Science, Stip, Macedonia {ana.10642@student.ugd.edu.mk}

Abstract: The possibilities for expansion and growth of businesses are increasing with the development of information technology. Adding the information technology in business sector functioning is bringing new concepts which are affecting the future of business and information technology as two inseparable sciences. Managing business performance is a critical requirement for maximizing business profitability. Business performance management is actually a set of integrated analytical processes which using technology is directed towards financial and operational activities in a company. Managing business performance influence the process of reducing costs, increasing revenues and strengthening the competitive advantages of companies, which can be implemented using the technologies of business intelligence. The paper is covering the key performance indicators and balanced scorecards, which provide a framework for organizing strategic objectives in four different fields, namely internal business processes, financial, customer and development. As performance measurement periods are becoming shorter, management simply must have the capability for rapid reaction. To do this requires monitoring and tracking capabilities that can generate complete and accurate information upon which they can directly react. This information provides the required business intelligence for proactively managing business performance.

Keywords: key performance indicators, balanced scorecard, non-financial data, business performance

1. Introduction

The companies functioning in the global economy are in a complex position because the business performance measurement time frames are becoming shorter. The profitability, growth and success are analyzed quarterly instead annually. To keep pace with the changes, companies need to react quickly to incorporate varying demands and needs from the market. Elasticity and business cleverness are among the most important means to remain competitive. What is needed is a complete and comprehensive approach that facilitates companies to line up strategic and operational objectives in order to fully manage realization of their business performance measurements.

Successful businesses need information to give them a single view of their enterprise. With this type of information, they can make more effective decisions, manage business operations and minimize process interruptions, align strategic goals and priorities both vertically and horizontally throughout the business and establish a business environment that promotes continuous innovation and improvement [1, 2].

All these needs for constant redefinition of business goals and strategies requires an IT system that can take up these changes and help business users optimize business processes to assure business objectives. Business performance management has the main role here by providing key performance indicators, which can be used to evaluate business performance. In fact, key performance indicator is a performance metric for a specific business activity that has an associated business goal. The goal is used to determine whether or not the business activity is performing within accepted limits. The observation and analysis of key performance indicators provide business users with the approach necessary for business performance optimization. Business performance management also becomes a great guide for IT departments who are being asked to make logical observation from simple numbers in a way that it helps them focus their resources in areas that will provide support to enable management to meet their business goals. They can now concentrate their tasks and focus on those tasks that help to meet business measurements and achieve business goals. These tasks include planning, budgeting, forecasting, modelling, monitoring, analysis, and so forth [3, 4, 5].

To enable the implementation of business performance management organizations may need to improve their business integration and business intelligence systems to provide proactive and personalized analytics and reports. Business integration and business intelligence applications and tools work together to provide the information required to expand and observe key performance indicators. If some activity is outside the limits given from the key performance indicator, a kind of signal can be generated to notify business users that corrective actions are needed. Business intelligence tools are used here to display these types of indicators and guide users in taking appropriate actions.

2. The connection between BPM and BI

Business performance management has important impact on the cost reduction, income increase and strengthening the competitive advantages of the company. This process enables to develop, observe and compare basic indicators for company operation through monitoring and management of core business processes and objectives that needs to be achieved by taking the appropriate actions that will give the expected results. BPM is a complex business approach for managing the combination of strategic and operational objectives with current business activities. This can be implemented with the usage of the business intelligence technologies. Business performance management is generating a high level of interest and activity in the business and IT community because it provides management with their best opportunity to meet their business measurements and achieve their business goals.

The creation and management of business performance is not a simple one-time process. The emergences of new technologies and changes in the company's goals that go along with contemporary economic trends have a huge impact on the management of companies. Products or services offered by the company itself suffer changes. As the changes in business environment are continuously occurring, companies need to modify business processes that affect their performance and success. To be one step before the competitors, companies must quickly detect strengths and weaknesses in their operations, which will enable them effective decision making. Business performance management allows flexibility for the companies that will adapt them to the rapid and ongoing changes. So, the needs of businesses are creating the usage of business performance management. But, the implementation of business performance is much more than installation and implementation of new technology. The company needs to examine the business environment and to identify necessary changes to existing business processes in order to be able to use solutions which business performance management can offer [6,7].

[9] BPM-abbreviation for Business Performance Management

Business performance management is actually a set of integrated analytical processes which using technology is focused to the financial and operational activities in a company. Basically, the process of business performance management include financial and operational planning, monitoring and reporting, as well as models and analysis of key performance indicators. These indicators relate to certain business activities that have common target. Monitoring and analysis of key performance indicators, enables managers and creators of the future of a company insight into the needs for optimal business performance. Applications and business intelligence tools are needed to provide information used to develop and monitor key performance indicators. For example, when a particular activity or process is outside the limits of the key performance indicators, alarming managers provoke corrective actions that need to be taken by them. Business intelligence is used to obtain key performance indicators and to guide managers to take appropriate steps to solve business problems that arise in the company.

Business intelligence is used by companies for long-term strategic planning, short-term tactical analysis and manage everyday operations and activities. Business performance management uses business intelligence to access, select, combine, and analyze information and their usage in making decisions that will affect the next steps taken by the management of the company.

Business intelligence has a great impact on business planning. This particularly applies to strategic issues such as increasing revenue, reducing costs and a decision about introducing new products or services. If the main goal of companies is to increase sales, then the use of business intelligence should give guidance with information about which products are mostly sold, which locations and price, what are competitors and the possible impact of marketing on total sales. Business performance management and business intelligence are complementary in supporting the strategic planning by providing systems that compare current situation in the company with business objectives and helps managers to identify ways of improving long-term business performance [8, 11].

Except the planning of long term activities for achieving the objectives of the company, the use of business intelligence can have a profound impact on daily operations and activities of the company regarding the development and execution of these short-term activities in an efficient manner. If one of the main objectives of the company is achieving bigger sales and profitability, then the way it can be realized, is reviewing the production and delivery of products in a shorter time with the lowest cost. Here tactical and operational part of the business intelligence is used to help decision making and taking the appropriate steps by the managers. The business intelligence can be used on well-known traditional way, where production and achievements of the planned production quantities and possible spending cuts in this process will be monitored. However, business intelligence can be used to monitor and control the working process to improve and manage the overall operation of the company. Some of the possible impact can be made by identifying opportunities to improve quality or reduce the variable costs associated with production. All these possibilities of business intelligence usage related to the establishment of strategies in a company, as well as taking the tactical and operational activities in accordance with business performance management, help the company to establish business plans and perform daily activities.

Managing the business performances include various types of information and data arising from the work of the company, such as information from regular business activities, analysis of past activities, business plans, forecasts, data from the external environment of the company and other. These data types are used and processed using business intelligence to create a basis that will enable business performance management. Analyzing from a financial aspect, key performance indicators and balanced scorecards are used as main financial techniques in business performance management. The various techniques of business intelligence are used in their development, such as: data mining, data warehousing, as well as on-line analytical processing [12, 13].

To overcome the problems of managing business performance using only the numbers and analysis, and to use business performance management to obtain specific numerical indicators as final results, non-financial data processing should be introduced. As examples we can mention customer satisfaction, research and development in the company, the external image and ratings of the company, the impact of the environment, employee satisfaction and other. All these data can be obtained by using social networks, blogs and web pages, and different types of media (newspapers, magazines, TV shows and others).

3. Balanced scorecards and KPI

In the process of setting the basics of business performance management, it is necessary to precisely define the key performance indicators. Each of these key performance indicators needs to express one of the major goals of the company and its future plans, so the management of these key business indicators will result in improved business performance. These indicators actually direct and guide the decisions of the company indicating whether the work the company is operating in accordance with predefined operating plans and strategies. Different types of companies have a number of key business indicators, from simpler to more complex. Business performance management needs to extract the most important indicators that are needed to process and thus to determine the next steps and ways to meet the objectives of the company. Among the long list of possible key performance indicators can be mentioned: the number of companies that are buyers of products, the average number of customers within a specified period, the value of products by customer, not fulfilled orders, temporary delay in delivery, accurate delivery, turnover, average costs of transportation to customers, sales trends, unplanned expenses, demographic separation of purchase, payment of outstanding debts and other. In the process of selection of key performance indicators managers can use as simple indicators as production in one shift, to more complex indicators that give results related to profitability by product, location or season. The choice depends on whether it is managed with daily operations or long-term business performance [14].

The need for business performance management is expressed in all levels and in relation to overall functioning in a company. Managers can recognize the need for strategic management of business performance that is the need to detect the linkage of strategy and business processes and activities undertaken to fulfil that strategy, and to analyze whether and how these processes successfully implement this strategy. Executive managers need performance management which will be consistent with the business processes they manage and should be linked to overall business strategy of the company, which provides the main reason for the use of balanced scorecards . Including business intelligence here, balanced scorecards actually are analytical applications that accumulate, model and display multidimensional performance information. These include financial, non-financial performance targets, daily indicators, analysis of trends in the company and other. Traditional business intelligence tools are used for complete critical processing of collected data, analysis and presentation in order to set objectives in managing business performance.

Balanced scorecards provide a framework for organizing strategic objectives in four different fields: financial, customer, internal business processes and development. The financial section deals with development strategy, profitability, and risk viewed from the perspective of shareholders and other stakeholders directly and indirectly related to the company. In terms of customers, the strategy is to create values and differences of the company in comparison to the other companies that will be visible by customers. Strategy in terms of internal business processes is giving strategic priorities for various business processes that affect the objectives of the company. Development, as one of the four parts from balanced scorecards, is providing a climate that will support organizational change, innovation and growth of the company. These four fields provide the basis for constructing the plan that will include and implement these strategies. Here are several critical elements that will have a direct connection to organizational strategy, such as the growth of productivity, profitability growth by increasing the part of the market where the company is represented, improve operational processes and achieving the goals, innovation in products and services, as well as the need for investment to generate sustainable development. Creating the logical architecture of the strategic framework with the help of these elements, managers have clear picture of the company’s goals and how those goals will be achieved [15, 16].

Non-financial indicators enable managers’ better insight to the overall functioning of the company, because many non-financial indicators can often reflect intangible values in the company, which accounting rules refuse to accept for processing. In addition, non-financial indicators provide information about specific activities that should be taken to achieve certain strategic objectives. Contemporary modes of operation require from the companies to identify areas where non-financial indicators can have a major impact on the implementation of the given strategy. In addition, proper selection of non-financial indicators and their proper connection with the financial indicators provide sufficient basis for deep analysis that managers should make for better functioning of the company. But, it is important to determine which non-financial factors have the greatest effect on long-term economic performance. Choosing an appropriate model according to which the managers will determine the non-financial indicators and establishing database, which transformation into information will give the values of the indicators, are the most important parts in setting the foundations for getting the non-financial indicators important for the companies [17].

4. Conclusions

The management in the company need to focus on ways of implementing business performance management in software tools, where using the balanced scorecards will overcome difficulties with the management of data in the company collected from different sources. These data should be integrated into data warehouse, where it will be saved for further processing and presented with usage of different graphical tools. Through the implementation of business performance management, multidimensional business data and specifically named information parts (perspectives, objectives, initiatives) that are used by balanced scorecards will be linked. Also, the connection between different parts will be established. Implementation applies in relation to the preparation of special reports that will provide a graphic display of important indicators. Well performed implementation will be of great importance for managing the companies and improve their business performance.

References

[1] H. Dresner, The Performance Managemnt Revolution (pp. 9-20). Hoboken, New Jersey: JOHN WILEY & SONS, INC. (2008).

[2] Kenny, G. (2005). Strategic Planning and Performance Management. Elsevier.

[3]A. Neely, Business Performance Measurement (pp. 280-304). Cambridge University Press. (2007).

[4] Parmenter, D. (2007). Key performance indicators:developing,imple menting and using winning KPI’s. John Wiley and Sons.

[5] Maisano, D. (2007). Management by measurement:Designing key indicators and performance measurement systems. Berlin: Springer.

[6] (2005). In A.-W. Scheer, Corporate Performance Mangement (pp. 7-31). New York: Springer. (2005).

[7]P. Taticchi, Business Performance Measurement and Menagement (pp. 1-34). London: Springer. (2010).

[8] Nils Rasmussen, P. S. (2002). FInancial Business Intelligence:Trends, Technology, Software Selection and Implementation. New York: John Wiley and Sons, Inc.

[9] Agrawal, D. (2008). The Reality of Real-Time Business Intelligence. In usiness Intelligence for the Real-Time Enterprise (pp. 75-88). Springer.

[10] Thomas H. Davenport, Jeanne G. Harris, (2007) The architecture of business intelligence, Harvard Business School Press

[11] Bill Hostmann, Nigel Rayner, Ted Friedman, (October 2006) Gartner’s business intelligence and performance management framework, Gartner Inc.

[12] Olson, D.L., Shi, Y.: Introduction to Business Data Mining. McGraw-Hill/Irwin, Englewood Cliffs (2007)

[13]Inmon, William H. Building the Data Warehouse. New York: John Wiley & Sons, Inc., 1996.

[14] Herzner, H. (2011). PROJECT MANAGEMENT METRICS, KPIs AND DASHBOARDS. New York: John Wiley & Sons.

[15] Kaplan, R. and D. Norton (1992). “The Balanced Scorecard – measures that drive performance.” Harvard Business Review(January/Febraury):

9.

[16] Libby, T., S. E. Salterio, and A. Webb. 2004. The balanced scorecard: The effects of assurance and process accountability on managerial judgment. The Accounting Review 79 (4): 1075-1094.

[17] Ittner, C. D., and D. F. Larcker. 1998. Are nonfinancial measures leading indicators of financial performance? An analysis of customer satisfaction. Journal of Accounting Research 36 (supplement): 1-35.

LINQ TO OBJECTS SUPPORTED JOINING DATA

Mariana Goranova[1,*]

[1,*]*Technical University of Sofia, mgor@tu-sofia.bg*

Abstract: Joins have been studied as a key operations in multiple application domains. This paper focuses on the study of joins as a first-class LINQ operators and their implementation as integrated component of the query processing. The join methods provided in the LINQ perform inner join, left outer join, and cross join. Our goal is to provide join operations, similar to SQL statements in the databases. We describe an efficient implementation of the following join operators: inner join, left outer join, right inner join, full outer join, left excluding join, right excluding join, full outer excluding join, and cross join. A simple example is used to present the potentialities of LINQ technology to solve the problem with the object-relational mapping.

Keywords: LINQ query, inner join, outer join, cross join, C# programming language

19 Introduction

Concept of joining is a key concept of accessing data. From SQL and relational point of view, almost every query requires joining data. SQL languages have powerful join capabilities. They support different types of joins, including inner joins, outer joins, and cross joins [1].

Language Integrated Query (LINQ) is the technology that addresses the problems between programming languages and databases. LINQ provides a uniform, object-oriented way to access data from heterogeneous sources and simplifies the interaction between object-oriented programming and relational data.

In this paper, we implement the set of join operators in LINQ that use syntax similar to SQL [3,4]. The main contributions include the study of joins as a first-class LINQ operators and their implementation as integrated component of the LINQ query processing.

The rest of the paper is organized as follows. Section 2 discusses the background. Section 3 presents the different types of SQL-like joins and syntax using examples in C#. Section 4 presents the conclusions and directions for future research.

20 Background

LINQ is a programming model that introduces queries as a first-class concept into any Microsoft .NET Framework Language [5]. LINQ provides a uniform way to access and manage data in the program, keeping existing heterogeneous data structures, regardless of their physical representation – the data source might be a graph of objects in-memory, relational table or XML file [2]. The software developers use the same query syntax over all different data access models.

The LINQ architecture is shown in Figure 1. The different data sources are as follows: LINQ to Objects, LINQ to Datasets, LINQ to SQL, LINQ to Entities, and LINQ to XML.

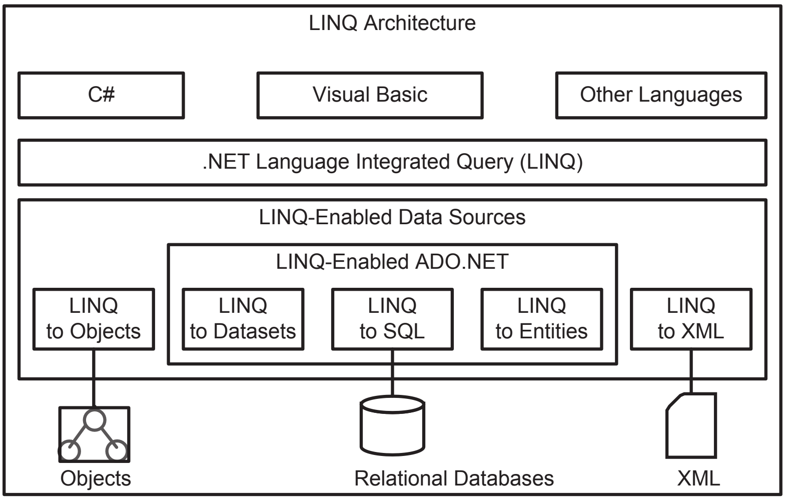


Figure 1 LINQ architecture

LINQ query is a set of operations on instances of some classes. The declarative description of operations on data using syntax very similar to SQL is the most important feature of LINQ because it enhances programmers' productivity.

21 Join operators

Joining data sets is the process of linking two data sources through a common attribute. Joining is an important operation in queries. It models a correlation between objects that is not implemented in the object-oriented programming.

7.3 Class model

In the example we will use a data structure that represents information about courses, with enrolls and students. Each course includes many enrolls. The class **Course** has information about **ID** number, **Title** and a reference to a set of **enroll**s. Class **Enroll** has information about **EnrollId**, **Grade** and faculty number **FN** of a student. Class **Student** has a faculty number **FN** and **Name**. The definitions of these types are represented in the Appendix. The data consists of a set of **courses**, each of which has enrolled **students**. The initialized instances are shown in the Appendix.

We assume we have two sets – **students** is on the left and **coursesEnrolls** is on the right. We can join these sets by their common **FN** attributes.

```
var coursesEnrolls =  from course in courses
                      from e in course.enroll
                        select e;
```

7.4 Inner join

The inner join is the most common join operator. It creates a result set of elements of the two sets (**students** and **coursesEnrolls**) that match in both sets. The inner join is implemented in the LINQ base library using the **Join** method.

SQL statement:

```
SELECT * FROM STUDENTS
INNER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
```

Query expression syntax:

```
var innerJoin =from x in students
  join y in coursesEnrolls
  on x.FN equals y.FN
  select new { X = x, Y = y };
```

Lambda expression syntax:

```
var innerJoin = students
  .Join(coursesEnrolls,
  x => x.FN, y => y.FN, (x, y) => new {
x, y })
  .Select(item => new { item.x, item.y });
```

Result:	FN	Name	EnrollId	Grade	FN
	222100	Petia Petrova	2	5	222100
	222101	Julian Emilov	4	6	222101
	222103	Neli Ivanova	6	6	222103
	222104	Ivan Georgiev	9	6	222104

FN values from **students** match with the **FN** from **coursesEnrolls**. The inner join only returns elements where the two sets intersect.

7.5 Left outer join

The left outer join creates a result set that includes all elements from the left set (**students**) with the matching elements from the right set (**coursesEnrolls**). The left outer join is implemented using the **GroupJoin** method on the left set and then using **from** operator to get the matching elements from the right set, if any exist. If there is not match the right side will contain null using the **DefaultIfEmpty** extension method.

SQL statement:

```
SELECT * FROM STUDENTS
LEFT OUTER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
```

Query expression syntax:

```
var leftOuterJoin =
  from x in students
  join y in coursesEnrolls
  on x.FN equals y.FN into yG
  from y1 in yG.DefaultIfEmpty()
  select new { X = x,
                 Y  =  y1  ==  null  ?
null : y1 };
```

Lambda expression syntax:

```
var leftOuterJoin =
  students
  .GroupJoin(coursesEnrolls,
  x => x.FN, y => y.FN, (x, g) => new {
x, g })
  .SelectMany(y                    =>
y.g.DefaultIfEmpty(),
    (item, y) => new { X=item.x, Y=y });
```

Result:	FN	Name	EnrollId	Grade	FN
	222100	Petia Petrova	2	5	222100
	222101	Julian Emilov	4	6	222101
	222102	Anely Borisova	0	0	-1
	222103	Neli Ivanova	6	6	222103
	222104	Ivan Georgiev	9	6	222104
	222105	Mila Ivanova	0	0	-1
	222107	Kristi Kirilova	0	0	-1
	222112	Anton Ivanov	0	0	-1

The result set contains all students but four students have no enrolls associated with them – the return objects by the **Enroll** class are null and the **NullReferenceException** is controlled.

7.6 Right outer join

The right outer join creates a result set that includes all elements from the right set (**coursesEnrolls**) with the matching elements from the left set (**students**). It closely likes to a left outer join with reversed sets.

SQL statement:

```
SELECT * FROM STUDENTS
RIGHT OUTER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
```

Query expression syntax:

```
var rightOuterJoin =
  from y in coursesEnrolls
  join x in students
  on y.FN equals x.FN into xG
```

Lambda expression syntax:

```
var rightOuterJoin =
  coursesEnrolls
  .GroupJoin(students,
  from x1 in xG.DefaultIfEmpty()
  select new { X = x1==null ? null
: x1,
              Y = y };
```

```
  x => x.FN, y => y.FN, (x, g) => new {
x, g })
  .SelectMany(y                    =>
y.g.DefaultIfEmpty(),
  (y, item) => new { X = item, Y = y.x });
```

Result:	FN	Name	EnrollId	Grade	FN
	222100	Petia Petrova	2	5	222100
	-1	null	3	6	222201
	222101	Julian Emilov	4	6	222101
	222103	Neli Ivanova	6	6	222103
	-1	null	7	5	222200
	222104	Ivan Georgiev	9	6	222104
	-1	null	10	5	222110
	-1	null	11	4	222111

The result set contains all enrolls where four enrolls have no students associated with them – the return objects by the **StudentI** class are null and the **NullReferenceException** is controlled.

7.7 Full outer join

The full outer join creates a result set that includes all elements from the left set (**students**) and the right set (**coursesEnrolls**) with the matching elements from the both sets where available. If there is not match the missing left/right side will contain null.

SQL statement:

```
SELECT * FROM STUDENTS
FULL OUTER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
```

Lambda expression syntax:

```
var fullOuterJoin = leftJoin.Union(rightJoin);
```

Result:	FN	Name	EnrollId	Grade	FN
	222100	Petia Petrova	2	5	222100
	222101	Julian Emilov	4	6	222101
	222102	Anely Borisova	0	0	-1
	222103	Neli Ivanova	6	6	222103

	222104	Ivan Georgiev	9	6	222104
	222105	Mila Ivanova	0	0	-1
	222107	Kristi Kirilova	0	0	-1
	222112	Anton Ivanov	0	0	-1
	-1	null	3	6	222201
	-1	null	7	5	222200
	-1	null	10	5	222110
	-1	null	11	4	222111

7.8 Left excluding join

The left excluding join creates a result set that includes only elements from the left set (**students**) that are not in the right set (**coursesEnrolls**). It performs the left outer join and then excludes the common elements from the right set.

SQL statement:

```
SELECT * FROM STUDENTS
LEFT OUTER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
WHERE COURSESENROLLS.FN IS NULL
```

Query expression syntax:

```
var leftExcludingJoin = from x in
students
  join y in coursesEnrolls
  on x.FN equals y.FN into yG
  from y1 in yG.DefaultIfEmpty()
  where y1 == null
  select new { X = x,
               Y = y1 == null ? nu
: y1 };
```

Lambda expression syntax:

```
var leftExcludingJoinl = students
  .GroupJoin(coursesEnrolls,
  x => x.FN, y => y.FN, (x, g) => new {
x, g })

.SelectMany(y=>y.g.DefaultIfEmpty(),
  (item, y) => new { X = item.x, Y = y })
  .Where(y=>y.Y==null);
```

Result:	FN	Name	EnrollId	Grade	FN
	222102	Anely Borisova	0	0	-1
	222106	Mila Ivanova	0	0	-1
	222107	Kristi Kirilova	0	0	-1
	222112	Anton Ivanov	0	0	-1

7.9 Right excluding join

The right excluding join creates a result set that includes only elements from the right set (**coursesEnrolls**) that are not in left set (**students**). It closely likes to a left excluding join with reversed sets.

SQL statement:

```
SELECT * FROM STUDENTS
RIGHT OUTER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
WHERE STUDENTS.FN IS NULL
```

Query expression syntax:

```
var rightExcludingJoin =
  from y in coursesEnrolls
  join x in students
  on y.FN equals x.FN into xG
  from x1 in xG.DefaultIfEmpty()
  where x1==null
  select new { X = x1 == null ? null :
x1,
                Y = y };
```

Lambda expression syntax:

```
var rightExludingJoin =
  coursesEnrolls
  .GroupJoin(students,
  x => x.FN, y => y.FN, (x, g) =>
new { x, g })
  .SelectMany(y                    =>
y.g.DefaultIfEmpty(),
  (y, item) => new { X = item, Y = y.x
})
  .Where(x=>x.X==null);
```

Result:	FN	Name	EnrollId	Grade	FN
	-1	null	3	6	222201
	-1	null	7	5	222200
	-1	null	10	5	222110
	-1	null	11	4	222111

7.10 Full outer excluding join

The full outer excluding join creates a result set that includes unique elements from the left set (**students**) and the right set (**coursesEnrolls**) that do not match. It performs the full outer join and then excludes the common elements from the both sets.

SQL statement:

```
SELECT * FROM STUDENTS
FULL OUTER JOIN COURSESENROLLS
ON STUDENTS.FN=COURSESENROLLS.FN
WHERE STUDENTS.FN IS NULL OR COURSESENROLLS.FN IS NULL
```

Lambda expression syntax:

```
var fullOuterExcludingJoin = leftExcludingJoin.Union(rightExcludingJoin);
```

Result:	FN	Name	EnrollId	Grade	FN
	222102	Anely Borisova	0	0	-1
	222105	Mila Ivanova	0	0	-1
	222107	Kristi Kirilova	0	0	-1
	222112	Anton Ivanov	0	0	-1
	-1	null	3	6	222201
	-1	null	7	5	222200
	-1	null	10	5	222110
	-1	null	11	4	222111

7.11 Cross join

The cross join or Cartesian product creates a result set that includes all possible ordered pairs whose first component is a member of the left set (**students**) and whose second component is a member of the right set (**coursesEnrolls**).

SQL statement:

```
SELECT * FROM STUDENTS
CROSS JOIN COURSESENROLLS
```

Query expression syntax:	**Lambda expression syntax:**
`var crossJoin =`	`var crossJoinl =`
`  from x in students`	`  students`
`  from y in coursesEnrolls`	`  .SelectMany(x=>coursesEnrolls,`
`  select new { X = x, Y = y};`	`  (x,y)=>new { X=x, Y=y});`

The result set contains 64 elements – all of the {student,enroll) pairs, even the combinations are not valid.

8 Conclusion and Future Work

We have proposed implementation of join operations using LINQ. These operations implement the behavior of the SQL join operations. We make attempt to solve the gap between the programming languages and the databases. These operations can be used for the purposes of analysis and visualization.

Plans for future work include the study and integration of join strategies as first-class LINQ operators in approaches that support SOA-based scientific data management.

References

[1] Jeff Atwood, Coding Horror (2007): *A Visual Explanation of SQL Joins*, Last access 10.11.2012, http://www.codinghorror.com/blog/2007/10/a-visual-explanation-of-sql-joins.html.

[2] M. Goranova and L. Stoyanova (2012): *Effective query implementation of scientific data based on LINQ to XML*. Annual Journal of Electronics 6(2), pp. 125-128.

[3] Juan Francisco Morales Larios (2012): *LinQ Extended Joins*, Last access: 10.11.2012, http://www.codeproject.com/Articles/488643/LinQ-Extended-Joins.

[4] Scott Mitchell (2009): *An Extensive Examination of LINQ: Grouping and Joining Data*, Last access: 10.11.2012, http://www.4guysfromrolla.com/articles/080509-1.aspx.

[5] P. Pialorsi and M. Russo (2010): *Programming Microsoft LINQ in Microsoft .NET Framework 4*, O'Reilly Media, Inc.

Appendix

```
class Course
{
   public int ID { get; set; }
   public string Title { get; set;
}
   public Enroll[] enroll;
   public    override    string
ToString()
   {
      string r = ID + "\t" + Title
+ "\n";
      foreach (var e in enroll)
         r += e.ToString();
      return r;
   }
}

class Enroll
{
   public  int?  EnrollId  {  get;
set; }
   public int? Grade { get; set;
}
```

```
List<Course> courses = new List<Course>() {
   new Course { ID = 1, Title = "Distributed
Systems",
     enroll = new Enroll[] {
       new   Enroll   {EnrollId=2,   Grade=5,
FN=222100},
       new   Enroll   {EnrollId=3,   Grade=6,
FN=222201}}},
   new Course { ID = 2, Title = "Computer
Graphics",
      enroll = new Enroll[] {
       new   Enroll   {EnrollId=4,   Grade=6,
FN=222101},
       new   Enroll   {EnrollId=6,   Grade=6,
FN=222103},
       new   Enroll   {EnrollId=7,   Grade=5,
FN=222200}}},
   new Course { ID = 3, Title = "Software
Engineering",
      enroll = new Enroll[] {
       new   Enroll   {EnrollId=9,   Grade=6,
FN=222104},
   public int? FN { get; set; }
   public     override     string
ToString()
   {
      return
EnrollId+"\t"+Grade+
              "\t"+FN;
    }
}

class Student
{
   public int? FN { get; set; }
   public  string  Name  {  get;
set; }
   public     override     string
ToString()
   {
     return FN + "\t" + Name;
   }
}
```

```
       new    Enroll    {EnrollId=10,    Grade=5,
FN=222110},
       new    Enroll    {EnrollId=11,    Grade=4,
FN=222111}}}
};

List<Student> students = new List<Student>()
{
   new  Student  {FN=222100,  Name="Petia
Petrova"},
   new  Student  {FN=222101,  Name="Julian
Emilov"},
   new  Student  {FN=222102,  Name="Anely
Borisova"},
   new   Student   {FN=222103,   Name="Neli
Ivanova"},
   new  Student  {  FN=222104,  Name="Ivan
Georgiev"},
   new   Student   {FN=222105,   Name="Mila
Ivanova"},
   new  Student  {FN=222107,  Name="Kristi
Kirilova"},
   new  Student  {FN=222112,  Name="Anton
Ivanov"}
};
```

GLOBALIZATION, INFORMATION TECHNOLOGY AND NEW DIGITAL ECONOMIC LANDSCAPE

Riste Temjanovski[11]

Abstract: Globalization is not a new phenomena. Globalization is largely driven by new technology and has resulted in a widening gap and new digital economic landscape between developed and developing countries. Digital economy gap can be described as the gap between those who have access to the Internet and network systems and those without access, or possess the lack of access to Internet network, hardware and informatics knowledge. Today, we can identify a number of national factors that go beyond wealth in explaining differences among countries in the level of ecommerce transactions. These include investment resources, technology, information and network infrastructure, competitive knowledge, and rule of law. This global problem calls for global convergent collective action to involve all the actors to widen the benefit of Information technology and knowledge to all.

In the 21st century world intelligences must take the action to bridging gap between developed and developing countries. Bridging the digital gap and alleviating information “poverty” to provide a more equitable and sustainable future for all, require new integrated approaches that fully incorporate existing and new scientific knowledge.

Keywords: Globalization, Information technology, digital gap, economic landscape, Information knowledge

[11] ***Associate Prof. Riste Temjanovski,*** *PhD,* Goce Delcev" University – Faculty of Economics – Stip, R.of Macedonia e-mail: riste.temjanovski@ugd.edu.mk

Introduction

Information and communication technologies (ICT) are considered as one of the main initiator of global economic transformation. Although they are the creators of the new economic design for a more comfortable setting, at the same time they can lead to new divisions between countries and regions. Especially it concerns all those who are not able to make priority IT resources as a model for transforming and taking full advantage of the development potential offered by ICT. As a result, it may further exacerbate existing problems, particularly to expand social and economic adverse amplitudes and slow processes of regional cooperation as a result of the increasing inter and intraregional development gaps in building modern economies, based information and knowledge. If ICT are properly directed, then they are increasingly seen as an effective source for inclusion and cultural transformation.

Internet is one of the most complex things ever created. It elevates the whole social organization to a higher level. Internet technology impact on the creation of digital economy and registers etc. "Third wave" of capitalism that affects the complete transformation of the business world, creates positive growth worldwide and lead to extraordinary wealth creation. As technological innovation is considered as a major dynamic factor in economic growth, leaders of economic growth and development can be not only large corporations but also small and medium enterprises if they are able to create, develop new technological solutions and shape new products or services. According to modern theories of economic growth, technological innovation, especially in the developed countries will be an important factor of the increase of capital, because technological progress increases the quality, and thus significantly contributes to economic growth and power. IT enables the creation of new markets, and provides the conduit for the fluid movement of resources and demand. As a result, firms and individuals worldwide can participate in innovation, wealth creation and social interaction in ways which were impossible before. Major area of technological advances in recent microprocessors, lasers, fiber optics and satellite technology, and in the forthcoming period would be genetic engineering and microbiology.

Era of global digital technology, "new economy" and creating a digital gap between countries

Economic growth and technology are inextricably linked. Tectonic changes in the world economy, combined with the expansive growth in technology irreversibly transform the global market. Today, globalization, Internet hyper competition gives a new dimension to the market and operation. All three forces, reinforce the pressure to reduce prices. The reasons should be sought in the growing interest in electronic commerce.

Digital gap is a very complex phenomenon. It has been discussed in the economics, politics, sociology, information science and philosophy. The term digital gap is simply defined as the gap that exists between those who have and those who do not have access to the modern ICT such as the telephones, computers, internet and related services. [1]

The Digital gap (divide) can be described as the gap between those who have access to the Internet and those who don't have access, and include lack of availability of hardware, communications and knowledge. [10]

The question is how to bridge this gap. Some have suggested that this bridge is the responsibility of governments, of some international institutions, academic backgrounds, and some think the individual opinion is important. If globalization is meant to bring benefits to all peoples and nations, the benefits of information technology must be shared between developed and developing countries.

If the emergence of the Internet in the 90s at last did a "simple vibration" in the working and living environment of the individual, the development of new generation wireless internet and other technological performance will cause real "tectonic shifts" in twenty-first century. They will shape the new economic landscape by creating a deep divide between countries that maximum follow information and technological waves and countries that are not able to follow these developments.

The new challenges of technological transformation

Information and communication technologies (ICT) are considered one of the main driving forces of global economic transformation. ICT has made major strides this past decade, improving significantly the process of doing business and outpacing all industries in its contribution to three key economic indicators: industrial output, employment and productivity. Historically, most companies in advanced economies modernized inside the framework of a domestic strategy, growing first within their own borders and then replicating their business elsewhere. Today’s emerging economies, however, are doing at a time when technology has made it much easier to gain access to global capital, talent and other resources, allowing them to instantly plan for a global market.

This digital divide is created by global technological competition that feels both developed and emerging economies. The virtuos circle is not just restructuring the world economy; it is leading to a new phase of industrial transformation. According to a study in which participated the leading information technology companies (AT & T and Cisco), and investigated the matter and actuality shows six dramatic changes that will face companies in the next five years: [2]

- The global digital economy comes of age
- Industries undergo a digital transformation
- The digital divide reverses
- The emerging markets customer takes center stage
- Business shifts into hyperdrive
- Companies reorganize to embrace the digital economy

Indeed, to compete on the global stage, and reap the benefits of the digital marketplace, IT experts agree that industries will continue to see sweeping changes over the next five years, particularly in IT (72%); telecommunications (66%); entertainment, media and publishing (65%); retail (48%); banking (47%) and life sciences (38%).That is the nature of technology, for both good and bad—it destroys old ways of operating that aren’t as powerful anymore.”

It is estimates that in 2000, only 4% of the world’s population had access to the Internet. Of these, more than half were in North America while less than 1% was in Africa. The advent of satellite technology and wireless application protocol offers new opportunities to facilitate Internet access in all over the world (city and rural community, schools and libraries etc.). It is estimated that the number of Internet users worldwide should reach 2.2 billion people in 2013, and that number will grow to almost 2.8 billion (about 38% of the world population) by 2015. Not surprisingly, the biggest spike will be in Asia - 43%, of which only 17% from China. So even though the reflections of the global economic crisis, positive growth has seen the number of Internet users in developing countries. It is believed that in 2010 the number of Internet users has increased by 15.6% compared to 2009 and amounted to 1.19 billion, compared to 885 million in developed countries, the growth for the same period was 7.79%.

With Internet access, developing counties can join the global market place and contribute to and participate in the global knowledge communities and global markets. They can have access to education, health commercial and other services at rapid speed and affordable costs.

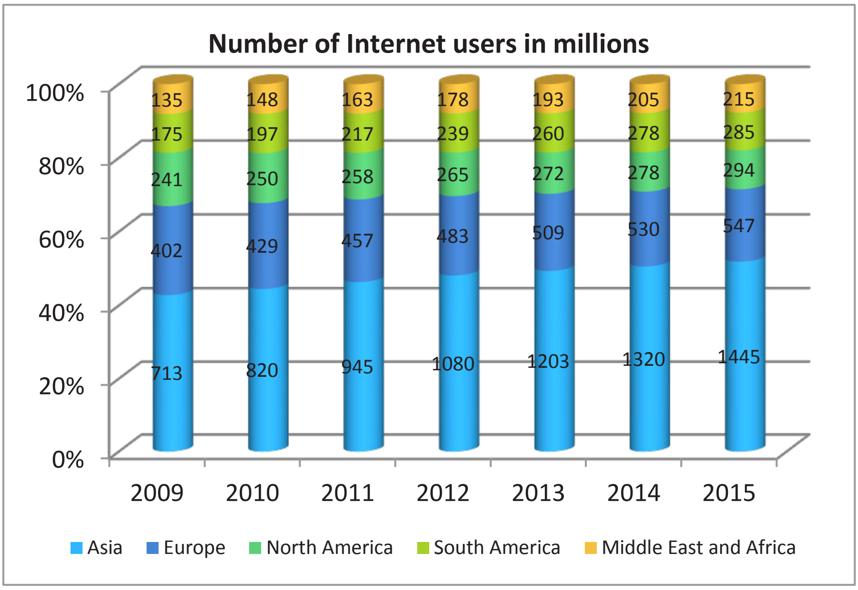


Figure 1 Number of Internet users in millions

The largest share, almost half of Internet users in the world will be in Asia. Internet access by country shows us two things: the Scandinavian countries (per capita registered users) most use Internet technology, followed by the countries of North America and Australia. But the situation is now rapidly changing. Australia is linked to the other world with new technology, as well as world leaders, North America and Scandinavia. It develops a new beginning and the end "the tyranny of isolation" for Australians.[12]

Although ICTs are those who can transform the new world more pleasant environment, they can at the same time lead to new divisions between countries and regions. Especially it concerns all those who are not able to priorities IT resources as a model for transforming and taking full advantage of the development potential offered by ICT.

Table 1 Internet access and broadband internet connections in households (%)

Country	2005	2006	2007	2008	2009	2010	2011
EU - 27	48	49	55	60	66	70	73
Belgium	50	54	60	64	67	73	77
Bulgaria		17	19	25	30	33	45
Czech	19	29	35	46	54	61	67
Denmark	75	79	78	82	83	86	90
Germany	62	67	71	75	79	82	83
Estonia	39	46	53	58	63	68	71
Ireland	47	50	57	63	67	72	78
Greece	22	23	25	31	38	46	50
Spain	36	39	45	51	54	59	64
France	:	41	55	62	69	74	76
Italy	39	40	43	47	53	59	62
Cyprus	32	37	39	43	53	54	57
Latvia	31	42	51	53	58	60	64
Lithuania	16	35	44	51	60	61	62
Luxembourg	65	70	75	80	87	90	91
Hungary	22	32	38	48	55	60	65
Malta	41	53	54	59	64	70	75
Netherlands	78	80	83	86	90	91	94
Austria	47	52	60	69	70	73	75
Poland	30	36	41	48	59	63	67
Portugal	31	35	40	46	48	54	58
Romania		14	22	30	38	42	47
Slovenia	48	54	58	59	64	68	73
Slovakia	23	27	46	58	62	67	71
Finland	54	65	69	72	78	81	84
Sweden	73	77	79	84	86	88	91

[12] Can quote the message one student from Australia: "It's great for us here in Australia, especially for our small and sheltered Tasmania. This will enable us to overcome the tyranny of the first geographical distance." Exports of high-valued services will grow. Knowledge capital will be traded on international prices. No need to leave the country if you do not want, because everyone can participate in the creation of knowledge in international prices internationally.

Great Britain	60	63	67	71	77	80	83
Iceland	84	83	84	88	90	92	93
Norway	64	69	78	84	86	90	92
Switzerland		:	:	:	:	:	:
Croatia		:	41	45	50	56	:
Macedonia		14	:	29	42	46	:
Serbia		:	26	:	37	:	:
Turkish	8	:	20	25	30	42	:

Source: Seybert H. (2011): *Internet use in households and by individuals in 2011*. European Commission: Eurostat. 66/2011.

As a result, it may further exacerbate existing problems, particularly to expand social and economic adverse amplitudes and slow processes of regional cooperation as a result of the increasing inter and intraregional development gaps in building modern economies, based information and knowledge. ICT is increasingly seen as an effective source for inclusion and cultural transformation, if properly is directed.

It is estimated that about 120 million people in Europe have never used the internet. Europe appears geographically "digital divide", as countries such as Greece, Romania and Bulgaria, Cyprus and Portugal lag behind technological advanced countries in northern Europe. Proportion of information "uneducated" population in these countries is as follows: Romania has 53%, Bulgaria 55%, Greece 50%, Cyprus 43% and Portugal 42% population does not use Internet technology. It is estimated that in these five countries there are 25 million people who have never used the internet.

Countries with the highest proportion of Internet Falkland Islands (100%), Iceland (93%), followed by the Netherlands, Norway, Sweden, Luxembourg, Denmark (all above 90%) and Finland 84%. While the inhabitants of the Scandinavian countries have high speed (broadband) internet access, two-thirds of the Greek people do not have basic access (according to Eurostat). [3]

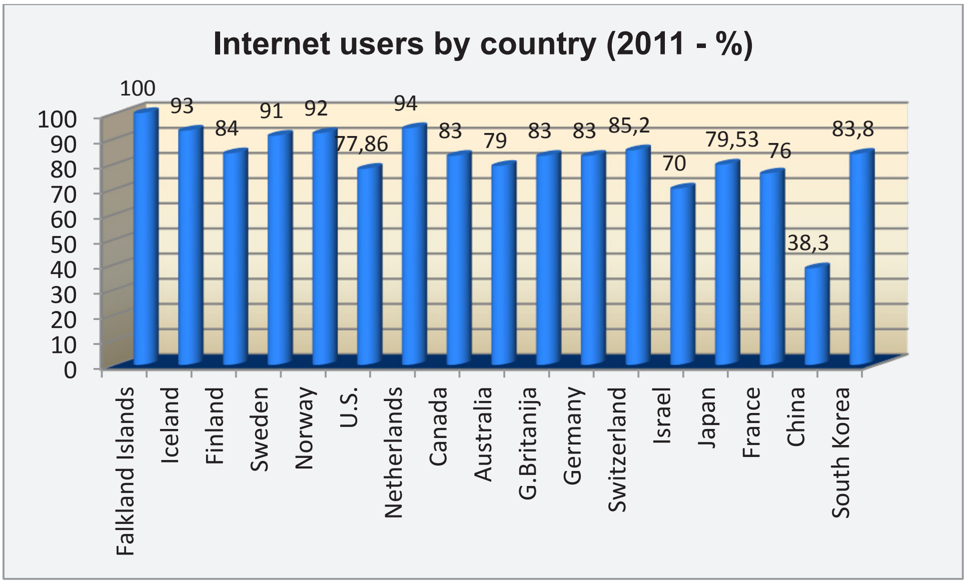


Figure 2 Internet users by country (2011 - %)

In the larger EU Member States the situation is following: In the UK 17% of the population has never used the Internet, while in Italy, Poland and Spain between 30-40% of the population stated that they do not have access to this technology (this percentage is equivalent of 49 million people used the internet). Germany in the last two years reduced the rate from 18% to 17%, France 24% Internet "illiterate" population total in these six countries accounted for 80 million.

Macedonia, unfortunately also belongs to the group of weak connected Internet technologies. According to these data is considered that 54% of Macedonia's population does not have access or do not use the internet.

In 2007, on average 97% of medium and large enterprises in the OECD use the Internet [4]. In Iceland, Finland, Switzerland, Denmark, Japan and Austria, almost 98% of companies (with more than 10 employees) use the Internet.

In last decade the share of Internet using in households are increasing. Among the countries in the OECD group average registered 58% of households with an internet connection. Evidently, young population is a driver for growth of using the IT. But in the last decade the share of the adult population in the use of Internet technology are increasing. Statistics show that in 2007 25% of the population in OECD grouping ordering goods and services online, while in Japan, 50% of the adult population uses these services. OECD countries are represented in this service by 30%, while the Nordic countries accounted for 50% in the use of electronic banking services. According J.P. Morgan e-commerce is expected in B2K to grow from $ 572 billion in 2010 to over $ 1,000 billion in 2014 (excluding travel and B2B trade). Given the magnitude of these numbers, it is clear that the digital economy is coming of age. [2]

Conclusion

Globalization and technological progress are making the old multinational structure obsolete. A multinational firm that simply links together a collection

of national businesses under a global umbrella has become anachronistic. Large international corporations are creating globally integrated organizations that can locate functions anywhere in the world to take advantage of low costs, availability of skills or access to natural resources. Advances in business analytics and information technology also make it possible to monitor performance and market developments more closely than in the past. Information and communication technologies (ICT) are considered one of the main driving forces of global economic transformation. They will shape the new economic landscape, but will also lead to the creation of a deepening divide between countries that maximum follow information and technological waves and countries that are not able to follow these developments. This digital divide is created by global technological momentum that feels both developed and emerging economies, and will reflect unfavorably to countries that do not follow "vibrating" market and the application of new information technology.

How this digital era shaped by technology and innovation, will be the flagship of the new economic developments and as nations, companies and individuals will fit into the "e-environment" depends on the dissemination of knowledge and lifelong learning.

Lastly, we should be aware that new challenges will face all entities: individuals, companies, leaders of large corporation’s states. All you need is to accept new changes and to lead the world towards a prosperous and bright future by reducing the existing political, economic and digital divisions and subdivisions. This means that the efforts of public and private sectors could be effectively combined resulting in more synergetic initiatives, with the international bodies and institutions such active drivers in the global economy.

References

1. Ali A., Hussain W., Ahmed A. (2011): *E-learning: Closing the digital gap between Developed and Developing countries.* Australian Journal of Basic and Applied Sciences, 5(2011): p. 903-908.
2. Oxford economics (2011): *The new digital economy: How it will transform business*. 2011. p.2-9.
3. Seybert H. (2011): *Internet use in households and by individuals in 2011*. European Commission: Eurostat. 66/2011.
4. OECD (2008): *The Future of the Internet Economy: a statistical profile.* OECD Ministerial Meeting on the future of the Internet economy. Seoul, Korea, 17-18 June 2008. p8
5. Дракер, П.(1991): *Иновације и предузетништво - пракса и принципи.* Београд: Привредни преглед. стр.69.
6. Koisur.(1997): *"Electronic commerce"*, Microsoft Press 1997, p.5
7. Kotler, P. and Armstrong, G. (2000) *Marketing- An introduction*. Prentice Hall, New Jersey. p.289
8. Kraus S., O' Dwyer M., Gilmore A. (2009): *Entrepreneurial Marketing*, Budapest, Hungary, 2009, p.1-2.
9. Loshin Pete, Vacca John(2004): *Electronic Commerce*, [Fourth Edition]. Hingham, Massachusetts: Charles River Media, Inc., 2004. p.3-5
10. Ruggie J., Dossal A. (200): Towards bridging the digital divide. [A discussion paper]
11. Seybert H. (2011): *Internet use in households and by individuals in 2011*. European Commission: Eurostat. 66/2011.
12. Темјановски Р.(2012). *Е-бизнис*. Штип: Универзитет„Гоце Делчев„, 2012.
13. Темјановски Р. (2008): *Претприемнички маркетинг менаџмент*. Скопје: ЕУРМ, 2008.
14. Hill, Charles W. L.(2007):*"International business: competing in the global marketplace*", 6th Edition, McGraw-Hill/Irwin, 2007, 90-91

WEB БАЗИРАН СОФТВЕР ЗА SCADA АПЛИКАЦИИ INTEGRAXOR

Марјан Стоилов[1], Василија Шарац[2,*]

[1]Прилепска пиварница дистрибутивен центар –Скопје, “Качанички пат„ б.б., 1000 Скопје, marjanstoilov@gmail.com.mk
[2]Електротехнички факултет, Универзитет Гоце Делчев, П. Фах 201, 2000 Штип, vasilija.sarac@ugd.edu.mk
** Василија Шарац, е - адреса: vasilija.sarac@ugd.edu.mk*

Апстракт. Во овој труд ќе биде претставен развој на пилот проект на SCADA софтвер базиран на web апликација преку пример на автоматизирано прозводство на слатки во една слаткарница. Самиот процес на производство се следи и контролира далечински со помош на софтверот InegraXor од било која точка во светот со користење на Interent конекција или од мобилен телефон при што предуслов е да се има Android оперативен систем. На тој начин може да се управува со самата рецептура на производството но и да се следи процесот на пакување на финалниот производ. Во овој труд апликацијата е развиена со поврзување кон одредени виртуелни портови но со редефинирање на портот може истата да биде поврзана и со реален процес преку програмибилни логички контролери (PLC) и сензори. Со развојот на микороконтролерите, сензорите и актуаторите овие апликации стануваа се поприсутни и излегуваат надвор од рамката на индустриската применливост.

Клучни зборови: системи за далечинско и дистрибуирано управување, автоматизација на производство, SCADA софтвер, web апликации

WEB BASED SOFTWARE FOR SCADA APPLICATIONS INTEGRAXOR

Marjan Stoilov[1], Vasilija Sarac [2,*]

[1]Prilepska Pivarnica Distributive Center-Skopje, St. “Kacanicki pat”, b.b., 1000 Skopje, marjanstoilov@gmail.com.mk
[2]Electrotechnical Faculty, University Goce Delcev, vasilija.sarac@ugd.edu.mk
**Vasilija Sarac, e-mail: vasilija.sarac@ugd.edu.mk*

Abstract: In this paper is presented development of pilot project of web based SCADA software. Application enables automated production of candies for one candy shop. The process of production is monitored and controlled remotely by the aid of the software IntegraXor from any part of the world where Internet connection is available or from the mobile phone in case that Android operative system is available. Consequently the recipe for production is controlled but as well as the process of final product packaging. In this paper application is developed by connecting it to virtual ports but by redefining the port itself it can by connected to the real-time process through programmable logical controllers (PLCs) and sensors. Development of microcontrollers, actuators and sensors has led to width spreading of this kind of applications and they are exceeding the frame of industrial application.

Keywords: systems for remote and distributed control, automation of production, SCADA software, web applications

22 Introduction

This paper presents the development of WEB application by using software package IntegraXor, software basically aimed for development of SCADA applications. IntegraZor is currently used in several areas of process control in thirty eight countries with the largest installations in U.K, U.S.A, Australia, Poland, Canada and Estonia. Integraxor SCADA software can be used for control of Peltier cooler a solid-state active heat pump which transfers heat from one side of the device to the other side against the temperature gradient. In this paper is presented developed application for SCADA controlled process of manufacturing of candies according to previously prescribed recipe as well as their final packing using software IntegraXor [1] . Recipe can be changed at any point of time from anywhere in the world where internet connection is available by the aid of software IntegraXor or even from the mobile phone where Android application is available. Paper presents the most important steps of software configuration and graphical animation which lead to fully configured system for control and data acquisition – SCADA. Application is developed by connecting to virtual ports but by redefining the port itself it can by connected to the real-time process through programmable logical controllers (PLCs) and sensors.

IntegraXor is web based software with option like SVG graphical visualization and animation, possibility for connection with field devices in real time with protocols like Modbus, OPC. Similar like other SCADA software it has alarms, log report, ODBC data base. It is designed by using web technologies in order to be created one complete tool for building sophisticated and intelligent real time systems. In order project to be built some pre conditions should be satisfied i.e. IntegraXor software must be installed as well as Adobe SVG viewer and Inscape SAGE. Presently IntegraXor 3.7 can be installed on Microsoft Windows XP (and latter versions) or on Microsoft Widows Server (and latter versions). Also on the computer must be available Microsoft Internet Explorer 8.0 or latter versions. Optionally as web browser can be used Mozilla Firefox 3.5 or Google Chrome 3.0. License for IntegraXor software is needed only for run-time systems. As web based product IntegraXor uses HTML and Javascript as programming language.

23 System configuration

SCADA systems are Systems for Supervisory Control and Data Acqusition, which means that these are the systems basically aimed for simultaneous measurements of process parameters, their monitoring and control. System has the functionalities of gathering process information, transmit them to the master terminal unit, conduct necessary analysis and commands and consequently display them on the computer screen (one or more). Control can be performed automatically or through interactive commands placed by the operator. System is consisted of:

- Master Terminal Unit
- Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC)
- Software for supervision and control of process information

PLC has number of available inputs/outputs (I/O) which are connected to sensors and actuators. By the aid of I/O , PLC reads the process threshold parameter, analog measured values and variables such us temperature and pressure as well as the position of rotating parts. Parameters and variables are stored in the PLC in the memory registers, each stored with the unique memory address. Data from the memory registers are available to the outside devices and systems through communication ports built into the PLC. In most common cases PLC has the nine pin serial port connected to Modbus as one of the communication protocols. Optionaly it can be Ethernet port or other field buses. IntegraXor is the tool for development of SCADA human-machine interface (HMI) and it has the communication drivers for direct data exchange with PLC through the communication port. In order IntegraXor to be connected to the PLC port must be created and it must be marked with a digital tag with adequate address of the tag for example 10001. Independently form the PLC IntegraXor can communicate with other devices such as robots and drivers which are supported by communication protocol and port. On Fig. 1 is presented basic network structure of IntegraXor.

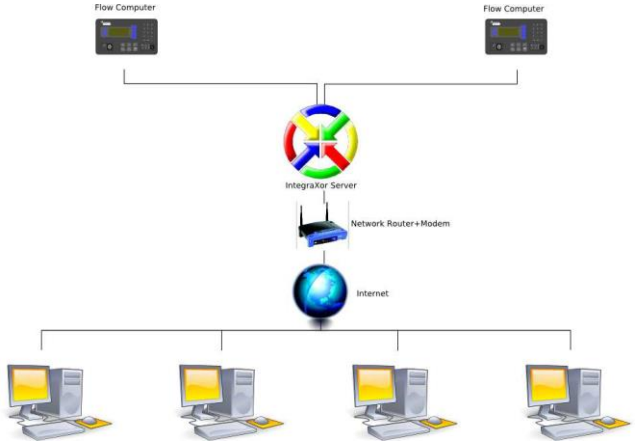


Figure 1. Basic network structure of IntegraXor

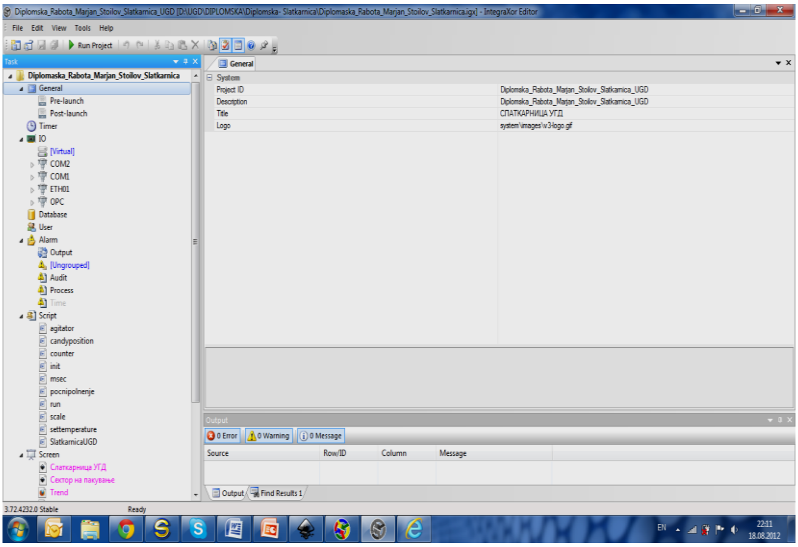
3. Software configuration

3.1 IntegraXor Editor and IntegraXor Server

IntegraXor is consisted of two programs:

- IntegraXor Server which is the operative , real-time program
- IntegraXor Editor , program where applications are created , devices are defined , connections to the process, PLCs etc.

On Fig.2 is presented basic layout of the project in IntegraXor Editor. Basic subfolder like: General, Timer, Port , Device, Tag, Database, User, Alarm, Script and Screen are defined. In “General” project name is set and web browser. Subfolder Port contains the PLC devices where tags are input. One port can have one or more devices connected to itself while one device can have from few to few thousand tags connected to the device. In subfolder Device there is a possibility to have one virtual device which is not connected to the process and allows input of tags which are not I/O. This virtual device is used for our application.


Diplomska_Rabota_Marjan_Stoilov_Slatkarnica_UGD [D:\UGD\DIPLOMSKA\Diplomska- Slatkarnica\Diplomaska_Rabota_Marjan_Stoilov_Slatkarnica.igx] - IntegraXor Editor

System
Project ID Diplomska_Rabota_Marjan_Stoilov_Slatkarnica_UGD
Description Diplomska_Rabota_Marjan_Stoilov_Slatkarnica_UGD
Title СПАТКАРНИЦА УГД
Logo system\images\w3-logo.gif

0 Error 0 Warning 0 Message

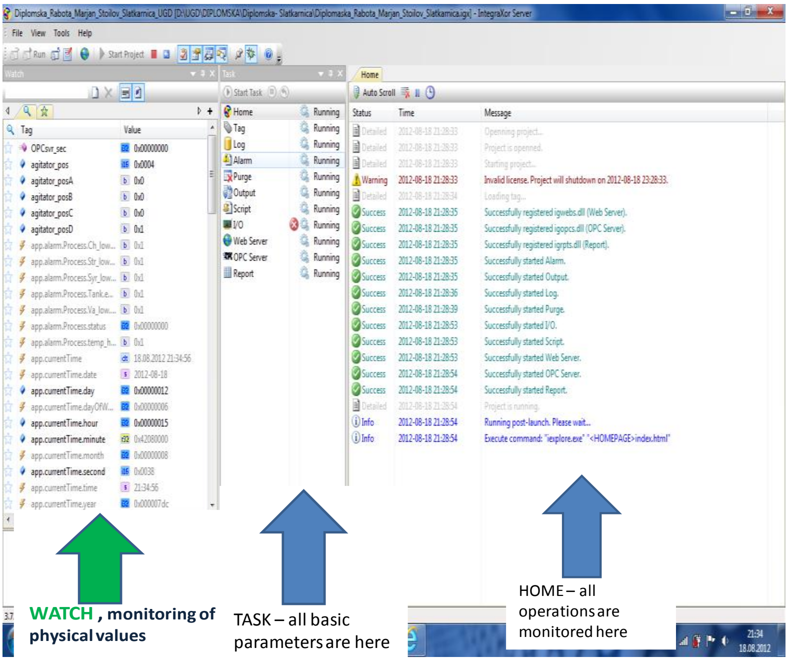
3.72.4232.0 Stable Ready

Figure 2. Window of the project in IntegraXor Editor

Tags have tree hierarchical structure. Tag is under the Device and Device is under the Port. In case that Tag should not be connected to any field device that Tag is connected to virtual device. Database is used for recording the logs (logs are all activities in the system which are recorded).The project folder generates the file with extension .mdb operating under Microsoft Acces which allows all project data and parameters to be analyzed. User subfolder creates system users which are allowed to enter the system with password. Alarms are connected with tags and their definition is according to project requirements. Program language (Script) which SCADA uses is on the base of standard JavaScript. In subfolder Screen user interface is created. For this purpose another application is used Inkscape +Sage. Inscape is software for picture editing. From project window in IntegraXor Editor the project is run by pressing the button “run project” which enables staring of IntegraXor Server which is the window for supervision and monitoring of all physical parameters (Fig. 3). IntegraXor Server enables supervision of tags for example in our application “level_syrup”. By double clicking on parameter value, the new value can be set – 10.5. If the process is stopped this value is recorded in data base.

3.2 Graphical animation

Human-machine interface (HMI) is created in program Inkscape+SAGE. It is graphical editor where numerous pre-prepared elements for graphical animation are available. For example for our reservoirs for syrup we can use rectangular element. By right click on chosen element we can select Object Properties and further on we can select “Bar” animation. In the field of “Bar” animation we input “app.currentTime.second” in the tag field. This tag “app.currentTime.second” is an internal tag which contais the time in seconds. In the field for minimum value 0 is input and in max field the value of 59. Consequently for our application four reservoirs are created with set tags in “bar” animation from minimum 0 to maximum 100. Web buttons are widely used in the animation. Most often used buttons are Start, Stop, Run, Open and Close. We will explain the process of creating the button which represents the filling of reservoir up to the value of 100. We draw rectangular



Diplomska_Rabota_Marjan_Stoilov_Slatkarnica_UGD [D:\UGD\DIPLOMSKA\Diplomska- Slatkarnica\Diplomaska_Rabota_Marjan_Stoilov_Slatkarnica.igx] - IntegraXor Server

Tag	Value
OPCsvr_sec	0x0000000
agitator_pos	0x0004
agitator_posA	0x0
agitator_posB	0x0
agitator_posC	0x0
agitator_posD	0x1
app.alarm.Process.Ch_low...	0x1
app.alarm.Process.Str_low...	0x1
app.alarm.Process.Syr_low...	0x1
app.alarm.Process.Tank.e...	0x1
app.alarm.Process.Va_low....	0x1
app.alarm.Process.status	0x0000000
app.alarm.Process.temp_h...	0x1
app.currentTime	18.08.2012 21:34:56
app.currentTime.date	2012-08-18
app.currentTime.day	0x00000012
app.currentTime.dayOfW...	0x00000006
app.currentTime.hour	0x00000015
app.currentTime.minute	0x42080000
app.currentTime.month	0x00000008
app.currentTime.second	0x0038
app.currentTime.time	21:34:56
app.currentTime.year	0x000007dc

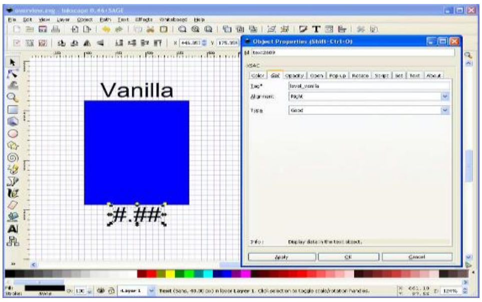
Home	Running
Tag	Running
Log	Running
Alarm	Running
Purge	Running
Output	Running
Script	Running
I/O	Running
Web Server	Running
OPC Server	Running
Report	Running

```
Status    Time                 Message
Detailed  2012-08-18 21:28:33  Openning project...
Detailed  2012-08-18 21:28:33  Project is openned.
Detailed  2012-08-18 21:28:33  Starting project...
Warning   2012-08-18 21:28:33  Invalid license. Project will shutdown on 2012-08-18 23:28:33.
Detailed  2012-08-18 21:28:34  Loading tag...
Success   2012-08-18 21:28:35  Successfully registered igwebs.dll (Web Server).
Success   2012-08-18 21:28:35  Successfully registered igopcs.dll (OPC Server).
Success   2012-08-18 21:28:35  Successfully registered igrpts.dll (Report).
Success   2012-08-18 21:28:35  Successfully started Alarm.
Success   2012-08-18 21:28:35  Successfully started Output.
Success   2012-08-18 21:28:36  Successfully started Log.
Success   2012-08-18 21:28:39  Successfully started Purge.
Success   2012-08-18 21:28:53  Successfully started I/O.
Success   2012-08-18 21:28:53  Successfully started Script.
Success   2012-08-18 21:28:53  Successfully started Web Server.
Success   2012-08-18 21:28:54  Successfully started OPC Server.
Success   2012-08-18 21:28:54  Successfully started Report.
Detailed  2012-08-18 21:28:54  Project is running.
Info      2012-08-18 21:28:54  Running post-launch. Please wait...
Info      2012-08-18 21:28:54  Execute command: "iexplore.exe" "<HOMEPAGE>index.html"
```

WATCH , monitoring of physical values
TASK – all basic parameters are here
HOME – all operations are monitored here
21:34
18.08.2012

Figure 3. Window of the project in IntegraXor Server

element. By right-clicking we select Object Properties. We select "Set" animation and we input level_vanila. In the field under name Source we input the value of 100. We use the text tool in order to give the button name "Full".



Id text2609

Tag* level_vanila

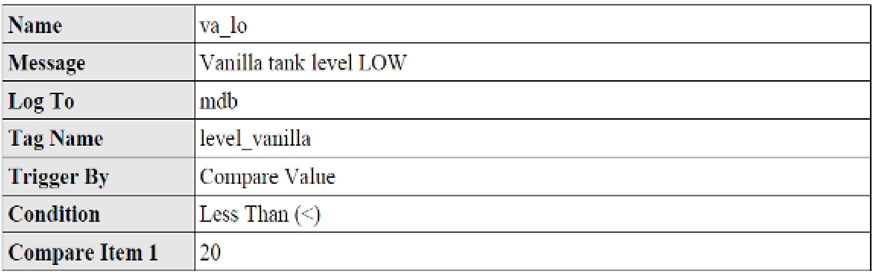
Alignment Right

Type Good

Figure 4. Window for creating graphical animation

3.3 Alarm configuration

Alarms are used in order to inform the SCADA user that allowed limit values are exceeded. Configuration of alarms is done in Project Editor. For example if level of vanilla is bellow 20, we want alarm to be switched on. In the project is input following alarm according to the description given in Figure. 5

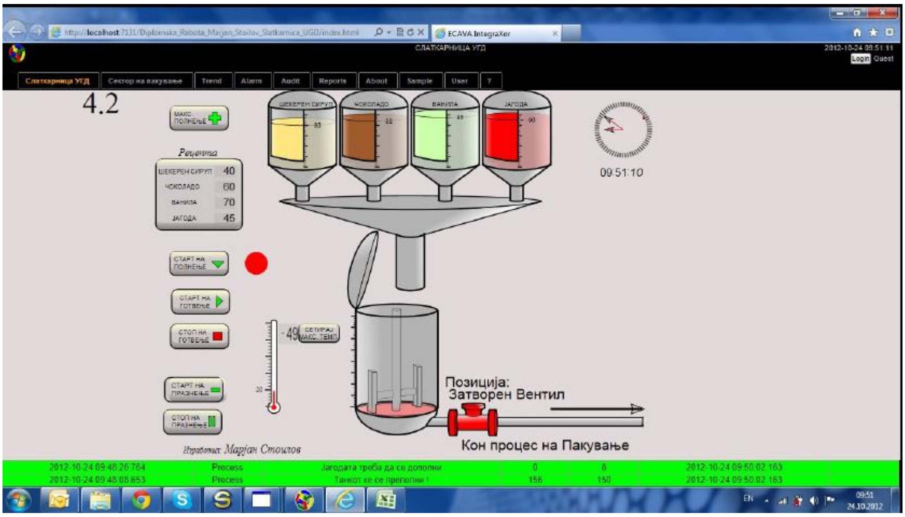


Name	va_lo
Message	Vanilla tank level LOW
Log To	mdb
Tag Name	level_vanilla
Trigger By	Compare Value
Condition	Less Than (<)
Compare Item 1	20

Figure 5. Alarm configuration

4. Results of SCADA configuration

As a result of software configuration and development of graphical application SCADA system for automated production of candies under prescribed recipe is developed [2]. On Fig. 6 is presented starting screed on our HMI in this SCADA application with four reservoirs containing different materials for cooking and we have different buttons for control of our application.



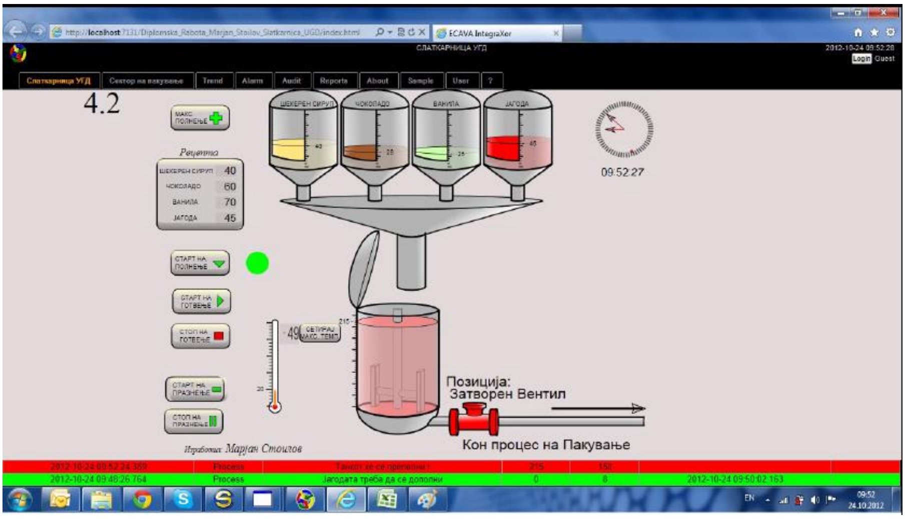
Рецепта

ШЕКЕРЕН СИРУП	40
ЧОКОЛАДО	60
ВАНИЛА	70
ЈАГОДА	45

```
2012-10-24 09:48:26.764   Process   Јагодата треба да се дополни   0     8     2012-10-24 09:50:02.163
2012-10-24 09:48:08.653   Process   Танкот ќе се преполни !        156   150   2012-10-24 09:50:02.163
```

Figure 6. HMI interface of application-starting screen

The limit values of reservoirs are set, receipt for cooking is set and by pressing the button “Start of filling” all reservoirs are filled to maximum level. In the same time tank for cooking is empty and maximum temperature for cooking is set to 49°C. By pressing the button with recipt four reservoirs are emptied according to the prescribed receipt and the adequate mix of materials is in put into the tank (Fig. 7).



Рецепта

ШЕКЕРЕН СИРУП	40
ЧОКОЛАДО	60
ВАНИЛА	70
ЈАГОДА	45

```
2012-10-24 09:52:24.369   Process   Танкот ќе се преполни !        215   150
2012-10-24 09:48:26.764   Process   Јагодата треба да се дополни   0     8     2012-10-24 09:50:02.163
```

Figure 7. HMI interface of application-start of cooking

After the main tank is filled by pressing the button “start of cooking” the tank is closed and cooking starts according to the receipt and prescribed temperature. The button “stop of cooking” stops the process of cooking. Afterwards main tank is emptied by pressing the button “Start of empting the tank”. Then main valve from Fig. 7 is opened and the main tank is emptied. So the whole process can be repeated once again for the next cycle of production with the same or adequately altered receipt.

5. Conclusion

In this paper is presented development of one SCADA application for industrial process using the application software for SCADA systems IntegraXor. Application is developed for candy factory where automatic filling of tank for cooking is performed under prescribed recipe. In order application to be developed software IntegraXor Editor is used where application is configured with all ports, alarms and parameters. Program execution is performed in software IntegraXor Server where all important parameters for the process are monitored and commands executed. Since this SCADA software is a web based application it can be used anywhere where internet connection is available, enabling fully control of industrial process from anywhere in the world, independently of the geographical position of the factory.

References

[1] T. Bah(2011): *Guide to Vector Drawing Program, 4th Edition*. Prentice Hall
[2] IntegraXor Tutorial(2008), Document nr. IGX-TUB-35RTW

БЕЗБЕДНОСТ КАЈ КОМПЈУТЕРСКИТЕ МРЕЖИ ОД АСПЕКТ НА КОНТРОЛА НА ПРИСТАП

Сашо Гелев[1]*, Јасминка Сукаровска Костадиновска[2]

*[1]Електротехнички факултет, Универзитет Гоце Делчев, П. Фах 201,
2000 Штип, saso.gelev@ugd.edu.mk*
** Сашо Гелев, е - адреса: saso.gelev@ugd.edu.mk*
[2] ул. Виенска бр. 4/10 Скопје*, jasme.sk@gmail.com*

Апстракт. Безбедноста на компјутерските мрежи е многу значаен процес, без кој во денешно време, незамисливо е функционирањето на една мрежа. Од особено значење се безбедносните услуги и механизми кои се користат за справување со различните видови на напади, како и стратегиите кои се преземаат за да се заштитат информационите системи. Контролата на пристап претставува еден механизам за определување на тоа кој има право на пристап кон определени ресурси. Таквата контрола кај компјутерските мрежи е имплементирана преку користење на повеќе методи: Access Control List – ите се темелат на дефинирани правила за пристапување, Firewall – ите чиј основен концепт на работа е на база на филтрирање на пакетите, proxy серверот кој има улога на посредник меѓу клиентот што бара услуги и другите сервери.
ISA Server – от е многу моќен Microsoft – ов производ, кој има способност да игра повеќе улоги во дадена средина. За прикажување на еден сегмент од огромниот сет на функции кои се обезбедени од ISA Server-от, практично е имплементиран ISA Server 2006 во виртуелна околина и се тестирани некои негови перформанси

Клучни зборови: ISA Server, правила на пристап, протокол, интернет сигурност

SECURITY IN COMPUTER NETWORKS FROM THE PERSPECTIVE OF ACCESS CONTROL

Saso Gelev[1]*, Jasminka Sukarovska Kostadinovska[2],
[1]*Electrotechnical Faculty, University Goce Delcev, saso.gelev@ugd.edu.mk*
*Saso Gelev, e - mail: saso.gelev@ugd.edu.mk
[2] str.Vienna no. 4/10 Skopje, jasme.sk@gmail.com

Abstract. Computer network security is a very important process, without which today we cannot imagine a fully functional network, especially without having security mechanisms and services used for handling different network attacks, and for creating strategies for securing informational systems. Access control is one of the mechanisms for granting and/or denying access to the specified resources. Such a control is implemented with using several different methods: Access Control Lists – based on defined access rules, Firewalls – for filtering incoming/outgoing packets, Proxy server – acts as a mediator between the clients and other servers.

ISA Server is a very powerful Microsoft product, capable of playing several roles in a specified deployment environment. To show a small segment of ISA Servers set of functions, ISA Server 2006 is implemented in a virtual environment and some of its performances are tested

Keywords: ISA Server, access rules, protocol, Internet security

1 Вовед

Во сите установи и компании се пропишува СИГУРНОСНА ПОЛИТИКА, односно ПОЛИТИКА НА КОРИСТЕЊЕ на Интернетот која мора да ја почитуваат сите кои се со компјутер приклучени на нејзините мрежни ресурси [3]. Сигурносните политики во деловниот свет се многу рестриктивни, се е забрането освен она што е изричито дозволено, а дозволено е само она што е неопходно за извршување на работата. Документот кој ја опишува оваа политика ќе содржи се што е потребно да се спречат инциденти: од начинот на кој, на пример, може да се влезе во управната зграда, регистрирање на влез и излез, постапка со доверливи информации и документи, па до начинот на физичка и програмска заштита на компјутерската опрема.

ISA Сервер (Internet Security and Acceleration Server) е Microsoft-ов производ, чија цел и задача се да овозможи заштита на ИТ средини од Интернет базирани закани, на начин на кој ќе им обезбеди на корисниците брз и сигурен далечински пристап до податоци и апликации [6]. ISA Серверот е наследник на Microsoft Proxy Server 2.0 и претставник на Microsoft за мрежна поддршка.

Она што е од особен интерес во врска со темата која е обработена во овој труд, секако е можноста која ISA серверот ја дава на администраторите, за креирање на политики за регулирање на користењето, зависно од корисник, група, дестинација, апликација, распоред и критериуми за типот на содржината.

ISA Серверот доаѓа во две изданија и тоа Standard Edition и Enterprise Edition.

2 INTERNET SECURITY

Може да се нагласат некои случаи на примена како што се:

- *Одбрана од надворешни и внатрешни веб базирани закани.* Создаден е да дава посилна безбедност при управување и заштита на мрежите.
- *Безбедност при објавувањето на содржината за далечински пристап.* Го олеснува далечинскиот пристап до корпоративните податоци, ресурси и апликации.
- *Безбедно поврзување на експозитури.* Овозможува лесна и ефективна site-to-site конекција помеѓу експозитурите и заштеда на пропусен опсег, преку кеширање и компресија на податоци.

Поставување стратегии на ISA SERVER 2006

Она што ISA Серверот го прави производ кој може да се издвои од останатите производи, е неговата способност да игра повеќе улоги во дадената средина[2]. Некои од тие улоги се следните: ISA Server-от како целосно функционален firewall на апликациско ниво, можноста за веб кеширање, поддршката на VPN, reverse proxy како и комбинации на било кои од овие работи.

Употреба на ISA SERVER 2006 како дополнителна заштита на веќе заштитени средини

Кога дадена организација веќе користи некаков вид на безбедносна технологија, ISA Server-от може да биде додаден како дополнителен слој на сигурност. Ова е добродојдена можност за подобрување на безбедноста на многу од организациите[1].

Еден пример на одлична интеграција на ISA Server-от е во мрежа со веќе постоечки firewall, каде е дополнителен слој на безбедност, користејќи ги своите функции на reverse proxy или доделен VPN сервер. Исто така, ISA Server-от може да се интегрира и во околини кои користат Remote Authentication Dial-In User Service (RADIUS).

ACCESS RULES

Кога станува збор за функционалноста на правилата за вмрежување кои се користат кај ISA серверите и опишувањето на дозволените комуникации помеѓу дефинираните мрежи, постојат три групи на листи на правила.

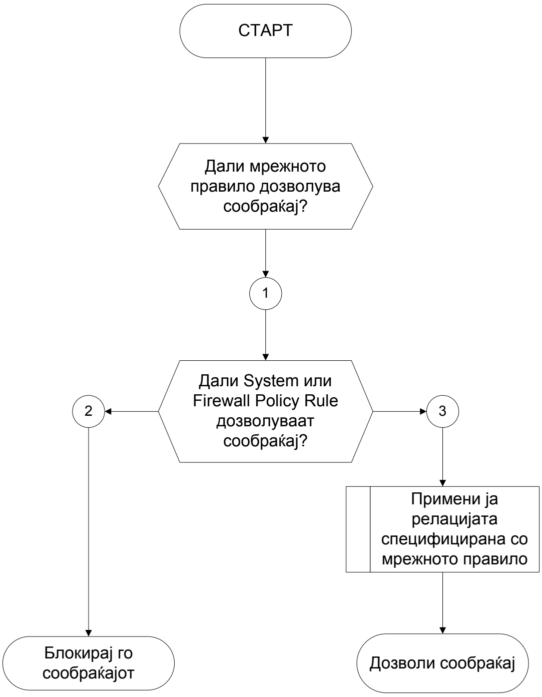
- **Мрежни правила:** Оваа листа ја опишува и дефинира топологијата на мрежата. Овие правила ја дефинираат врската помеѓу мрежните ентитети и типот на дефинираниот однос. Мора да бидат јасно и коректно дефинирани мрежните објекти и нивните меѓусебни релации, затоа што тоа е од исклучително значење за целокупната работа на ISA серверот.
- **System policy rules:** Оваа листа содржи 30 вградени правила за пристап и сите тие се применети на Local Host мрежата. Тие ги контролираат комуникациите од и до ISA серверот и се потребни за извршување на функции како што се автентикација, мрежна дијагностика, logging и далечинско управување.
- **Firewall policy rules:** Оваа листа содржи правила кои ги дефинира firewall администраторот. Ова е листа која содржи три можни видови на правила: access rule, web publishing rule и server publishing rule. Оваа листа вклучува и едно специјално

предефинирано правило Last, кое го блокира целиот пристап до и од сите мрежи. Ова стандардно правило не може да биде изменето или избришано. Затоа, секое блокирање или овозможување на сообраќајот со ISA серверот е дефинирано со правила.

Со следниот дијаграм (слика 1) е дадено како ISA серверот ги применува правилата над трите листи при било кое излезно барање.

Кога правилата на пристап се поклопуваат со параметрите на барањето, тоа значи дека се применува тоа правило и ISA серверот не одговара на барањето на други правила. Овде се појавува прашањето, кога правилото на пристап се поклопува со бараните параметри. ISA серверот го применува правилото, после извршената проверка на некои критериуми, кои се одвиваат по следниот редослед:

1. **Протокол:** Еден или повеќе дефинирани протоколи со излезна насока за примарна конекција.
2. **Од (извор):** Еден или повеќе мрежни објекти кои можат да вклучат Network, Network Sets, Computers, Computer Sets, Address Ranges и Subnets.
3. **Распоред:** било кој дефиниран распоред.
4. **До (дестинација):** еден или повеќе мрежни објекти кои вклучуваат Network, Network Sets, Computers, Computer Sets, Address Ranges, Subnets, Domain Name Sets и URL Sets.
5. **Content group:** Секој тип на содржина кој е дефиниран во сетот.


СТАРТ
Дали мрежното правило дозволува сообраќај?
1
Дали System или Firewall Policy Rule дозволуваат сообраќај?
2
3
Примени ја релацијата специфицирана со мрежното правило
Блокирај го сообраќајот
Дозволи сообраќај

Слика 1 Дијаграм за примена на правилата од страна на ISA Server 2006

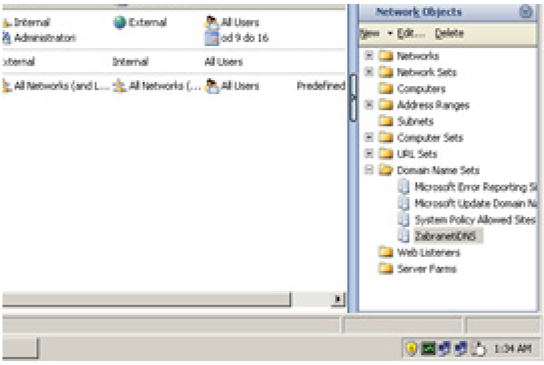
3 ЕКСПЕРИМЕНТАЛЕН ДЕЛ

Идејата за експериментот е добиена од креирањето на правила за пристап, на ISA Server, а за таа цел инсталиран е ISA Server 2006 на виртуелен PC. Исто така инсталиран е и Microsoft Windows Server 2003 R2 со Routing and Remote Access Service и VPN и со две мрежни карти, едната LAN, а другата WAN. Алатка која е користена за креирање на тест процедурата е Microsoft Visual Studio 2008, Professional Edition.

Сценарио

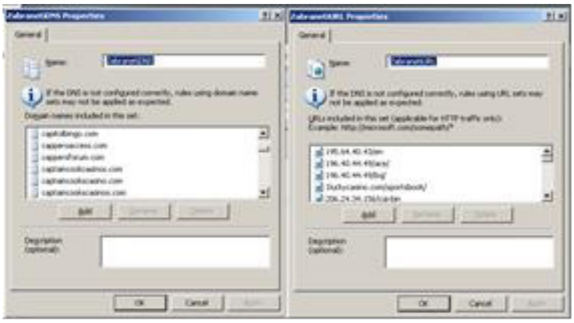
Една од многуте опции кои ги нуди ISA Server-от кога е во прашање контролата на пристап е забрана и дозвола на определени сајтови и домени. Кога е потребно да се направи забрана за неколку сајтови или домени, тоа може мануелно да се конфигурира. Се поставува прашањето што ќе се случи ако е потребно да се забранат голем број (илјадници), како на пример цели листи на блокирани сајтови. Би било премногу неблагодарно ако тие се внесуваат мануелно како што е претходниот случај. ISA Server-от има решение за ваквиот проблем и сето тоа би се направило со само неколку минути работа. Се користат VB скрипти кои што читаат од текстуална датотека исполнета со имиња на домени кои сакаме да ги блокираме и истите ги додава во *Domain Name Set*–от или *URL Set*-от, претходно дефинирани на ISA Server-от. Скриптите кои се користени, се од сајтот http://technet.microsoft.com/hiin/library/cc302454%28en-us%29.aspx. [4] Користени се два типа на VB скрипти, една за додавање на *Domain Name*, а друга за додавање на *URL*. Синтаксата за користење на скриптите е следна:

AddListToDomainNameSet.vbs domains.txt ZabranetiDNS
AddUrlsToUrlSet.vbs urls.txt ZabranetiURL



Слика 2 Скрипти Забранети URL и Забранети DNS

Со користење на претходните скрипти се врши полнење на ZabranetiDNS и ZabranetiURL, што може да се види на следната слика


ZabranetiDNS Properties

Name: ZabranetiDNS

If the DNS is not configured correctly, rules using domain name sets may not be applied as expected.

Domain names included in this set:

captolbingo.com
capperaccess.com
cappersforum.com
captaincookcasinos.com
captaincookscasino.com
captaincookscasinos.com

Description (optional):

ZabranetiURL Properties

Name: ZabranetiURL

If the DNS is not configured correctly, rules using URL sets may not be applied as expected.

URLs included in this set (applicable for HTTP traffic only):
Example: http://microsoft.com/somepath/*

195.64.40.43/en
196.40.44.49/aro/
196.40.44.49/bg/
Duchycasino.com/sportsbook/
206.24.34.156/carbn

Description (optional):

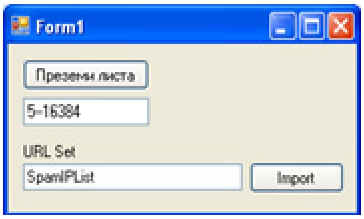
Слика 3 Полнење на листитеЗабранети URL и Забранети DNS

Од практични причини, целиот овој процес на полнење згодно би било да се автоматизира. Еден начин е со користење на Windows Service кој ќе ги „собира“ веб локациите или IP адресите и автоматски ќе ги импортира. За тоа, може да се искористи креираната програма изработена во C#, која од некој извор, превзема листа од IP адреси. Во случајов користена е листа на IP адреси контролирани од спамери, која преку програмата, автоматски се импортира во URL Set –от.

Тест процедура

На ISA Server-от се креира URL Set со име SpamIPList.

Програмата за тестирање превзема листа од адресата: http://www.spamhaus.org/drop/drop.lasso. [7]. Листата се состои од цели IP адреса/ранг. Од листата се издвојуваат 5 линии и се запишуваат во текстуална датотека IPList.txt. Потоа се наведува името на URL сетот каде што сакаме да ја импортираме листата.



5-16384

URL Set: SpamIPList

Слика 4 Форма дефинирање на URL сетот каде ќе се импортира листата

Понатаму, автоматски се извршува .vbs скриптата со параметри: креираната датотека IPList.txt и зададеното име на URL сетот. На ISA Server-от се проверува дали се импортирани IP адресите.

Резултати

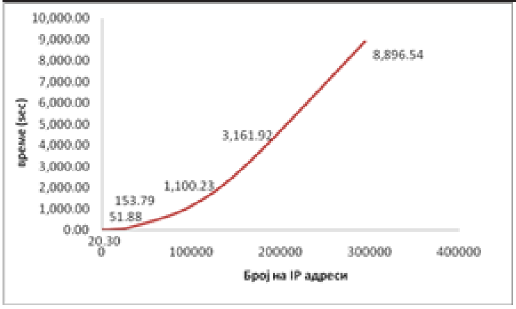
Со повеќекратно извршување на тест процедурата за различен број на линии од листата, соодветно се добиваат резултати за бројот на IP адреси и времетраењето на импортирањето на истите во URL Set-от на ISA Server-от. Целта на тестирањето е да се покаже дека оваа постапка успешно ги импортира IP адресите, но проблем се појавува при времетраењето на импортот за голем број на адреси. Овие резултати се добиени на машина со послаби хардверски карактеристики, но реално серверите имаат подобри карактеристики.

По извршеното тестирање, добиени се следните резултати:

Табела 1 бројот на IP адреси и времетраењето на импортирањето на истите во URL Set-от на ISA Server-от.

Број на линии	Број на адреси	Време за импорт
1	1024	00:00:20.31
2	2048	00:00:21.82
3	6144	00:00:23.47

4	14336	00:00:51.88
5	16384	00:00:54.02
6	32768	00:02:33.79
7	98304	00:18:20.23
8	163840	00:52:41.92
10	294912	02:28:16.54



Слика 5 Графички приказ на резултатите

4 ЗАКЛУЧОК

Предноста со ваквото ажурирање на листите е автоматизмот. Изворниот код од програмата може да се искористи за креирање на Windows Service, со што би се придонело за постојано ажурирање. Потребно е да се истакне дека, постојат провајдери кои нудат сервиси за автоматско превземање на листите, така што со претходна регистрација и претплата, може да се дојде до истите.

Од друга страна, како што може да се види од резултатите, стапката на раст на временската сложеност при пресметувањето е многу висока кога се извршува импортирање на голем број на IP адреси во URL Set – от на ISA Server-от. Тоа е негативност на ваквиот пристап. Уште една негативна страна е тоа што не е овозможено едитирање на постоечка листа, со што би се намалило времето и потрошувачката на ресурси при импортирање на истата. Веројатно, поправилен пристап за администрирање и менаџирање на ISA Server-от е користењето на неговиот SDK (Software Development Kit) со што би се забрзала постапката и би се овозможило поедноставно ажурирање.

На крај, сакам да нагласам дека во овој експеримент е земена листа на IP адреси контролирани од спамери, но може да се земе тоа да биде листа на домени или URL листи.

ЛИТЕРАТУРА

[1] Michael Noel, *Microsoft ISA Server 2006 Unleashed,* 2008 by Sams Publishing

[2] Dr.Thomas W. Shinder, Debra Littlejohn Shinder, *How to Cheat at Configuring ISA Server 2004*, Syngress Publishing Inc. 2006

[3] Сашо Гелев, Интернет Технологии, ЕУРМ 2010

[4] http://technet.microsoft.com/enus/library/cc302621.aspx

[5] http://www.portcullissystems.com/index.php?option=com_content&view=article&id=73:isa&catid=14:test1&Itemid=125

[6] http://www.microsoft.com

[7] http://www.spamhaus.org/drop/drop.lasso

FREQUENCY DISTRIBUTION OF LETTERS, BIGRAMS AND TRIGRAMS IN THE MACEDONIAN LANGUAGE

Aleksandra Mileva[1]*, Stojanče Panov[1], Vesna Dimitrova[2]

1Faculty of Computer Science, "Goce Delčev" University in Štip,
Republic of Macedonia
e-mail: aleksandra.mileva@ugd.edu.mk, stojance.10139@student.ugd.edu.mk

2Faculty of Computer Science and Engineering, "Ss. Cyril and Methodius" University in Skopje, Republic of Macedonia
e-mail: vesna.dimitrova@finki.ukim.mk

Abstract: Frequency analysis in cryptanalysis is based on the fact that, in any given piece of written text, certain letters and combinations of two or three letters occur with varying frequencies. In this paper we present average frequency distribution of letters, bigrams and trigrams in the Macedonian language. Letter frequency of the most common first letter and last letter in words is also given. Our results are based on approximately 15000 pages of written text from the following subjects: poetry, prose, drama, natural sciences, social sciences, law, different laws, economy, and computer science. Obtained letter frequency sequence is "А О И Е Т Н Р С В Д К Л П М У З Ј Г Б Ч Ш Ц Ж Њ Ф Ќ Х Ѓ Џ Љ Ѕ", the most common letter pairs are "НА АТ ТА НИ ТЕ РА ОТ СТ ТО КО" and the most common trigrams are "ИТЕ АТА УВА ИЈА АЊЕ СТА ОСТ ВАЊ ПРО ПРЕ".

Keywords: frequency distribution of letters, bigrams, trigrams, Macedonian language.

24 Introduction

Frequency analysis is a cryptanalysis's tool for breaking classical ciphers. It studies frequencies of letters and group of letters in a given ciphertext. For example, if you have got a message encrypted using the simple substitution cipher that you want to break, you can use frequency analysis. Each letter of the plaintext is replaced with another, and any particular letter in the plaintext will always be transformed into the same letter in the ciphertext. You can still recognise the original letter, because the frequency characteristics of the original letter will be passed on the new letters. Usually, cryptanalyst may need to try several combinations of mappings between ciphertext and plaintext letters, before he/she discovers the original plaintext.

Letter frequencies are also important for design of some keyboard layouts like Dvorak Simplified Keyboard, for several games like Scrable, for data-compression techniques such as Huffman coding, etc.

Letter frequencies for the English can be found in several sources, like [1, 2], for German in [3], for Spanish in [4], for Italian in [5], etc. The absence of similar results for the Macedonian language was our basic motivation for this study.

25 Letter frequency distribution

In our experiments, we use approximately 15000 pages of written text, or more accurate: 2000 pages of prose and poetry, 1700 pages of drama, 2000 pages of natural sciences (geology, mining, geography, etc), 1400 pages of social sciences (history, pedagogy, etc), 1400 pages of law, 3000 pages of different laws, 1600 pages of economy and 2000 pages of computer science.

Obtained results for Macedonian letter frequency distribution are given in Table 1. Obtained relative frequencies of letters, ordered by Macedonian alphabet and by frequencies, are shown on Figure 1 and 2, respectively.

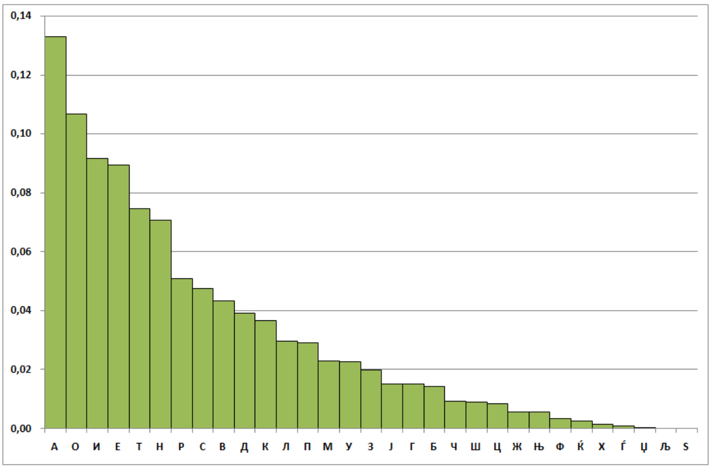


Figure 1 Relative frequencies of letters in text

Table 1 Macedonian letter frequency

Letter	Count	Frequency
А	3.819.909	13,293%
О	3.068.901	10,679%
И	2.632.308	9,160%
Е	2.570.604	8,945%
Т	2.144.354	7,462%
Н	2.033.735	7,077%
Р	1.462.718	5,090%
С	1.365.208	4,751%
В	1.247.904	4,343%
Д	1.123.847	3,911%
К	1.055.096	3,672%
Л	850.394	2,959%
П	840.787	2,926%
М	663.552	2,309%
У	649.953	2,262%
З	568.707	1,979%
Ј	434.240	1,511%
Г	432.547	1,505%
Б	412.019	1,434%
Ч	265.775	0,925%
Ш	263.335	0,916%
Ц	246.244	0,857%
Ж	163.334	0,568%

Њ	159.379	0,555%
Ф	99.687	0,347%
Ќ	75.905	0,264%
Х	41.978	0,146%
Ѓ	30.340	0,106%
Џ	7.086	0,025%
Љ	4.252	0,015%
S	2.708	0,009%

Note that, these frequencies are averages, that means that letter A will not always constitute 13,293% of all the letters in a text, and may not even be the most common letter. If you analyse just one sentence, its letter frequency distribution probably will not match the bar chart above. But if you pick a longer Macedonian text, the match should be surprisingly good.

By analysing Table 1, one can see that the “top twelve” letters comprise about 81,3% of the total usage and the “top eight” letters comprise about 66,5% of the total usage.

Recent analysis show that letter frequencies, tend to vary by subject. In the Table 2 and on the Figure 3 we give the letter frequency distribution by examined subjects.

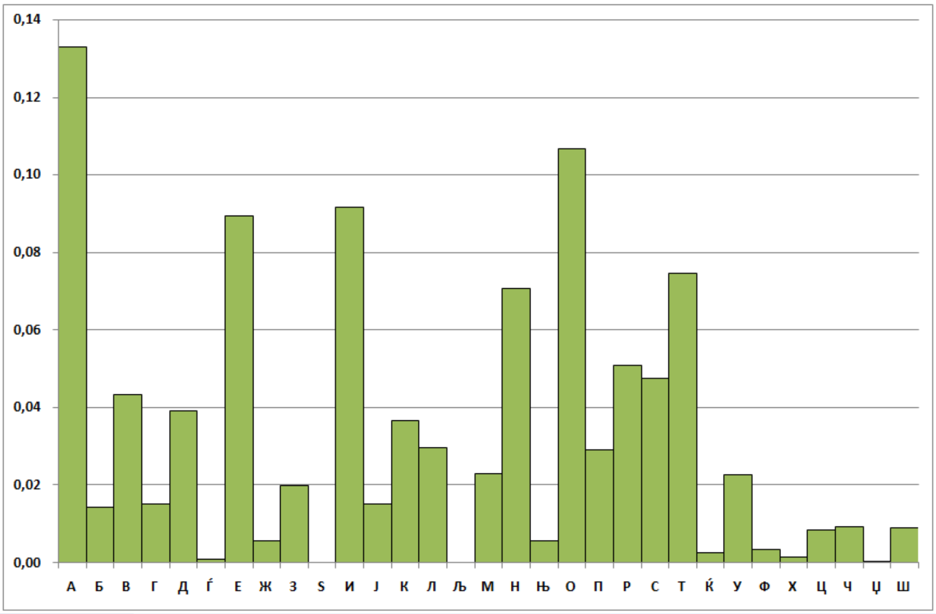


Figure 2 Relative frequencies ordered by frequency

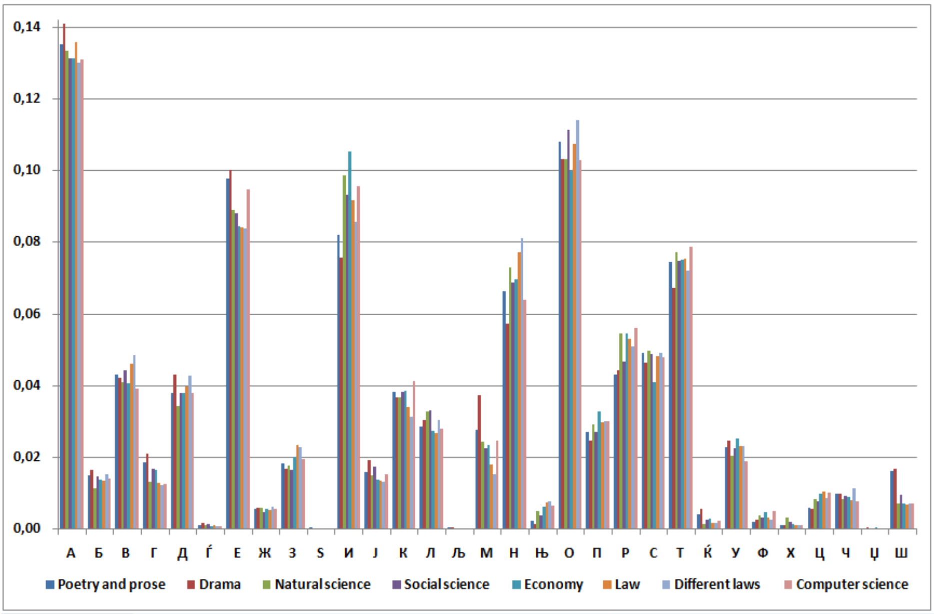


Figure 3 Relative frequencies of letters in text by subjects

Table 2 Macedonian letter frequency by subjects

L.	**Frequency for poetry and prose**	**Frequency for drama**	**Frequency for natural science**	**Frequency for social science**	**Frequency for economy**	**Frequency for law**	**Frequency for different laws**	**Frequency for computer science**
А	13,507%	14,081%	13,341%	13,129%	13,127%	13,591%	13,000%	13,099%
Б	1,508 %	1,647 %	1,142 %	1,480 %	1,387 %	1,363 %	1,519 %	1,408 %
В	4,296 %	4,225 %	4,098 %	4,436 %	4,070 %	4,618 %	4,844 %	3,914 %
Г	1,869 %	2,102 %	1,314 %	1,688 %	1,650 %	1,290 %	1,232 %	1,274 %
Д	3,805 %	4,298 %	3,435 %	3,783 %	3,789 %	3,988 %	4,272 %	3,786 %
Ѓ	0,126 %	0,169 %	0,122 %	0,135 %	0,095 %	0,118 %	0,068 %	0,068 %
Е	9,785 %	10,007%	8,912 %	8,819 %	8,451 %	8,418 %	8,386 %	9,480 %
Ж	0,574 %	0,604 %	0,592 %	0,483 %	0,561 %	0,532 %	0,622 %	0,569 %
З	1,821 %	1,672 %	1,762 %	1,656 %	2,016 %	2,338 %	2,281 %	1,970 %
Ѕ	0,038 %	0,017 %	0,006 %	0,012 %	0,008 %	0,000 %	0,002 %	0,003 %
И	8,215 %	7,579 %	9,863 %	9,311 %	10,545%	9,168 %	8,580 %	9,578 %
Ј	1,582 %	1,926 %	1,514 %	1,755 %	1,380 %	1,337 %	1,326 %	1,521 %
К	3,839 %	3,682 %	3,666 %	3,832 %	3,860 %	3,406 %	3,129 %	4,144 %
Л	2,866 %	3,051 %	3,281 %	3,302 %	2,746 %	2,677 %	3,046 %	2,786 %
Љ	0,045 %	0,047 %	0,013 %	0,016 %	0,007 %	0,002 %	0,004 %	0,006 %
М	2,773 %	3,742 %	2,453 %	2,271 %	2,353 %	1,790 %	1,543 %	2,481 %

Н	6,644%	5,744%	7,306%	6,865%	6,958%	7,736%	8,114%	6,407%
Њ	0,239%	0,130%	0,512%	0,398%	0,620%	0,749%	0,792%	0,657%
О	10,811%	10,315%	10,323%	11,135%	9,985%	10,742%	11,401%	10,300%
П	2,722%	2,455%	2,912%	2,703%	3,289%	2,982%	3,024%	3,024%
Р	4,303%	4,436%	5,448%	4,679%	5,464%	5,311%	5,095%	5,601%
С	4,902%	4,653%	4,971%	4,888%	4,084%	4,814%	4,910%	4,794%
Т	7,456%	6,726%	7,732%	7,494%	7,507%	7,543%	7,220%	7,866%
Ќ	0,410%	0,556%	0,146%	0,272%	0,280%	0,187%	0,166%	0,242%
У	2,292%	2,469%	2,039%	2,263%	2,527%	2,328%	2,317%	1,904%
Ф	0,214%	0,270%	0,380%	0,320%	0,463%	0,311%	0,263%	0,513%
Х	0,119%	0,118%	0,324%	0,200%	0,131%	0,114%	0,114%	0,099%
Ц	0,585%	0,562%	0,827%	0,777%	0,989%	1,043%	0,869%	1,015%
Ч	0,993%	0,983%	0,849%	0,919%	0,894%	0,797%	1,128%	0,770%
Џ	0,032%	0,063%	0,007%	0,026%	0,053%	0,013%	0,010%	0,011%
Ш	1,629%	1,672%	0,708%	0,952%	0,710%	0,693%	0,724%	0,710%

26 Bigram and trigram frequency distribution

For cryptanalysis, more complex use of statistics can be achieved made, such as considering frequency of pairs of letters (digrams or bigrams or digraphs), triplets (trigrams), and so on. This provide more information to the cryptanalyst, for instance, Њ and Е nearly always occur together in that order in Macedonian language, even though Њ itself is rare.

Bigram and trigram frequency distribution for Macedonian language are presented in Table 3. “Top twenty” bigrams in Macedonian language comprise about 31,2% of the total usage and “top ten” bigrams comprise about 18,3% of the total usage.

Table 3 “Top thirty” bigrams and trigrams in Macedonian language ordered by frequencies

Bigrams	Count	Frequency
НА	752.140	3,235%
АТ	432.434	1,860%
ТА	420.266	1,808%
НИ	410.148	1,764%
ТЕ	399.981	1,721%
РА	392.436	1,688%
ОТ	375.777	1,616%
СТ	375.112	1,614%
ТО	358.245	1,541%
КО	338.492	1,456%
ВА	338.320	1,455%
ВО	335.956	1,445%
ЕН	328.730	1,414%
ОД	319.684	1,375%
ПР	295.522	1,271%
РЕ	286.956	1,234%
КА	282.442	1,215%
ИТ	278.301	1,197%
ПО	276.883	1,191%
НО	269.854	1,161%
ЗА	261.579	1,125%
ДА	228.540	0,983%
ЈА	228.029	0,981%
СЕ	222.786	0,958%
УВ	209.417	0,901%
РИ	207.967	0,895%
ОВ	206.159	0,887%
ТИ	203.082	0,874%
ЛИ	199.693	0,859%
РО	195.123	0,839%

Trigrams	Count	Frequency
ИТЕ	227.851	1,261%
АТА	207.369	1,147%
УВА	203.097	1,124%
ИЈА	128.096	0,709%
АЊЕ	115.397	0,639%
СТА	110.629	0,612%
ОСТ	104.699	0,579%
ВАЊ	87.284	0,483%
ПРО	86.551	0,479%
ПРЕ	86.010	0,476%
ЕТО	77.521	0,429%
ИСТ	74.462	0,412%
РЕД	73.494	0,407%
АКО	73.165	0,405%
НАТ	71.059	0,393%
ИРА	66.287	0,367%
ШТО	65.471	0,362%
НОС	64.349	0,356%
ЕНИ	64.270	0,356%
АНИ	62.884	0,348%
ПРИ	61.401	0,340%
ИОТ	59.740	0,331%
НИТ	59.468	0,329%
ОТО	58.371	0,323%
ААТ	57.511	0,318%
ОВИ	55.883	0,309%
РАН	55.117	0,305%
ИНА	55.035	0,305%
СКИ	53.291	0,295%
МЕН	52.775	0,292%

"Top twenty" trigrams in Macedonian language comprise about 11,3% of the total usage and "top ten" bigrams comprise about 7,5% of the total usage.

9 Letter frequency distribution from the Macedonian dictionary

We examined also the Macedonian letter frequency distribution for more than 80000 Macedonian basic words from the Macedonian dictionary [6, 7, 8, 9]. Obtained results are given in Table 4.

Another interesting analysis about letters is the letter frequency of the most common first letter in words and most common last letter in words. We use the same sample from the dictionary for this analysis, and results are presented in Table 5. It is interesting that approximately 73% of all the examined words finished with a vocal. In 27,327% of examined words that vocal is А, and in 22,581% the vocal is И. The most frequent first letter in word with 23,880% is П.

Table 4 Macedonian letter frequency for words in the Macedonian dictionary.

Letter	Count	Frequency
А	92.952	12,996%
И	61.135	8,548%
Е	59.170	8,273%
О	52.885	7,394%
Р	47.300	6,613%
В	40.902	5,719%
Н	38.244	5,347%
У	34.068	4,763%
Т	32.226	4,506%
П	31.793	4,445%
С	31.193	4,361%
К	26.045	3,642%
Л	23.945	3,348%
Д	19.002	2,657%
З	17.290	2,417%
Ј	16.998	2,377%
М	14.103	1,972%
Ќ	11.233	1,571%
Њ	10.807	1,511%

Б	10.620	1,485%
Г	10.058	1,406%
Ч	9.690	1,355%
Ш	6.660	0,931%
Ц	6.415	0,897%
Ж	4.046	0,566%
Ф	3.018	0,422%
Х	1.281	0,179%
Џ	793	0,111%
Ѓ	545	0,076%
Ѕ	478	0,067%
Љ	327	0,046%

Table 5: Letter frequency of the most common first and last letter in words.

First letter		**Last letter**	
Letter	**Frequency**	**Letter**	**Frequency**
П	23,880%	**А**	27,327%
С	8,769%	**И**	22,581%
Н	6,901%	**Е**	19,262%
З	6,220%	**Н**	7,562%
Р	5,814%	**Т**	6,023%
К	5,458%	**О**	3,733%
О	5,127%	**К**	2,648%
Д	4,294%	**Р**	2,520%
И	3,974%	**В**	1,746%
Б	3,607%	**М**	1,205%
В	3,446%	**Л**	0,894%
М	3,251%	**Ц**	0,828%
Т	2,742%	**Ч**	0,651%
Г	2,564%	**С**	0,615%
А	2,092%	**Д**	0,444%
У	1,612%	**Г**	0,380%
Л	1,513%	**Ј**	0,269%
Ш	1,489%	**П**	0,241%
Ф	1,256%	**Ш**	0,212%
Е	1,182%	**З**	0,209%

Ч	1,097%	**Ж**	0,155%
Ц	0,920%	**Ф**	0,150%
Х	0,724%	**У**	0,114%
Ж	0,723%	**Б**	0,097%
Ј	0,521%	**Х**	0,073%
Џ	0,274%	**Ќ**	0,023%
Ѕ	0,180%	**Љ**	0,018%
Ќ	0,175%	**Џ**	0,009%
Ѓ	0,130%	**Њ**	0,007%
Љ	0,057%	**Ѓ**	0,004%
Њ	0,009%	**Ѕ**	0,000%

10 Conclusion

In this paper we investigate the frequency distribution of letters, bigrams and trigrams in the Macedonian language and in the Macedonian dictionary, too. We investigate, letter frequency of the most common first letter and last letter in basic words from the Macedonian dictionary, also.

References

[1] H. S. Zim (1962): *Codes and secret writing*. Scholastic Book Services.

[2] H. Beker and F. Piper (1983): *Cipher Systems: The Protection of Communications*, John Wiley & Sons, pp. 397.

[3] A. Beutelsacher (2005): *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Ohne alle Geheimniskrämerei, aber nicht ohne hinterli ... utzen und Ergötzen des allgemeinen* Publikums, Aufl., Wiesbaden: Vieweg Verlagsgesellschaft, pp.10.

[4] F. Pratt (1939): *Secret and Urgent: the Story of Codes and Ciphers*, Blue Ribbon Books, pp 254-255.

[5] S. Singh (1999): *Codici e Segreti*, RCS.

[6] A. Petrovski (2005): *About a Macedonian Computational Dictionary*, Proceedings of 2nd Balkan Conference in Informatics BCI 2005, Ohrid, 17-19 November, pp. 76-83.

[7] K. Zdravkova and A. Petrovski (2007): *Derivation of Macedonian Verbal Adjectives*, International Conference RANLP, Borovets, 27-29 September, Incoma, Ltd, pp. 661-665.

[8] K. Zdravkova (2007-2008): *Создавање компјутерски ресурси за македонскиот јазик*, Македонски јазик, Институт за македонски јазик „Крсте Мисирков“, година LVIII-LIX, pp. 153-174.

[9] T. Erjavec (2010): *MULTEXT-East Version 4: Multilingual Morphosyntactic Specifications, Lexicons and Corpora*, Proceedings of the International Conference on Language Resources and Evaluation, LREC 2010, 17-23 May, Valletta, Malta, pp. 2544-2547.

TOWARDS A GENERIC METADATA MODELING

Pavel Saratchev[1]

[1]*Technical University of Sofia, PhD Student, pavel.saratchev@triwdata.com*

Abstract: This document describes the creation of a generic metadata model prototype, combining the principles of Generic Modeling and Data Vault architectures.

Keywords: Generic, Metadata, Modeling.

27 Introduction

Metadata is essential component for the correct operation and further development of a BI/DWH-system. Despite this fact, most organizations do not have centralized processing and management of metadata. The main reasons for this fact are defined as:

- no established standards[13] - every software vendor has its approach to the preservation and management of metadata.
- additional resources and investments - resulting from a complex concept and implementation for centralized management of metadata.
- lack of clear understanding about the benefits which could bring a centralized management of the metadata.

For the reasons above, the goal of this paper is to design and implement a prototype for a generic metadata model which can be used for the creation of central repository for management of metadata with the following characteristics:

- universal model which can accept any type of metadata and so give a single point of view over all objects, business rules, processes and their dependencies throughout the systems in the organization.
- optimized and flexible structure with relative small amount of tables, which will facilitate the maintenance and reduce the costs of ownership.
- historization of the metadata with the ability to track changes and recover old versions of the data.

28 Conception

Meta data is often defined as “data about data”. This definition is rather abstract and can be interpreted differently in different context. But at this ambiguous aspect of the definition are expressed its accuracy and content. This is data that emerge from the modeling of certain objects and links between them in a given abstraction level and context. The model in every subsequent abstraction level is the meta model of the previous one. On fig. 1 is presented the dependence of models and meta data at various abstraction levels.

The real objects exist in the real world of abstract level 0. The model of the real object is abstract (simplified) image for a particular purpose[14] in a given context. With the modeling of real objects in the first abstraction level a

[13] Metadata standards: DDI, ISO 19115, ISO 19506, ISO 23081, MARC, CWM and many others.

[14] The purpose of modeling can be simulation, explanation, etc.

model 1 was created, which consists of metadata about the real object. A consequent modeling of the model 1 at the second level is a model 2, which in turn consists of a metadata from model 1. In the context of a real object, model 2 is its meta model and model 3 its meta meta model, which in turn is a model of a model 2 and meta model of model 1. Each model in fig. 1 has its own convention and language model[15]. By building a meta model on a higher abstraction level we can combine or consolidate different models having different conventions, semantics and meta data.

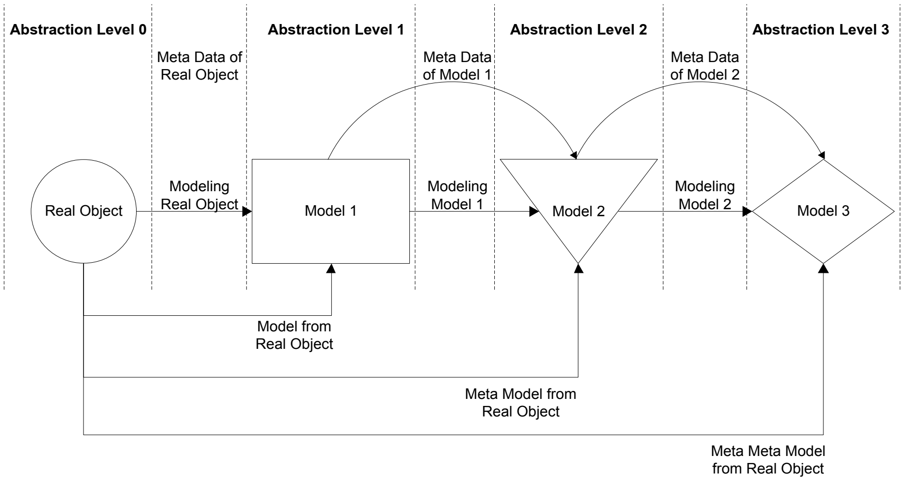


Figure 1 Models and Metadata

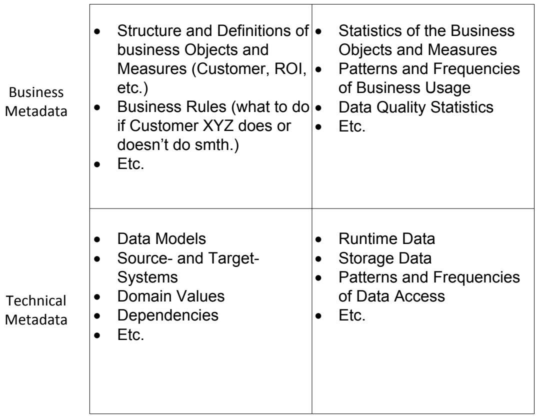
Meta data that arise from the modeling of objects and related processes are defined as *structural* metadata. Depending on the area of its origin, the data is classified as technical and business metadata. For example, technical metadata can serve as a description of a table that consists of columns of certain specific format. Example of business metadata could be the definition of a customer - which is a natural or legal person with certain attributes that has purchased a given product or service. The structural metadata gives the user the ability to navigate through its structure and in this way to get an understanding of the real objects without ever having touched them.

Structural metadata is a relatively static data, dependent on how often the underlying object or its model changes. Related objects however undergo changes mainly in the long run. In contrast, metadata derived from the interaction[16] of the objects is dynamic in nature and is known as *operational* metadata. Operational metadata could be statistics that describe events and

[15] The various conventions and language modeling are represented by the different forms of fig. 1.
[16] In this case the interaction between the objects is modeled.

processes related to the real objects. Depending on the area of its origin, metadata is also classified as technical or business. On fig. 2 is presented a classification of technical/business and structural/operational metadata.

In order to manage metadata with different origin and classification type the corresponding model has to be created in a high abstraction level with generic architecture. This will allow the creation of one single generic model for every type of metadata.



Business Metadata	• Structure and Definitions of business Objects and Measures (Customer, ROI, etc.) • Business Rules (what to do if Customer XYZ does or doesn't do smth.) • Etc.	• Statistics of the Business Objects and Measures • Patterns and Frequencies of Business Usage • Data Quality Statistics • Etc.
Technical Metadata	• Data Models • Source- and Target-Systems • Domain Values • Dependencies • Etc.	• Runtime Data • Storage Data • Patterns and Frequencies of Data Access • Etc.

Figure 2 Classification of Metadata[17]

The purpose of the Generic Modeling [2] is that some parts of the model or the whole model could be reused in other models without any or with minor local changes. In addition to this requirement changes of the data model should be minimized or avoided if possible, even with changing business rules. To achieve this goal the business model is divided to business rules and independent from them generic data model. In order for the model to be generic, the architect should follow the principles of generic design: [3]

1. *Candidate attributes should be treated as representing relationships to other entity types.*
2. *Entities should have a local identifier within a database or exchange file. These should be artificial and managed to be unique. Relationships should not be used as part of the local identifier.*
3. *Activities, associations and event-effects should be represented by entity types (not relationships or attributes).*
4. *Relationships (in the entity/relationship sense) should only be used to express the involvement of entity types with activities or associations.*

[17] For other examples of metadata ref. [1].

5. *Entity types should represent, and be named after, the underlying nature of an object, not the role it plays in a particular context.*
6. *Entity types should be part of a subtype/super type hierarchy of generic entity types in order to define a universal context for the model.*

The model produced with the Generic Modeling architecture is capable to adapt changes of business rules without any or with minor local changes. Its standardization [4, 5] allows it to be combined with other generic models and to be exchanged [6] between different organizations. Data is presented very consistently without any denormalization, which leads to the elimination of any anomalies.

Despite the advantages of this approach there are also some drawbacks. Mostly, they are reflected in the complexity of the data model. Large number of entity classes[18] and their relations leads to extremely large and complex data models that are practically incomprehensible in scope and can be managed only with a specialized software. The extensive normalization of the generic models leads to significantly lower performance of the queries.

To avoid these disadvantages we'll apply the Generic Modeling principles to the Data Vault (DV) [7, 8] architecture. The DV-architecture is optimized for storage and handling of the so called *raw data* and consists of three main types of entities: *Hubs*, *Satellites* and *Links*.

Hubs consist of lists of unique business keys. Example of hub can be the table of the entity **Product** which will contain all **ProductNr** (product numbers) of products that are known in the system as well as several technical attributes which are recorded by the ETL-processes and can be used for control such as: **SQN**, **LOAD_DTS**, **EXTRACT_DTS** and **REC_SRC** - sequence, load date timestamp, extract date timestamp and record source.

Satellites consist of descriptive data for business keys and/or their associations. They are built in the form of slowly changing dimensions (SCD 2) [9] and contain all historized information about the hubs or connections including the technical attributes listed above and **LOAD_END_DTS** - load end date timestamp, which contains the date on which the data set got a new version in its history.

Links in their turn consist of unique lists of associations which are representing the relations of two or more business keys. Basically they define the interactions between business objects which are represented by the hubs.

[18] For ISO 15926 there are more than 10.000 predefined entity classes.

On fig. 3 are listed the basic elements of the DV-architecture, which in this case consist of three hubs **Product**, **Customer** and **Order** with their satellites related with a link which records the history of the their relations.

With the separation of the attributes in hubs, satellites an links, DV present a highly flexible architecture with the following characteristics:

- changes in the data model is mostly carried out by adding additional links and satellites.
- different models can be just put together with creating of additional links and satellites.
- historization is done only within the highly denormalized satellites, which allows effective management of their life cycle.

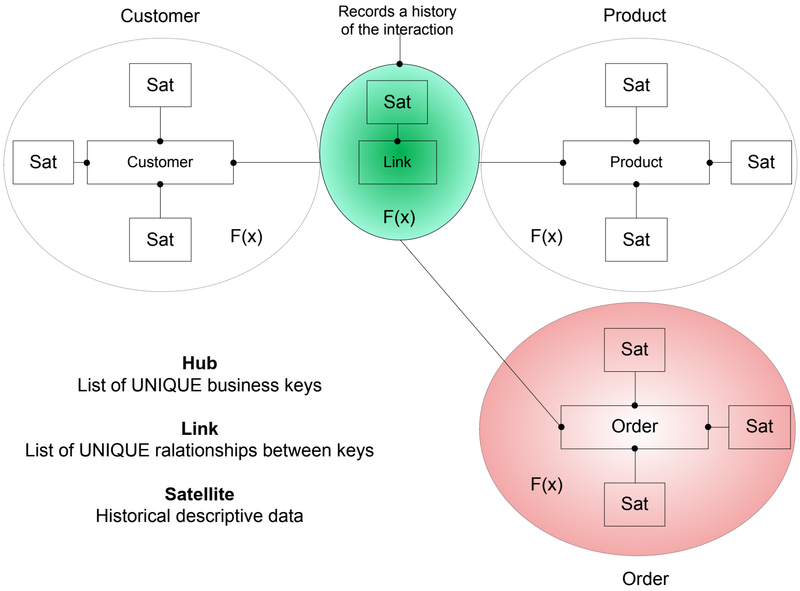

Customer
Records a history of the interaction
Product
Sat
Sat
Customer
Sat
F(x)
Sat
Link
F(x)
Sat
Product
Sat
F(x)
Sat
Hub
List of UNIQUE business keys
Link
List of UNIQUE ralationships between keys
Satellite
Historical descriptive data
Sat
Order
Sat
F(x)
Sat
Order

Figure 3 Example Data Vault ([8] p. 20)

- classification of the tables makes easier the navigation and orientation through the model and facilitates the standardization of the ETL-processes.
- model is optimized for storing the data but not for query the data. However, the advantages of this architecture outweighed this disadvantage.

By combining the principles of Generic Modeling with the Data Vault structure we can create a model which is generic enough to contain all kind of metadata and still be manageable.

29 Implementation

To achieve our goal we'll start the modeling in a high abstraction level. Every single object, which can exist alone will be presented as an object within the hub **H_OBJECT** and will have certain attributes respectively in the hub **H_ATTRIBUTE**. Objects and attributes will have certain types **H_OBJECT_TYPE** and **H_ATTRIBUTE_TYPE**. On fig. 4 is presented the first draft of the model.

Every object can have any number of attributes, and each attribute can be owned by any number of objects. Relationship between the entities objects and attributes will have cardinality **(n:m)** and be implemented through an additional entity **L_OBJECT_ATTRIBUTE**. In the same way will be expressed the relationships between all other entities. Thus will observe the third and fourth principle of Generic Modeling that require activities and associations to be modeled with separate entities which are the links. Relations between the attribute type and attribute **L_ATTRIBUTE_ATTRIBUTE_TYPE** and object with object type **L_OBJECT_OBJECT_TYPE** are modeled on the same principle. Object types can also have attributes, which is modeled by their relation on the same principle. Object types can also have attributes, with the link **L_ATTRIBUTE_OBJECT_TYPE**.

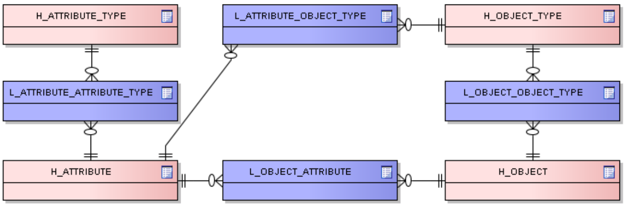


Figure 4 First Draft of the Generic Metadata Model

All of the entities are named after their main character, which is the requirement of the fifth generic principle. The prefixes **H**-HUB and **L**-LINK are implying their use which is a hub and a link. Every entity model will have an artificial primary key (technical key), which is the second principle of the Generic Modeling. Because of the fact that technical keys do not change or change extremely seldom, modeling with hub and links results in one extremely stable and yet flexible architecture. Changes in the structure of the model are implemented mainly by adding new hubs which interact with other with the help of new links without changing the consistency in the rest of the model.

The sixth principle of the Generic Modeling demands that the entities have to be a part of sub/super type hierarchy to determine the universal context of their design. To satisfy this principle and extend the meaning of the relation in the model will be added the entities H_RALATION and type of relation hub H_RELATION_TYPE, as well as the links L_OBJECT_RELATION_TYPE, L_OBJECT_RELATION and L_OBJECT_RELATION_TYPE representing the relations, shown on fig. 5:

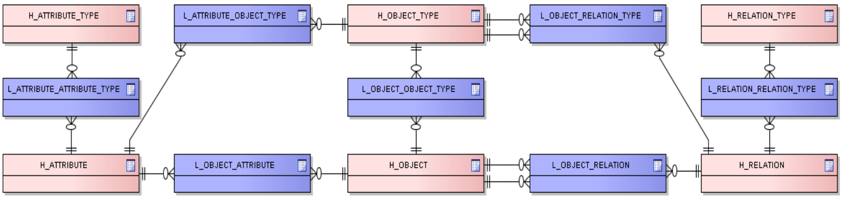


Figure 5 Second Draft of the Generic Metadata Model

The hubs **H_RELATION_TYPE** and **H_RELATION** are used to classify all possible kinds of references - hierarchies, associations, relations, connections, etc. between the entities **H_OBJECT** and **H_OBJECT_TYPE**. The relations will be provided by the hub **H_RELATION** and the links **L_OBJECT_RELATION** and **L_OBJECT_RELATION_TYPE**, which will be done by double referencing the hub with **H_OBJECT** and **H_OBJECT_TYPE**. The double reference will be done with two foreign keys in the link, both of which will referencing the primary key of the corresponding hub. With the use of hub **H_RELATION** the reference will be performed in a certain context, which satisfies the requirement of universal context of design.

A detailed presentation of the link L_OBJECT_RELATION with the hubs **H_OBJECT** and **H_RELATION** is shown on fig. 6:[19]

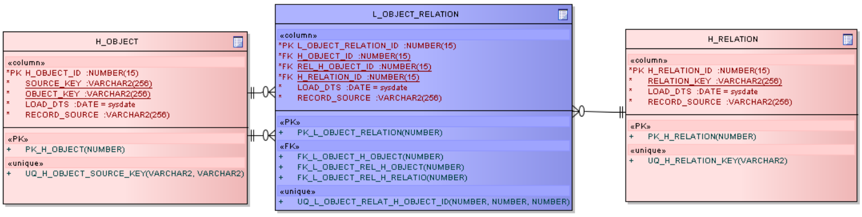

H_OBJECT
«column»
*PK H_OBJECT_ID :NUMBER(15)
* SOURCE_KEY :VARCHAR2(256)
* OBJECT_KEY :VARCHAR2(256)
* LOAD_DTS :DATE = sysdate
* RECORD_SOURCE :VARCHAR2(256)
«PK»
+ PK_H_OBJECT(NUMBER)
«unique»
+ UQ_H_OBJECT_SOURCE_KEY(VARCHAR2, VARCHAR2)
L_OBJECT_RELATION
«column»
*PK L_OBJECT_RELATION_ID :NUMBER(15)
*FK H_OBJECT_ID :NUMBER(15)
*FK REL_H_OBJECT_ID :NUMBER(15)
*FK H_RELATION_ID :NUMBER(15)
* LOAD_DTS :DATE = sysdate
* RECORD_SOURCE :VARCHAR2(256)
«PK»
+ PK_L_OBJECT_RELATION(NUMBER)
«FK»
+ FK_L_OBJECT_H_OBJECT(NUMBER)
+ FK_L_OBJECT_REL_H_OBJECT(NUMBER)
+ FK_L_OBJECT_REL_H_RELATIO(NUMBER)
«unique»
+ UQ_L_OBJECT_RELAT_H_OBJECT_ID(NUMBER, NUMBER, NUMBER)
H_RELATION
«column»
*PK H_RELATION_ID :NUMBER(15)
* RELATION_KEY :VARCHAR2(256)
* LOAD_DTS :DATE = sysdate
* RECORD_SOURCE :VARCHAR2(256)
«PK»
+ PK_H_RELATION(NUMBER)
«unique»
+ UQ_H_RELATION_KEY(VARCHAR2)

Figure 6 Second Draft of the Generic Metadata Model

Hub **H_OBJECT** has an artificial primary key **H_OBJECT_ID** and one composite business key[20] consisting of **SOURCE_KEY** and **OBJECT_KEY**. **SOURCE_KEY** is the key of the source from which the object keys have been

[19] The link **L_OBJECT_RELATION_TYPE** is modeled in the same way.

[20] The combination of **SOURCE_KEY** and **OBJECT_KEY** must be unique.

imported. The key is composite because the business keys of different objects from different sources may have the same values. **H_OBJECT** is the only hub with a composite business key. All other hubs have one artificial primary key, one business key and two technical attributes **LOAD_DTS** and **RECORD_SOURCE**, which are common attributes[21] in the Data Vault modeling representing the date on load and source of the data.

Link **L_OBJECT_RALATION** has one attribute **L_OBJECT_RELATION_ID** which plays the role of an artificial primary key and a combination of three foreign keys, one to the primary key of hub **H_RELATION** and two to the primary key of hub H_OBJECT (**H_OBJECT_ID** and **REL_H_OBJECT_ID**).[22] This modeling technique could be applied to model a hierarchy with unlimited depth and structure. To demonstrate this approach let's model an organization with the following characteristics:

- the organization O1 is divided into two main departments D1 and D2.
- the business activity of department D2 take place in two regions, which are managed by the units U1 and U2.
- with expanding the organization in the future an emergence of new departments and units is expected.
- both new and old departments and units may also have their subdivisions.
- the organization's structure should remain flexible, allowing reformation of departments, units, divisions and subdivisions.
-

The model of the described above structure is a hierarchy with levels of certain elements that can be represented as follows:

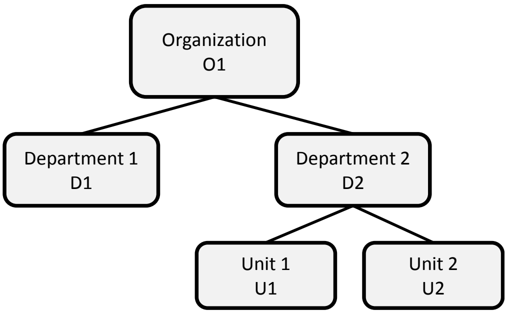
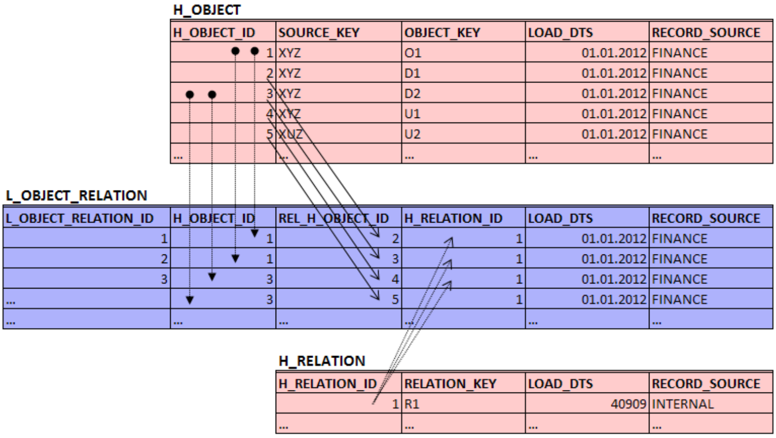


Figure 7 Organization's Structure: Organization, Department, Unit

[21] **LOAD_DTS** and **RECORD_SOURCE** are used in all hubs, links and satellites in the model.
[22] The other links in the model have the same standardized structure similar to **L_OBJECT_RALATION**.

The metadata for the model shown on fig. 7, will be inserted in link **L_OBJECT_RALATION** and hubs **H_OBJECT** and **H_RALATION** is presented on fig. 8:



H_OBJECT

H_OBJECT_ID	SOURCE_KEY	OBJECT_KEY	LOAD_DTS	RECORD_SOURCE
1	XYZ	O1	01.01.2012	FINANCE
2	XYZ	D1	01.01.2012	FINANCE
3	XYZ	D2	01.01.2012	FINANCE
4	XYZ	U1	01.01.2012	FINANCE
5	XUZ	U2	01.01.2012	FINANCE
...	...	...	...	...

L_OBJECT_RELATION

L_OBJECT_RELATION_ID	H_OBJECT_ID	REL_H_OBJECT_ID	H_RELATION_ID	LOAD_DTS	RECORD_SOURCE
1	1	2	1	01.01.2012	FINANCE
2	1	3	1	01.01.2012	FINANCE
3	3	4	1	01.01.2012	FINANCE
...	3	5	1	01.01.2012	FINANCE
...	...	...	...	...	...

H_RELATION

H_RELATION_ID	RELATION_KEY	LOAD_DTS	RECORD_SOURCE
1	R1	40909	INTERNAL
...	...	...	...

Figure 8 Organization's Structure: Organization, Department, Unit

In hub **H_OBJECT** is inserted the metadata of organization, departments and units. The primary keys are doubled referenced in the link **L_OBJECT_RALATION** as foreign keys, modeling a hierarchy between them. In **H_OBJECT_ID** are placed the keys of the parent element, while the **REL_H_OBJECT_ID** these of their direct descendants. A reference to **H_RALATION** classifies the relationship between the object and its related object as “parent-child”. By expanding the organization's new departments and units will be added at the appropriate level and their metadata will be loaded accordingly.

Presented at this stage entity types are the hub and the link that contain only business keys of real objects and the relations between them. Metadata however comprises not only business keys, but many additional attributes. Typical of these attributes is that they describe the real objects and their references and change over time. In the Data Vault modeling all attributes of this type are placed in the satellites, which are referencing a hub or connection. On fig. 9 are shown the corresponding satellites for the hub **H_OBJECT** and link **L_OBJECT_RALATION**:

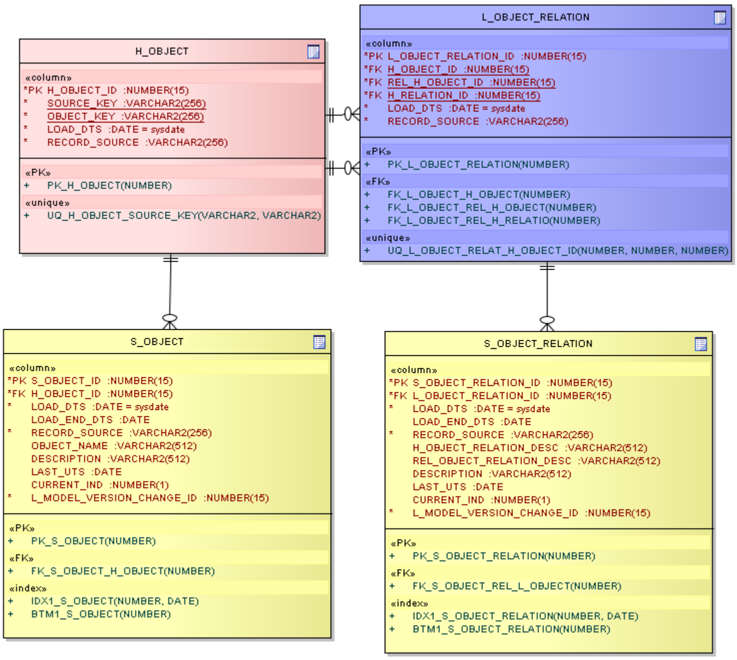
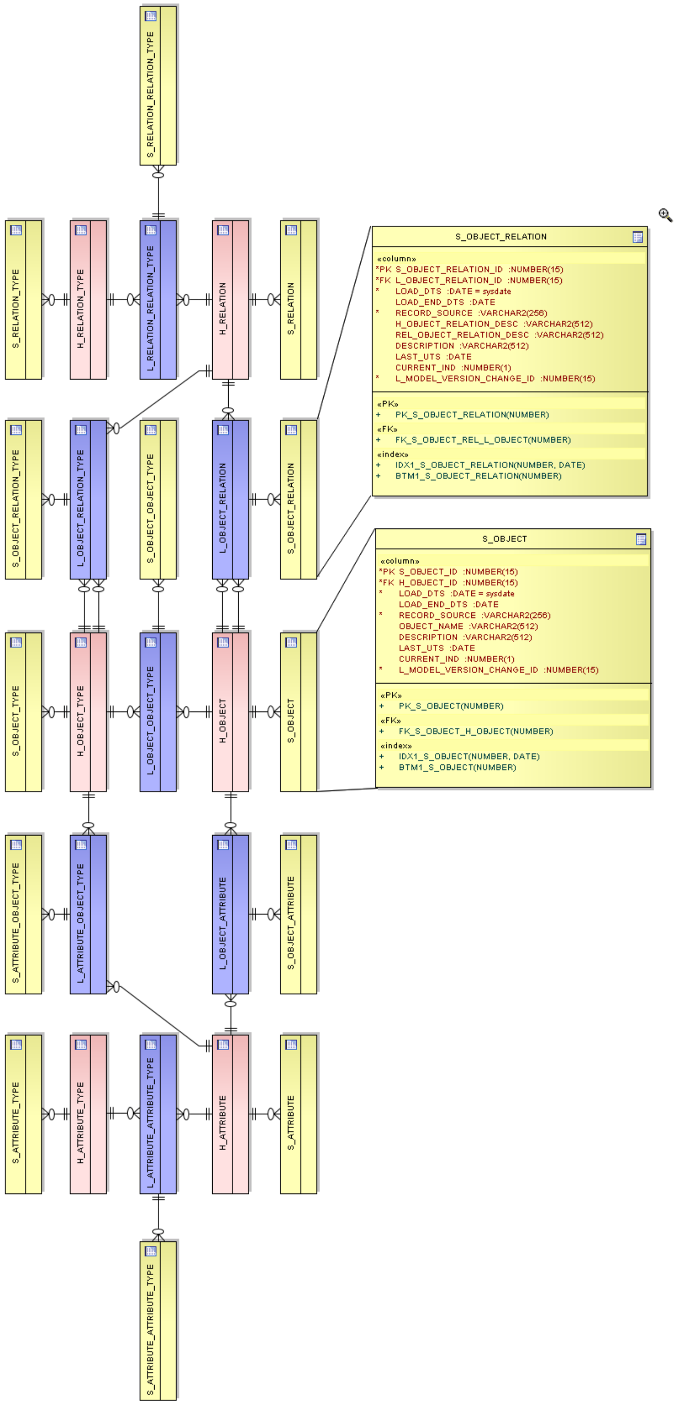

H_OBJECT
«column»
*PK H_OBJECT_ID :NUMBER(15)
* SOURCE_KEY :VARCHAR2(256)
* OBJECT_KEY :VARCHAR2(256)
* LOAD_DTS :DATE = sysdate
* RECORD_SOURCE :VARCHAR2(256)
«PK»
+ PK_H_OBJECT(NUMBER)
«unique»
+ UQ_H_OBJECT_SOURCE_KEY(VARCHAR2, VARCHAR2)
L_OBJECT_RELATION
«column»
*PK L_OBJECT_RELATION_ID :NUMBER(15)
*FK H_OBJECT_ID :NUMBER(15)
*FK REL_H_OBJECT_ID :NUMBER(15)
*FK H_RELATION_ID :NUMBER(15)
* LOAD_DTS :DATE = sysdate
* RECORD_SOURCE :VARCHAR2(256)
«PK»
+ PK_L_OBJECT_RELATION(NUMBER)
«FK»
+ FK_L_OBJECT_H_OBJECT(NUMBER)
+ FK_L_OBJECT_REL_H_OBJECT(NUMBER)
+ FK_L_OBJECT_REL_H_RELATIO(NUMBER)
«unique»
+ UQ_L_OBJECT_RELAT_H_OBJECT_ID(NUMBER, NUMBER, NUMBER)
S_OBJECT
«column»
*PK S_OBJECT_ID :NUMBER(15)
*FK H_OBJECT_ID :NUMBER(15)
* LOAD_DTS :DATE = sysdate
LOAD_END_DTS :DATE
* RECORD_SOURCE :VARCHAR2(256)
OBJECT_NAME :VARCHAR2(512)
DESCRIPTION :VARCHAR2(512)
LAST_UTS :DATE
CURRENT_IND :NUMBER(1)
* L_MODEL_VERSION_CHANGE_ID :NUMBER(15)
«PK»
+ PK_S_OBJECT(NUMBER)
«FK»
+ FK_S_OBJECT_H_OBJECT(NUMBER)
«index»
+ IDX1_S_OBJECT(NUMBER, DATE)
+ BTM1_S_OBJECT(NUMBER)
S_OBJECT_RELATION
«column»
*PK S_OBJECT_RELATION_ID :NUMBER(15)
*FK L_OBJECT_RELATION_ID :NUMBER(15)
* LOAD_DTS :DATE = sysdate
LOAD_END_DTS :DATE
* RECORD_SOURCE :VARCHAR2(256)
H_OBJECT_RELATION_DESC :VARCHAR2(512)
REL_OBJECT_RELATION_DESC :VARCHAR2(512)
DESCRIPTION :VARCHAR2(512)
LAST_UTS :DATE
CURRENT_IND :NUMBER(1)
* L_MODEL_VERSION_CHANGE_ID :NUMBER(15)
«PK»
+ PK_S_OBJECT_RELATION(NUMBER)
«FK»
+ FK_S_OBJECT_REL_L_OBJECT(NUMBER)
«index»
+ IDX1_S_OBJECT_RELATION(NUMBER, DATE)
+ BTM1_S_OBJECT_RELATION(NUMBER)

Figure 9 H_OBJECT, L_OBJECT_RALATION, S_OBJECT and S_OBJECT_RALATION

The cardinality of hubs and links to their satellites is **(1:n)**, every primary key has at least one reference key in its satellite. The satellites are built on the principle of slowly changing dimension (SCD 2) and contains the entire history of the hub or connection. With the satellites to their corresponding hubs and links the model can be presented in its final shape, which is shown on fig. 10

The presented satellite's attributes can be extended for the different requirements and needs. In addition there could be more satellites for one hub or link, containing completely different business attributes. This approach is often applied for the data which is coming from different sources.



```
S_OBJECT_RELATION
«column»
*PK S_OBJECT_RELATION_ID  :NUMBER(15)
*FK L_OBJECT_RELATION_ID  :NUMBER(15)
*    LOAD_DTS  :DATE = sysdate
     LOAD_END_DTS  :DATE
*    RECORD_SOURCE  :VARCHAR2(256)
     H_OBJECT_RELATION_DESC  :VARCHAR2(512)
     REL_OBJECT_RELATION_DESC  :VARCHAR2(512)
     DESCRIPTION  :VARCHAR2(512)
     LAST_UTS  :DATE
     CURRENT_IND  :NUMBER(1)
*    L_MODEL_VERSION_CHANGE_ID  :NUMBER(15)
«PK»
+    PK_S_OBJECT_RELATION(NUMBER)
«FK»
+    FK_S_OBJECT_REL_L_OBJECT(NUMBER)
«index»
+    IDX1_S_OBJECT_RELATION(NUMBER, DATE)
+    BTM1_S_OBJECT_RELATION(NUMBER)
```

```
S_OBJECT
«column»
*PK S_OBJECT_ID  :NUMBER(15)
*FK H_OBJECT_ID  :NUMBER(15)
*    LOAD_DTS  :DATE = sysdate
     LOAD_END_DTS  :DATE
*    RECORD_SOURCE  :VARCHAR2(256)
     OBJECT_NAME  :VARCHAR2(512)
     DESCRIPTION  :VARCHAR2(512)
     LAST_UTS  :DATE
     CURRENT_IND  :NUMBER(1)
*    L_MODEL_VERSION_CHANGE_ID  :NUMBER(15)
«PK»
+    PK_S_OBJECT(NUMBER)
«FK»
+    FK_S_OBJECT_H_OBJECT(NUMBER)
«index»
+    IDX1_S_OBJECT(NUMBER, DATE)
+    BTM1_S_OBJECT(NUMBER)
```

Figure 10 Generic Model for Metadata Repository

11 Concluding Remarks

With adopting of the presented generic metadata repository the organizations may lay the foundations of a centralized and efficient management of all types of models and metadata. Thus it is possible cataloging of technical and business processes in the organization, monitoring the structural dependence and changes, restoring their old versions and changes. The presented model has been designed generic and can be extended or adapted to the requirements of the organization. Standardized structure and typing of the entities contribute to rapid orientation in the model and allow the establishment of standard methods and processes for their loading and query. This in turn reduces the cost of implementation and administration and contributes to optimal use of available resources, which are often quite limited in the organizations. Generic concept of modeling is suitable not only for metadata repository, but also for models that will be created for transactional and master data.

References

Book:

[1] D. Marco. *Building and Managing the Metadata Repository: A Full Lifecycle Guide*. John Wiley & Sons, Inc., 2000.

Technical report:

[2] J. Fowler. *Step for data management, exchange and sharing*. Technical report, Technology Appraisals, 1995.

[3] M. West. *Developing high quality data models.* Technical report, Shell International Limited, 1996.

Web page:

[4] ISO 15926-4:2007 *Industrial automation systems and integration -- Integration of life-cycle data for process plants including oil and gas production facilities -- Part 4.* 12.2012. http://www.iso.org/iso/catalogue_detail.htm?csnumber=41329

[5] ISO 10303-233 *Industrial automation systems and integration -- Product Data Representation and Exchange*. 11.2012. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55257

[6] ISO 10303-11:2004 *Industrial automation systems and integration -- Product data representation and exchange -- Part 11: Description methods: The EXPRESS language reference manual* 12.2012.

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=38047

Book:

[7] D. Linstedt, K. Graziano, and H. Hultgren. *The New Business Supermodel. The Business of Data Vault Modeling*. John Wiley & Sons, Inc., 2000.

[8] D. Linstedt. *Super Charge Your Data Warehouse*. Lulu, second edition, August 2009.

[9] R. Kimball. *The Data Warehouse Toolkit*. John Wiley & Sons, Inc., 2000.

ECONOMIC VALUE OF INFORMATION SYSTEMS IN PRODUCTION PROCESSES

Aleksandar Krstev*, Zoran Zdravev**

**Faculty of Informatics, UGD – Shtip, R. Macedonia*

*** Faculty of Informatics, UGD – Shtip, R. Macedonia*

Abstract

In this paper will be shown the application of information systems and technologies in production processes in modern conditions (production). The successful implementation of goals and objectives of the enterprise depends on its effective use of information resources. Information resources are the basis for their strategic success. Information support of the enterprise depends not only on the availability of information resources and opportunities and implementation of information innovation, streamline information flows of the company, the issues of its effective information interaction with market players. Information support of the enterprise depends not only on the availability of information resources and opportunities and implementation of information innovation, streamline information flows of the company, the issues of its effective information interaction with market players as Bulgaria, Macedonia, Serbia, Croatia.

***Keywords**: information, resources, knowledge, data, providing, method, system, innovations, estimation, infrastructure, space, enterprise, product, forming, informative streams*.

Introduction

One of the basic concepts of normal business is management activities. Management as a philosophy of modern business, quality management and economic decision-making directly related to the presence of complete, timely and accurate information about market demand for goods, consumer tastes, market conditions, competitors' actions, etc., as well as the performance object management. Significant amounts of information associated with prompt payments, search and providing relevant information for managers making decisions requiring the need for new, modern information technology.

Information resources are the basis for activities of enterprises in EU, they define their strategic success. Background information support of business formed under the direct influence of factors of external and internal environment and focusing the company on growing information resources used for management.

Information support of the enterprise depends not only on the availability of information resources and opportunities and implementation of information innovation, streamline information flows of the company, the issues of its effective information interaction with market players. Information support of the enterprise depends not only on the availability of information resources and opportunities and implementation of information innovation, streamline information flows of the company.

Up to date, the characteristics of informational support of the enterprise paid insufficient attention both in theoretical and in practical aspects.The aim of the investigation is to develop theoretical, methodological and practical recommendations for activities of the enterprise. To achieve this goal have been resolved following objectives:

- The essence of information and for activities of industry in EU and the necessity for activities of the enterprise and its main objective;
- The possibility of development of information support on national and regional levels on the example of the Bulgarian company;
- Analyzed the structure and dynamics of market information products and services in EU;

Functional-based approach methods

Methodological basis of the paper is a collection of ways scientific knowledge, and general scientific principles, methods and techniques used in the study process. The theoretical basis of scientific work were EU scientists in the field of management and information support its activities.

This paper uses system-structural analysis (features and the role of information resources in modern enterprises, the analysis of market information products and services in EU), procedural and situational approaches (with the justification necessary for activities of the enterprise, while developing a coherent organization of information support enterprise development), functional-based approach (the development of fundamental approaches to the formation of enterprise information space), dynamic methods, theory, simulation and optimization method (the construction of information and control system, the formation of decision support systems), graphical methods, methods for expert evaluation, system analysis and modeling (in developing ways to evaluate and select information innovations).

Scientific novelty of the results

The main scientific result of research is to develop fundamental approaches to building information-control system, formation of enterprise information space and the sequence evaluation and selection of information innovations that are based on the principles and methods of information theory and information systems and enterprise management. Scientific novelty of research results is as follows:

- proposed sequence of formation of information and control systems for industrial businesses, which allows you to build a hierarchical access to administrative information and optimize their management structure and its information flows;
- fundamental approaches to industrial enterprise information space based on his selection of functional and content structure and structural decomposition of the production process as an object of management;
- forms and directions for activities of industrial enterprises using the proposed decision support system based on the formation of information databases and complex simulation models for enterprises;
- methods and forms for activities of the enterprise;

The practical significance of the results

Developed in the paper approaches, methods and results are methodical base for activities on the basis of principles and methods of information resources management, information and innovation development. In results that are most practical importance, are:

- recommendations for the development of enterprise information infrastructure based on the proposed implementation of a regional information-analytical framework to support their development, thereby ensuring consistency and improvement of information exchange of the market of the Republic of Macedonia;
- Recommendations on the evaluation and selection of information innovations that can solve the problem of a multidimensional comparison of software products and evaluate risk factors for the decision on the choice of information innovation.

The special role of information and information resources of modern countries and enterprises due to their direct participation in any economic processes and the ever increasing level of information the market environment and society in general. The current stage of economic development requires the use of scientifically-based methods of data collection, analysis, processing and use of information and its interrelated forms, which should promote the potential of enterprise information resources and consistent implementation of its directions of development. Under the provision of business information refers to a set of forms, methods and tools of information resources needed to implement and suitable analytical and administrative procedures to ensure stable operation of the business, its sustainable development perspective.

Accordingly, in the work using an approach based on the idea of resource cycle, the main resource characteristics and specific features of functional information and resources provided by the scheme of their reproductive cycle (Fig. 1).

At the time, the primary role in this process are information and Internet technologies that are still classified as "high technology", but actually has a base that is essential for modern developed economies. The increase in turnover in foreign trade, particularly in the global fate of cumulative export is one of the main factors characterizing the sophistication and competitiveness of national economy, which necessitates the study of industrial development prospects of each country through use of new technologies in foreign offices and industrial centers abroad. It is proved that the search for answers to these and similar questions directly affecting the different aspects of evaluation and selection of information products or services offered and identify factors that determine the "quality system" of information resources. It should be noted that at present no methodology of quantitative and qualitative assessment of information resources, and forecasting needs of society in them. This reduces the efficiency of information as information resources, and increases the duration of the transition from an industrial to an information society.

The characteristics of the theoretical foundations for activities of the enterprise allows to determine the possibility of a synergistic effect of the interaction of information and production areas and increase their effectiveness and concluded that the impact of this process depends on the degree conditions and opportunities for activities of enterprises in countries.

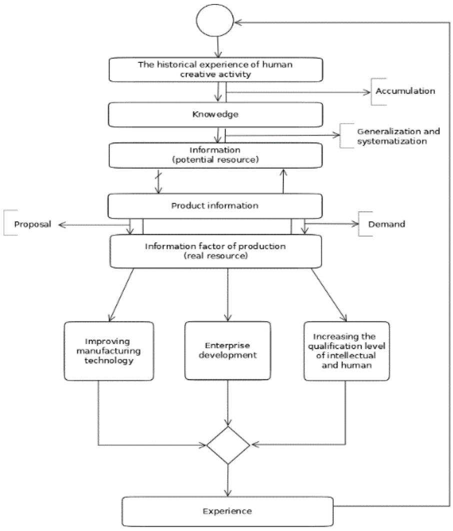

The historical experience of human creative activity
Accumulation
Knowedge
Generalization and systematization
Information (potential resource)
Product information
Proposal
Demand
Information factor of production (real resource)
Improving manufacturing technology
Enterprise development
Increasing the qualification level of intellectual and human
Experience

Fig. 1. Reproductive cycle of information resources

Building sustainable market information services in EU began in mid-50's were at this period the main suppliers of information services were entirely information services of academic, professional, scientific and technical societies, government agencies, educational institutions. In EU today is rapidly forming the market of information products and services. In recent years a much stronger technical and technological base of information is increasing sales volume of information, computers, and telecommunication equipment. Contribution of industries of information and communication technologies and the amount of information and communication services in the EU countries today is already about up to 10-25%. Market information and communication technologies, a major market segments and greatest information products and services in general has kept growth. Services market today is still not well developed, but its growth rates are large, as more consumers willing to pay high price for quality services and service.

In some EU countries, the first stage of deployment of a national WiMAX network based on Cisco Mobile WiMAX technology and architecture of IP NGN. Network is based on technology Cisco ® Mobile WIMAX and Cisco solutions for access and aggregation. By the end of 2009 Max Telecom plans to have coverage of its network in the home to 90 percent of the population.

The analysis of main directions of development of EU markets of information products and services, which allowed to identify the main components of their structure and features of this information products and services. It is determined the information needs of the market and level of development of advanced information technologies. The proposed sequence of stages of development and implementation of regional development programs enterprise information infrastructure of some EU examples (Fig. 2), which is aimed at providing some of the important tasks of the effective interaction of market information, improving information support enterprise development in the region and the formation of their information infrastructure.

In Fig. 3. Definition of socio-economic impact of the structure and functioning of such effects increase for activities of enterprises of countries held by economic and mathematical tools and methods of simulation. The assessment showed that increasing information of the enterprise significantly changes the trajectory of its development at every stage of life cycle.

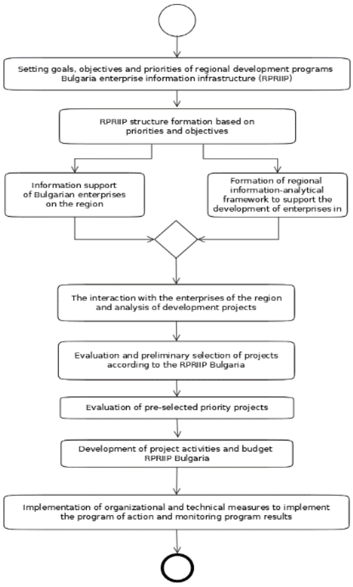
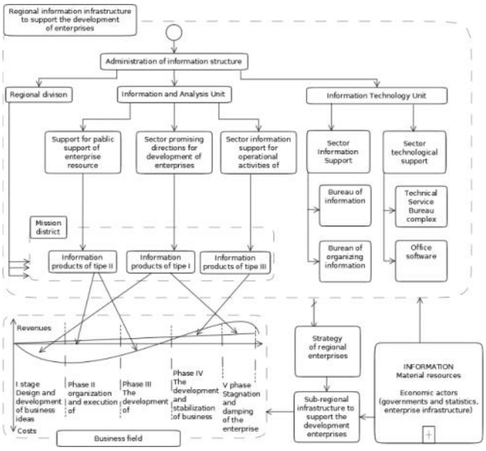

Setting goals, objectives and priorities of regional development programs Bulgaria enterprise information infrastructure (RPRIIP)
RPRIIP structure formation based on priorities and objectives
Information support of Bulgarian enterprises on the region
Formation of regional information-analytical framework to support the development of enterprises in
The interaction with the enterprises of the region and analysis of development projects
Evaluation and preliminary selection of projects according to the RPRIIP Bulgaria
Evaluation of pre-selected priority projects
Development of project activities and budget RPRIIP Bulgaria
Implementation of organizational and technical measures to implement the program of action and monitoring program results

Fig. 2. Stages of formation and realization of regional development programs enterprise information infrastructure of Bulgaria

In the sense formalized integrated structure management, information transfer and management decisions is the basis of improvement of management and are based on structural decomposition of the production process as an object of management, functional management and structuring of formal documents.


Regional information infrastructure to support the development of enterprises
Administration of information structure
Regional divison
Information and Analysis Unit
Information Technology Unit
Support for pablic support of enterprise resource
Sector promising directions for development of enterprises
Sector information support for operational activities of
Sector Information Support
Sector technological support
Bureau of information
Technical Service Bureau complex
Mission district
Information products of tipe II
Information products of tipe I
Information products of tipe III
Burean of organizing information
Office software
Revenues
I stage Design and development of business ideas
Phase II organization and execution of
Phase III The development of
Phase IV The development and stabilization of business
V phase Stagnation and damping of the enterprise
Costs
Business field
Strategy of regional enterprises
Sub-regional infrastructure to support the development enterprises
INFORMATION Material resources
Economic actors (governments and statistics, enterprise infrastructure)

Development and management decisions is a complex process, whose implementation should be based primarily on accurate and comprehensive information on all management levels. In this context it plays a special role of information management systems, effectiveness of which determines the ultimate effectiveness of the functioning of businesses. The task to enhance the process for activities on the basis of construction of its information-control system depends, first, of its objectives, functions and tasks, and second - on the content and consistency of information management systems. On the efficiency of the process aimed proposed decision support system, based on a formation of information databases and complex simulation models for enterprises. Fig. 4.

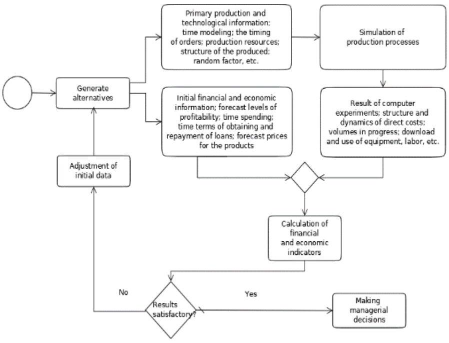

Primary production and technological information; time modeling; the timing of orders; production resources; structure of the produced; random factor, etc.
Simulation of production processes
Generate alternatives
Initial financial and economic information; forecast levels of profitability; time spending; time terms of obtaining and repayment of loans; forecast prices for the products
Result of computer experiments; structure and dynamics of direct costs; volumes in progress; download and use of equipment, labor, etc.
Adjustment of initial data
Calculation of financial and economic indicators
No
Yes
Results satisfactory?
Making managerial decisions

Fig. 4. Consistency management decisions with DSS

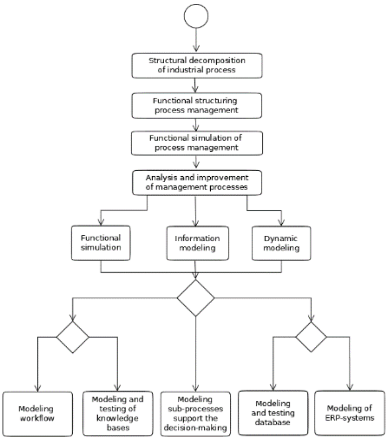

Structural decomposition of industrial process
Functional structuring process management
Functional simulation of process management
Analysis and improvement of management processes
Functional simulation
Information modeling
Dynamic modeling
Modeling workflow
Modeling and testing of knowledge bases
Modeling sub-processes support the decision-making
Modeling and testing database
Modeling of ERP-systems

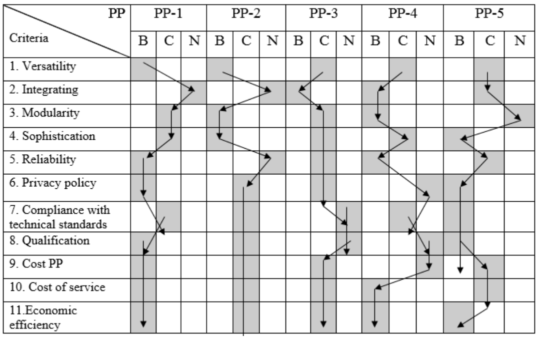
Fig. 5. The sequence of formation of information-control system of enterprise machines

Effective management decisions require processing large volumes of information and the collection, analysis and aggregation of information flows coming to the enterprise. (Fig. 5).

The problem of designing an efficient structure of information and control Systems Company in the proposed deal on the basis of the evolutionary method using genetic algorithms. The functioning of such a structure of information and control systems to optimize enterprise management and information flow and its standard processes. One of the main criteria optimization criterion defined time performance of typical data processing procedures.

To improve information support for enterprises in the paper suggested the main directions of assessment and selection of information innovation. Proved that the evaluation and selection of information innovations is a difficult task for multi commercial solution is selected in the basic classes of innovative information systems and provided their estimates based on the proposed principles and criteria.

Given sufficient diversity of modern market information products and services as of the assessment team identified the following information innovations, like software, and proposes a way to value them. A multiple comparison procedure involves the use of both quantitative estimates and qualitative expressed in descriptive categories, which enhances the analysis by obtaining estimates for criteria that cannot expose quantitative measurements. These estimates form the scale of measurement is the basis for decisions on selection of software. (Table 1).



PP / Criteria	PP-1			PP-2			PP-3			PP-4			PP-5		
	B	C	N	B	C	N	B	C	N	B	C	N	B	C	N
1. Versatility	▨			▨				▨			▨			▨	
2. Integrating			▨			▨	▨			▨				▨	
3. Modularity		▨		▨				▨		▨					▨
4. Sophistication		▨		▨				▨			▨		▨		
5. Reliability	▨					▨		▨		▨				▨	
6. Privacy policy	▨				▨			▨				▨	▨		
7. Compliance with technical standards		▨			▨				▨		▨		▨		
8. Qualification	▨				▨				▨			▨	▨		
9. Cost PP	▨				▨			▨				▨		▨	
10. Cost of service	▨				▨			▨		▨				▨	
11.Economic efficiency	▨				▨			▨		▨			▨		

Designation of priorities: B – high, C – average, N - is low.

According to the principles of multidimensional comparison for each pair of software products designed indicators match and inconsistencies by building a matrix of risk.

CONCLUSIONS

The paper on the basis of studies carried out theoretical studies and practical solution to current scientific and practical tasks to improve information of the enterprise. Key findings and results that were obtained during the research, are as such.

1. The special role of information and information resources in modern enterprises of the EU, due to their direct participation in economic processes and the ever increasing level of information the market environment and society in general.
2. Determined that information for the enterprise should be based on the complex use of potential and existing information resources.
3. Courtesy of the general characteristics of information resources and formed the basic approaches to evaluation using an information approach, theories of information resources and economic information and implementation of these approaches.
4. The organizational-economic model of a single regional information-analytical framework to support the development of industrial enterprises. Determined the effect of the functioning of this structure and the impact of information increase the activity of enterprises using economic and mathematical tools and methods of simulation.
5. A decision support system, which is forming the basis of information databases and complex simulation models for enterprises. On the basis of this system model of decision making in production by building a set of management information and use of industrial engineering resources.

The method of evaluation and selection of information innovation by building an appropriate model, evaluation and selection of software and the sequence information of this procedure in view of risk factor. The role of information and informative resources in activity of modern enterprises, conditioned by their direct participation in economic processes and constantly increasing level of informatization of market environment and society on the whole. It is definite, that the informative providing of activity of enterprise must be based on the complex use of informative resources potential and present taking into account their basic features of each EU country.

References:

1. Krstev, A. The results of scientific research, conclusions and recommendations reported, discussed and received approval for international scientific conference "Economic problems of adaptation and development of engineering sector in Bulgaria and Ukraine in the circumstances" (Sofia, Bulgaria, 2009).

2. Krstev, A. Ukrainian scientific-practical conference with international participation "The economic problems of the sustainable development of the enterprise in a market economy" (Odessa, 2009).
3. Krstev, A. “Improvement of the Operative Information Providing of Activity of Industrial Enterprises of Bulgaria and Ukraine” (Kiev, Ukraine, 2010).

TUNING PID CONTROLLING PARAMETERS FOR DC MOTOR SPEED REGULATION

Done Stojanov[1]

[1]Faculty of Computer Science, University ,,Goce Delcev" – Stip, done.stojanov@ugd.edu.mk

Abstract. Modern robots are sophisticated and complex systems, composed of: sensors, high-speed processors and actuators. Different size DC electrical motors are used as actuators, converting electrical energy into mechanical movement. Without them, robots can't perform movements, what is completely on the contrary on modern robotics concepts. Motor speed regulation is an important engineering task. Having appropriately tuned the controller, the desired speed is reached in a short time interval, with minimum speed overshoot. Tuning motor speed controlling parameters in order to reach the desired speed within a short time interval, keeping speed's overshoot as small as possible is discussed in this paper. The paper demonstrates how the general Black-Box methodology can be applied for that purpose. Speed's simulations are performed in Matlab, having connected PID controller and DC electrical motor in a closed-loop unity feedback control system.

Keywords: robotics, Black-Box methodology, actuator, optimal speed control.

30 Introduction

The parameters of the first process controller were defined by A. Callendar [2] in 1934. Callendar's work demonstrates how *proportional-derivate* (PD) controlling parameters can be set up for control of *integration plus delay* (IDP) modeled process. Few years after, tuning rules for setting up *proportional-integral* (PI) and *proportional-integral-derivate* (PID) controller [1] were revealed. Since then PI and PID controllers have become widely used in the industry. According H. Takatsu and T. Itoh [4], approximately 95% of controllers are of PI or PID type.

Direct current (DC) electrical motors are widely used in industrial applications including mechatronics, automobile, robotics and aerospace systems [3,6]. DC motor speed control is one of the fundamental engineering tasks. It can be regulated by a PID controller, setting up appropriately: the proportional, integral and the derivate gain. The proportional term provides an overall control action proportional to the error signal. The integral term reduces steady-state errors, while the derivate term improves the settling time [5].

In this paper, DC motor speed control is considered, using as a regulator PID controller. Based on the Black-Box methodology, PID controlling parameters are dynamically changed in order to reach motor's desired speed, holding speed's overshoot and the settling time under certain threshold. Speed's simulations are performed on a concrete DC motor, for different values of the proportional, integral and derivate gain, according to the presented approach.

31 Preliminaries

A closed-loop unity feedback control system (Fig. 1) is considered, composed of PID controller and DC motor as an actuator. Tachogenerator measures motor speed, generating speed-proportional output voltage. Its transfer function equals 1. PID controller transfer function is $C(s) = k_p + \frac{k_i}{s} + k_d s$. Speed's rise time, defined as the time needed for reaching 90% of the steady value for the first time, is highly influenced by the value of the proportional gain - k_p . By changing the integral gain - k_i , the steady-state error can be reduced or completely eliminated. Speed's overshoot and the settling time are controlled by k_d - the derivate gain. Speed's overshoot is defined as a difference between the peak and the steady value, while the setting time is the time needed for reaching steady value of the parameter being controlled, which in this case is motor speed.

Motor's transfer function is $M(s)=\dfrac{K}{JLs^2+(JR+Lb)s+K^2+bR}$, where K is motor's constant, J is the moment of inertia, strictly depending of rotor's construction and motor's load, L is motor's inductance, R is motor's resistance, while b is the damping ratio of the mechanical part. Motor's transfer function is derived from equations (1) and (2), applying Laplace Transformations on (1) and (2), describing motor's electrical and mechanical properties. Rotor's angular displacement is $\theta(t)$, motor's speed $\dfrac{d\theta(t)}{dt}$ is the output, while the applied voltage $v(t)$ is taken as an input.

$$v(t)=L\frac{di(t)}{dt}+Ri(t)+K\frac{d\theta(t)}{dt} \tag{1}$$

$$J\frac{d^2\theta(t)}{dt^2}+b\frac{d\theta(t)}{dt}=ki(t) \tag{2}$$

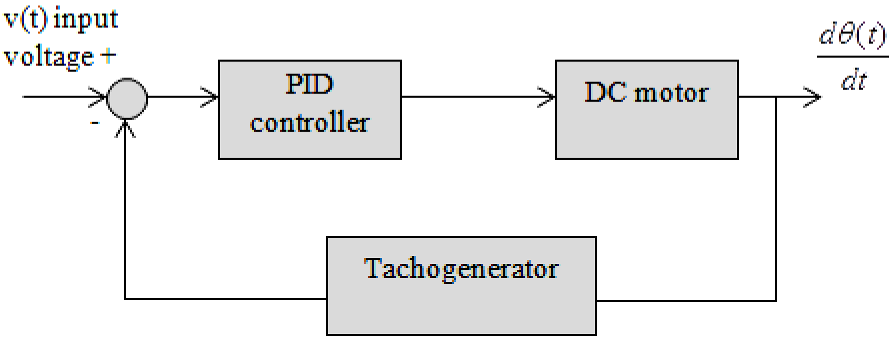


Figure 1 DC motor speed control scheme

32 Main Results

Motor speed should follow input voltage $|v|=|s_{stac}|$, holding the settling time under certain threshold $t_{\max}$, with overshoot not greater than $os_{\max}$ rad/s, where s_{stac} is speed's steady value, and $os_{\max}$ is the maximum permitted overshoot. The overshoot is calculated with the formula $os=|s_{\max}-s_{stac}|$, where $s_{\max}$ is the peak value of the speed during the transient response.

DC motor's characteristics are given in Table 1. The motor is controlled by a PID controller, connected in a closed-loop unity feedback control system as shown on Figure 1. PID controlling parameters should be tuned such as the settling time is less than 0.6 s and the overshoot is not greater than 0.05 rad/s. Using black-box approach, measuring motor's speed response for different combinations of PID controlling parameters (Tab. 2), PID controlling parameters are tuned such as the previous requirements are satisfied.

For $k_p = 5, k_i = 5$ and $k_d = 5$, speed's settling time is 3.95 s (Tab. 2, Fig. 2). Doubling PID controlling parameters, speed's settling time equals 3.5 s (Tab. 2, Fig. 2). For $k_p = 100, k_i = 10$ and $k_d = 10$, the settling time equals 0.576 seconds (Tab. 2, Fig. 2), what is certainly less than 0.6 s.

Regarding the speed's overshoot, for $k_p = 5, k_i = 5$ and $k_d = 5$, the overshoot equals $os = | s_{\max} - s_{stac} | = | 10.3 - 10 | = 0.3$ rad/s (Tab. 2, Fig. 3). For $k_p = 10, k_i = 10$ and $k_d = 10$, it equals |10.1-10|=0.1 rad/s (Tab. 2, Fig. 3). For $k_p = 100, k_d = 10$ and $k_i = 10$, speed's overshoot equals 0, |10-10|=0 rad/s (Tab. 2, Fig. 3), what is certainly less than 0.05 rad/s.

Table 1 Motor properties

Property	**Value**
J-motor's inertia	0.01 *Kg×m*^{2}
b-damp ratio	0.00003 *Nm/rad/s*
K-motor's constant	0.023 *Nm/W*$^{1/2}$
R-Resistance	1 *Ω*
L-Inductance	0.5 *H*

Table 2 Speed's settling time and overshoot for different combinations of PID controlling parameters

			Settling time (s)	**Overshoot (rad/s)**	**Satisfies constrains**
5	5	5	3.95	0.3	No
10	10	10	3.5	0.1	No
100	10	10	0.576	0	**Yes**

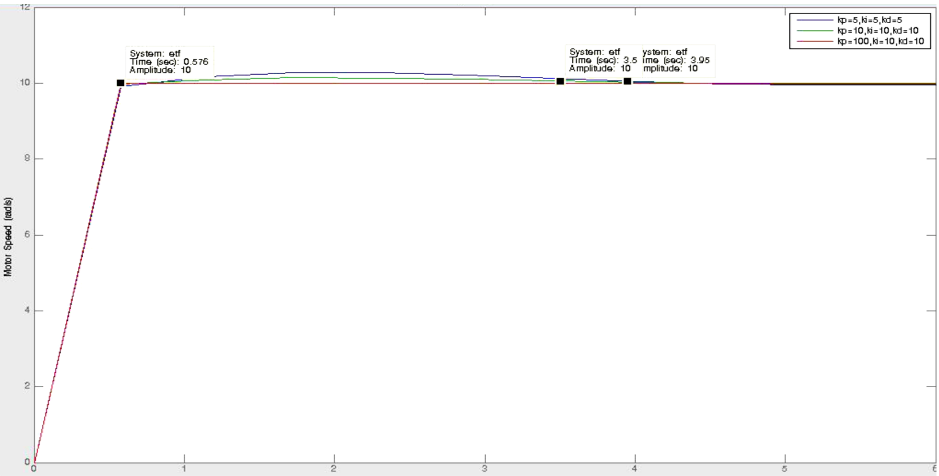


Figure 2 DC motor's speed settling time for tunning parameters of PID controller given in Table 2

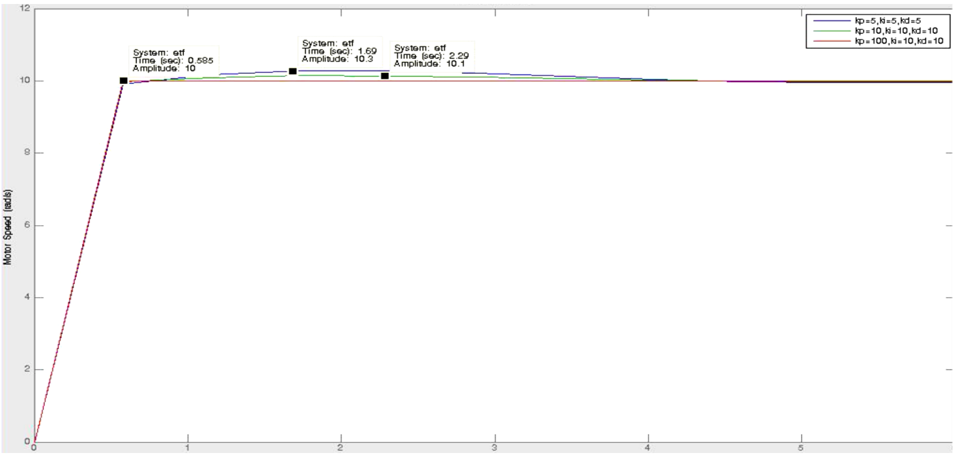


Figure 3 DC motor's speed overshoot for tunning parameters of PID controller given in Table 2

For all three different tunning combinations of PID controlling parameters, the desired speed has been always reached i.e. the steady-state error equals 0. The desired speed is reached within different time interval (settling time). Also the speed's overshoot, defined as a difference between the maximum and steady value of the speed, is different, for different PID controller tunning. General engineering tendency is to reach the desired speed in a short time interval, keeping overshoot as small as possible. If the PID controller is appropriately tunned, the desired speed is reached in less than a second, without overshoot. For the DC motor being considered, tunning PID controlling parameters such as the proportional gain equals 100, the derivate and the integral gain equal 10, the desired speed is reached in approximately half second, without overshoot, what is absolutely acceptable by engineering viewpoint.

33 Conclusion

The Black-Box methodology, measuring system's output for different combinations of controlling parameters, in order to reach the desired output, has been successfully implemented in the case of a closed-loop unity feedback control system, composed of PID controller and DC motor as an actuator. PID controlling parameters are dynamically changed, in order to reach the desired output – motor speed of 12 rad/s, which has to be reach in a time interval less than 0.6 s, keeping speed's overshoot less than 0.05 rad/s. Combination of PID controlling parameters have been found $k_p = 100, k_i = 10$ and $k_d = 10$, such as the desired speed is reached in approximately half second, without speed overshoot, if DC motor with properties given in Table 1 is used as an actuator.

References

[1] A. Callendar, D.R. Hartree and A. Porter (1935): *Time-lag in a control system*. Phil. Trans. Royal Society of London Series A 235, pp. 415-444.

[2] A. Callendar (1934): *Preliminary notes on automatic control*, File No. R.525/15/3. I.C.I. Alkali Ltd.

[3] B. Nguyen and J. Ryu (2009): *Direct Current Measurement Based Steer-By-Wire Systems for Realistic Driving Feeling*. Proceedings of the IEEE International Symposium on Industrial Electronics, pp. 1023-1028.

[4] H. Takatsu and T. Itoh (1999): *Future needs for control theory in industry – report of the control technology survey of Japanese industry*. IEEE Trans. Control Syst. Tech. 7(3), pp. 298-305.

[5] K. H. Ang, G. Chong and Y. Li (2005): *PID Control System Analysis, Design and Technology*. IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY 13(4), pp. 559-576.

[6] S. C. Won, D. J. Lim and D. H. Chyung (1985): *D-C motor driven robotic manipulator control*. IEEE Decision and Control 24, pp. 330-333.

COMPARISON OF THE PERFORMANCE OF THE ARTIFICIAL BOUNDARIES P3 AND P4 OF STACEY

Zoran Zlatev[1], Vasko Kokalanov[2], Aleksandra Risteska[3]

[1]zokizlatev@gmail.com

[2]vasko.kokalanov@ugd.edu.mk

[3]aleksandra.risteska@ugd.edu.mk

Abstract: In this paper a research of the performance of the two variation of the artificial (transparent) boundaries of Stacey, P3 and P4 has been made [4]. Boundaries effect is being examined through determining of the relative reflected seismical energy back to the model. As the reflected energy is smaller, the boundary is more transparent. Testings are being made with numerical methods based on central finite differences, CFD, on materials with different ratio of the propagating velocities of the compressional and tangential waves $C = \alpha / \beta$. The testing will show how artificial boundaries are refer of different values of this ratio and in which case of values smallest or highest error is obtained [7].

Keywords: Numerical simulation, computational model, partial differential equations, numerical scheme.

1. Introduction

In the era of supercomputers, obtaining solutions to the many problems that previously could not be solved become a reality, especially for problems involving partial differential equations, in which the analytical solution exists only for the simplest conditions. With the use of numerical methods, a problem can be solved from the start time until a desired time at all spatial points. Most popular numerical methods for solving partial differential equations are finite element method and the method of finite differences. Usually, the finite element method uses implicit schemes in which the unknown sizes of all spatial points are determined simultaneously for each time step by solving a system of linear algebraic equations. In contrast, most computational schemes based on finite differences are explicit, where the solution is determined by the solution of the previous time step and the equations are independent [1]. Solving a complete linear system of N^{th} order requires 0(N^2) operations while a system of n independent equations is *0*(*N*). Because of this, explicit schemes are preferred in numerical analysis, especially for problems involving many equations with many unknowns (where N is large). Systems that appear in implicit schemes are usually straight and symmetrical, and so the order of complexity is lower than $0(N^2)$ but still higher than that for explicit schemes. On the other hand, implicit schemes are unconditionally stable, not the case with explicit schemes. Furthermore, the final elements as numerical tool are more useful than final differences for modeling complex and irregular geometries. However, for problems of large scale [2], that arise in seismology for example, explicit schemes are recommended because they are cheaper (require less computer resources) and are easier to implement in numerical algorithms. In the last few decades, with the rapid development of computing machines, researchers studying wave phenomena using computer simulations of mathematical models. With these simulations can predict how the facility will respond to seismic impulses.

This means to determine which locations of the building will have a concentration of voltages and large permanent deformations that may lead to the crashing of the object. Besides vulnerability of the objects, computer simulations of mathematical models help us to study the damage on the ground. Some of the most important challenges that arise in the numerical simulations of the spread of waves:

- Modeling artificial boundaries
- Modeling of the free surfaces
- Modeling of contact between two or more different media
- Modeling of nonlinear model

2. **Structure of Paper**

Artificial (absorbing transparent) boundaries are artifacts that serve as tend to simulate the entry of the wave in the model and its going out of the model. In this paper, the effect of the artificial boundaries we evaluate according reflected (parasitic) energy from wave that leaves the model. The smaller this reflected energy, the border is better (more transparent). In the field of artificial boundaries in the numerical methods have worked more researchers [3]. According to the formulation of local artificial boundaries are divided into three types:

- paraxial
- extrapolated
- multidirectional

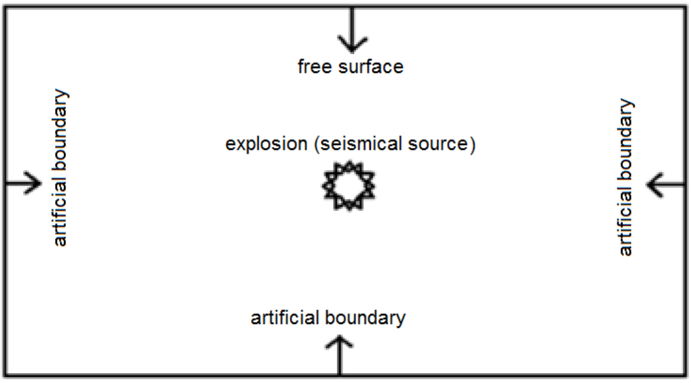
Representative of the first group boundaries is the boundary of Robert Clayton and Bjorn Engquist. They worked on getting and implementation paraksijalni artificial limits on SH and PSV waves. Furthermore, modification and improvement of these boundaries was made by Stacey [4]. Liao and Wong [6], provide a new approach in the execution and implementation of artificial boundaries in the numerical models through extrapolated formulation. Higdon [5] proposes and implements multidirectional formulation of artificial boundaries. Despite the artificial boundaries challenge in numerical modeling of wave propagation is modeling of the free surface. More researchers have investigated the causes of errors in approximation of the free surface. Dominant unstable mode, can often be determined explicitly (Stacey [4]). So using this approach may be proved that the approximation of Ilan (1975) is unstable if

$$\alpha > \sqrt{3} \cdot \beta \qquad (1)$$

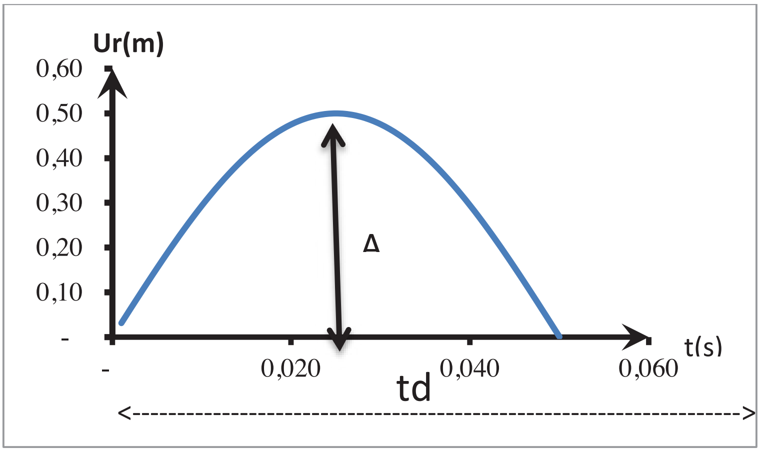
In this paper we study the performance of two proposed variants of the artificial boundaries Stacey [4] for different ranges of the ratio of propagation velocities compressional P waves, α, and tangential SV seismic waves, β. For the most part of the materials the ratio between α and β lies between 1.59 (quartz) and 2.42 (nobium). For example,for steel α/β is 1.83, aluminum is about 2.05. In this paper the stability of the artificial boundaries of Stacey was investigated for values of α/β in this range, and also for much smaller and much larger values. Stacey proves that the approximation of the free surface inevitably leads to numerical instabilities of the numerical scheme. But these instabilities have a very slight increase. They become significant only for very long computer tests, and for many practical uses them quite satisfactory. Parallel to the research of artificial boundaries, performed research and improving the accuracy of numerical schemes which approximated partial differential equations in the interior of the computational domain. In this paper, we use an explicit scheme of Kelly [5]. This is an explicit scheme with second-order accuracy both in time and in space $O(\Delta t^2, \Delta x^2)$. We study Stacey boundaries P3 and P4 for ratios $C = \alpha/\beta$ in range $1.5 < C < 7$ [7]. On the pictures 2a, 3a and 4a are presented the energy generated in the model of the effects of the explosion (input power) and energy out of the model with the propagation of the wave (output energy). When artificial boundaries would have been ideally transparent, because conservativity of the energy, at the end of the analysis, input and power output should be equal. The picture 2a) graphically presented input and output energy ratio $C = \frac{\alpha}{\beta} = 1.5$. Moreover vertical – axis time is represented in seconds and the ordinate is represented energy (MJ). This image refers to P3 boundary of Stacey. On the picture 2b) graph refers to the same energy and the same ratio between $\frac{\alpha}{\beta}$ but this picture refers to P4 [4] boundary Stacey. This picture shows that the energy input and output differ significantly, suggesting that C = 1.5, P4 Stacey border is not transparent as opposed to the same case in the picture 2a) or Stacey P3. Pictures 3a) and 3b) can already be seen that the energies are close with the difference that in the picture 3a) Stacey P3 they begin to split and error begins to grow slowly. In the picture 4a) both energies begin to separate significantly while in the picture 4b) they begin to approach that sees the difference between the algorithms is Stacey Stacey P3 and P4. And Stacey among Stacey P3 and P4 with increasing interval in $\frac{\alpha}{\beta}$ it will grow error and if we go to the values for c = 6,5 and higher system will appear very large errors [7]. Tests were made as Stacey P3 for two seconds and Stacey P4 for two seconds and would present only difference in errors compared to the increase of the ratio $\frac{\alpha}{\beta}$. In picture 5 with the full line is designated algorithm Stacey P4 and with dashed line Stacey P3 and this is the error that occurs in both algorithms for a period of one second and thus notes that at the same time the error starts to increase, while in picture 6 are presented mistakes for interval of 2 seconds, and notes that many before the error starts to grow.

3. Additional Informatioin

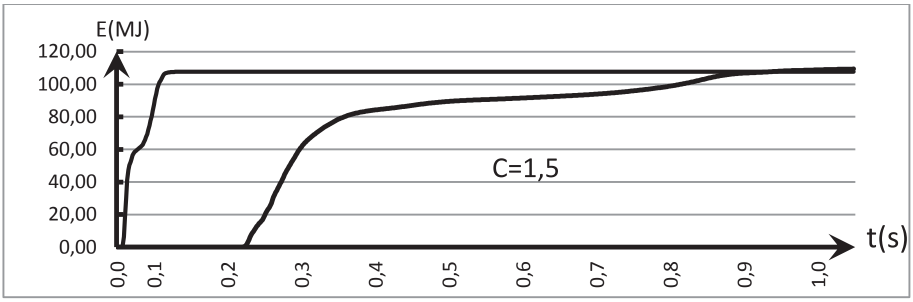
3.1. Pictures



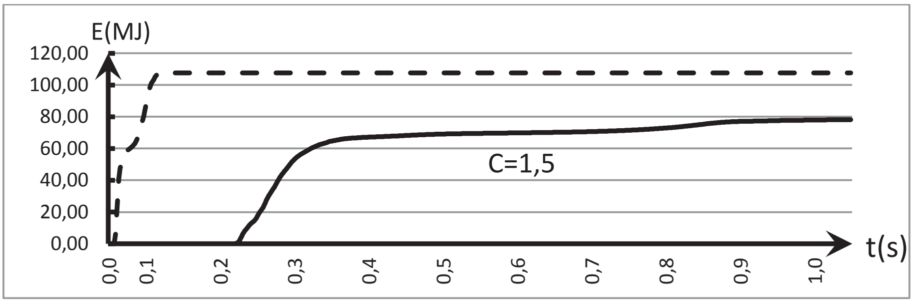
Picture 1a: Soil stretch that includes a source of explosion, free surfaces and three artificial boundaries



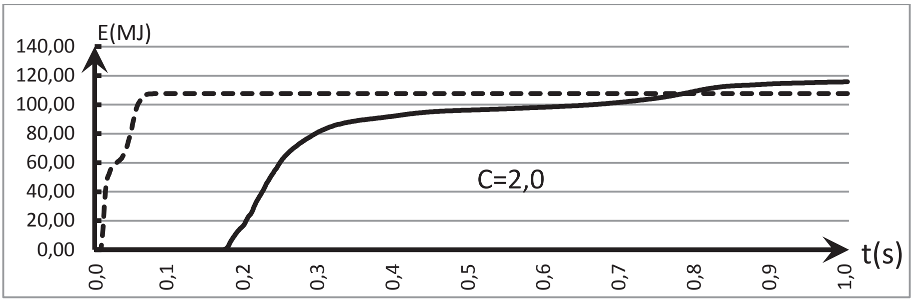
Picture 1b: Explosion source approximated polusinusoiden pulse with amplitude A = 0.5 m and duration td = 0,05 s



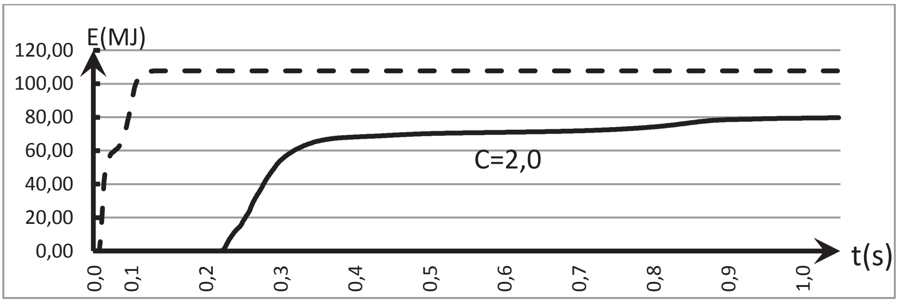
Picture 2a: Stacey P3, the dotted line represents the input power, the full line represents the power output in the ratio c = 1,5 in α/β



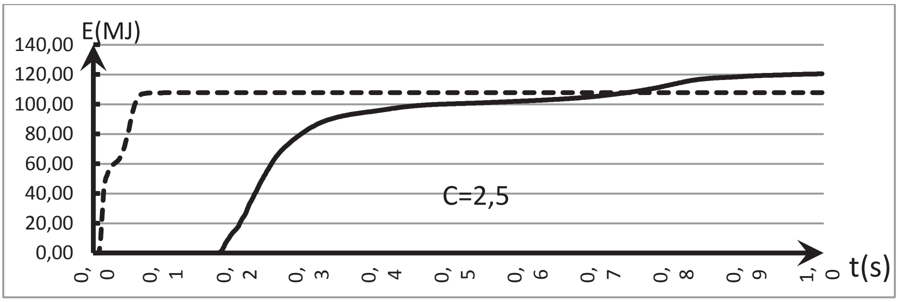
Picture 2b: Stacey P4, the dotted line represents the input power, the full line represents the power output in the ratio c = 1,5 in α/β



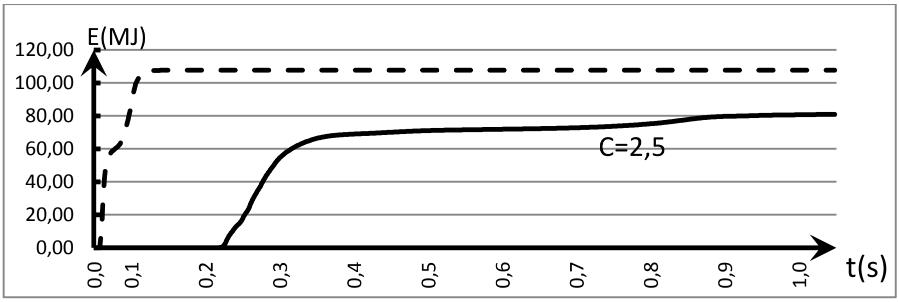
Picture 3a: Stacey P3, the dotted line represents the input power, the full line represents the power output in the ratio c = 2,0 in α/β



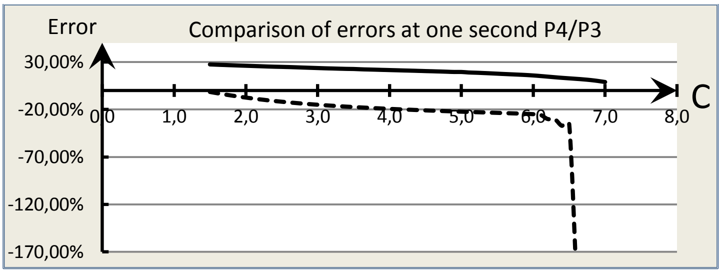
Picture 3b: Stacey P4, the dotted line represents the input power, the full line represents the power output in the ratio c = 2,0 in α/β



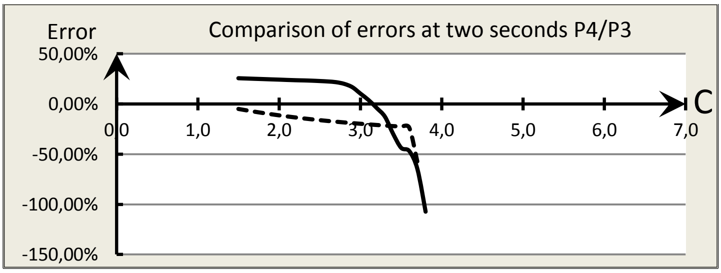
Picture 4a: Stacey P3, the dotted line represents the input power, the full line represents the power output in the ratio c = 2,5 in α/β



Picture 4b: Stacey P4, the dotted line represents the input power, the full line represents the power output in the ratio c = 2,5 in α/β



Picture 5: The full line represents the error in Stacey P4 while dotted is error in Stacey P3



Picture 6: The full line represents the error in Stacey P4 while dotted is error in Stacey P3

4. **Conclusion**

The stability and the accuracy of this border is of great importance, although there is many other boundary conditions. To say wich boundary condition is the best you need do make very large analysis and examinations about particular problem. In this paper has been found that between P3 and P4 boundary conditions of Stacey, P3 is better and more stable model. From the results obtained in this paper can be concluded that the stability interval is present betweeen ratio of the velocities of the tangential and compresional waves from 1.5 to 2.5. Thereby calculations are made for larger intervals, which indicates to which values of C P3 and P4 are stable. For real materials, 1.5 <C <2.5, P3 is more accurate than P4. The goal is to make better calculations that will be followed with more accurate applications for exploring the natural dislocations of the earth core.

5. **References**

[1] D.M. Boore (2003): Simulation of ground motion using the stochastic method, Pure and Applied Geophysics, 160, 635-676.

[2] K.R. Kelly, R.W. Ward, S. Treitel, R.M. Alford (February 1976): Synthetic Seismograms: A fiite difference approach, Geophysics Vol. 41, No. 1, pp 2-27.

[3] N. Dai, A. Vafidis, E. Kanasewich (February 1994): Composite Absorbing Boundaries for the Numerical Simulation of Seismic Waves, Bulletin of the seismological society of America, Vol. 84, No. 1, pp 185-191.

[4] R. B. Stacey "New Finite – Difference Methods for free surfaces with a stability analysis," Bulletin of the Seismological Society of America, vol. 84, No. 1, pp 171-184, February 1994.

[5] R.L.Higdon "Absorbing Boundary Conditions for elastic waves," Geopysics, vol. 56, No. 2, pp. 231-241, February 1991.

[6] ZP. Liao & H.L. Wong "A Transmitting Boundary for the numerical simulation of elastic wave propagation," in *Soil Dynamics and Earthquake Engineering 3,* 1984, 174-183

[7] Z. Zlatev (2012): *Numerical simulation of seismic waves propagation generated by explosions.* Masters thesis, University Goce Delcev- Stip.

CORRESPONDENCE BETWEEN ONE-PARAMETER GROUP OF LINEAR TRANSFORMATIONS AND LINEAR DIFFERENTIAL EQUATIONS THAT DESCRIBE DYNAMICAL SYSTEMS

Marija Miteva[1,*], Limonka Lazarova[2]

[1] Marija Miteva
Faculty of Computer Science
University of Goce Delcev
Stip, Republic of Macedonia
marija.miteva@ugd.edu.mk

[2] Limonka Lazarova
Faculty of Computer Science
University of Goce Delcev
Stip, Republic of Macedonia
limonka.lazarova@ugd.edu.mk

Abstract: Mathematical formalization of the notion of determined process leads to the notion of one-parameter group of linear transformations. In this paper we define one-parameter group of diffeomorphisms and see their relationship with vector fields, which connect the one-parameter group of diffeomorphisms with differential equations.

Key Words: deterministic process, phase velocity vector, vector field, diffeomorphism, phase space, phase flow, phase curve

1. Introduction and basic concepts

Starting with the definition of the derivative and differentiation of function, we know that the derivative characterizes some change. Therefore, many different processes in the nature, due to some change, can be described by differential equations.

The theory of ordinary differential equations is one of the basic instrument for the application of mathematics. Mathematical modeling of various scientific and engineering processes is based on systems of differential equations as a boundary problem. The most explored class of systems of differential equations, which are constructed by the experimentally established lawfulness in the process, is the class of autonomous systems. Apart from analytical solution of differential equation systems, the qualitative theory also uses geometric interpretation of the solution, defining phase space, so that any solution is a trajectory (curve) in that phase space, but the most important is kinematics interpretation which describes the solution as a motion of a point along a curve. The main assignment of the theory of differential equations is defining and exploring the motion of systems along phase velocity vector field. Or, in other words, exploring the problem for the type of phase curves, whether they remain in a bounded area or unlimited grow (periodic, stable, unstable solutions) [2, 4, 6, 9].

Basic concepts and definitions given bellow are taken from [10, 5, 3].

Definition 1.1: *A process is said to be deterministic if its entire future course and its entire past are uniquely determined by its state at the present instant of time. The set of all possible states of a process is called its phase space.*

Definition 1.2: *A process is said to be differentiable if its phase space has the structure of a differentiable manifold and if its change of state with time is described by differentiable functions.*

The motion of systems is usually described by the motion of the points along a curve in the phase space. The velocity of a motion of the phase point along that curve is determined by the point itself. That way, every point of the phase space determines a vector, called *phase velocity vector*. All phase velocity vectors form a *phase velocity vector field* in the phase space. This vector field determines the differential equation of the process.

Definition 1.3: *Transformation on a set is one-to-one mapping of the set onto itself.*

Definition 1.4: *A collection of transformations of a set is called a transformation group if it contains the inverse f^{-1} of each of its transformations f and the product fg of any two of its transformations f and g, with $(fg)(x) = f(g(x))$.*

If we consider this transformation group as a set A with defined two operations: $A \times A \to A$ and $A \to A$ ($(f, g) \to fg$ and $f \to f^{-1}$), then we are faced with the algebraic notion of abstract group. Here, the operation composition (product) of mappings is the basic operation, f^{-1} is inverse, and identity mapping is the unit in this group.

Now, let G be a group and M is a set.

Definition 1.5: *We say that it is given an action of the group G on a set M if for each element $g \in G$ there is a corresponding transformation $T_g : M \to M$ such that the corresponding transformation to the product of each two elements of G is a transformation which is product of the transformations corresponding to those two elements, while the corresponding transformation to each inverse element is appropriate inverse transformation, i.e.*

$$T_{fg} = T_f T_g \qquad\qquad T_{f^{-1}} = (T_f)^{-1}$$

We should mention that every transformation group on a set is action on that set. Actually, $T_g \equiv g$.

Transformation T_g is also called *action of the element* $g \in G$ on the set M . The action of the group G on the set M determines a mapping $T : G \times M \to M$ defined with: $(g, m) \to T_g m$. The element $T_g m = gm$ is obtained by the action of g on m . If we fix an element $m \in M$ and act on it by all the elements of the group G we will obtain the set $\{gm \mid g \in G\} \subseteq M$. We call this set the *orbit* of the point m .

Definition 1.6: *A one–parameter group of transformations of a set is an action on that set by the group of all real numbers.*

One–parameter group of transformations of a set M is usually denoted with $\{g^t\}$. Here, $g^t : M \to M$ is a transformation corresponding to the point $t \in R$. Actually, a one–parameter group of transformations on a set M is a collection of transformations g^t parametrized by the real parameter t such that for any real numbers s and t the following two relations hold:

1) $g^{t+s} = g^t g^s$
2) $g^{-t} = \left(g^t\right)^{-1}$.

The parameter t is usually called *time* and the transformation g^t is called *transformation in time t*.

The one–parameter group of transformations of a set is mathematical equivalent of the physical concept two-sided deterministic process. Let M

be a phase space of the process. Each point of that space is a definite state of the process. Assume that at the moment $t=0$ the process was in the state x. Then at another moment t the process will be at another state. Let us denote this new state of the process $g^t x$. This way for every $t \in R$ we define a mapping $g^t : M \to M$ from the phase space of the process into itself. The mapping g^t takes the state of the process at the moment 0 to the state at the moment t. We call this *transformation of the process in time t.*

The mapping g^t defined as above is really a transformation. This follows from the fact that, according to the definition of determinacy of the process, each state uniquely determines both the past and the future of the process. $g^{t+s} = g^t g^s$ property is also satisfied: suppose that at the initial moment the process was in the state x. The process could pass in a new state at the moment $t+s$ either directly ($x \to g^{t+s}x$), either first getting the state $g^t x$ in the time t and then see where this state $g^t x$ moves in time s.

Some concrete examples for application of one-parameter group of transformations while solving differential equations were given in [1].

The one-parameter group of transformations on a set M is also called *phase flow* with phase space M . The orbits of a phase flow are called its *phase curves* or *trajectories*. The points lying on a phase curves are called *fix point* of the flow.

Definition 1.7: *A smooth mapping, which inverse mapping is also smooth is called diffeomorphism (all coordinate functions and their inverse functions are smooth).*

Definition 1.8: *One-parameter group of diffeomorphisms is one-parameter group of transformations whose elements are diffeomorphisms satisfying the additional condition that $g^t x$ depends smoothly on both of the arguments t and x.*

See [8] for an application of diffeomorphisms in a dynamical systems.

Definition 1.9: *One-parameter group of linear transformations is a one-parameter group of diffeomorphisms whose elements are linear transformations.*

The phase velocity vector of the flow $\{g^t\}$ at the point $x \in M$ is the velocity with which the point $g^t x$ leaves x, *i.e.*

$$v(x) = \frac{d}{dt}\Big|_{t=0}(g^t x) \qquad (1)$$

The phase velocity vectors of a flow at all points of M form a smooth vector field (because $g^t x$ depends smoothly on t and x). It is the *phase velocity field*.

Definition 1.10: *The points where the phase velocity vector vanishes are called equilibrium points or singular points of the phase velocity field.*

Remark 1.1: *The fixed points of the flow are actually the singular points of the phase velocity field, i.e. the points where the phase velocity vector vanishes and vice versa.*

Definition 1.11: *Let $A: R^n \to R^n$ be a linear operator. A linear differential equation is an equation with the phase space R^n, defined by the vector field $v(x) = Ax$, i.e.*

$$x' = Ax \qquad (2)$$

If we fix a coordinate system x_i, $i = 1,...,n$ in R^n then the equation $x' = Ax$ can be written as a system of n equations

$$x_i' = \sum_{i=1}^{n} a_{ij} x_j \ , \qquad i = 1,...,n \qquad (3)$$

where $\lfloor a_{ij} \rfloor$ is the matrix of the operator A in the considered coordinate system.

So, the differential equation $v(x) = Ax$ is actually a system of n first order linear ordinary differential equations with constant coefficients.

Definition 1.12: *Let $A: R^n \to R^n$ be a linear operator. The operator e^A is defined on the following two equivalent ways:*

1) $e^A = E + A + \frac{A^2}{2!} + \frac{A^3}{3!} + ... + \frac{A^n}{n!} + ...$

2) $e^A = \lim_{n\to\infty}\left(E + \frac{A}{n}\right)^n$*, where E denotes identity operator.*

2. Correspondence between one-parameter group of linear transformations and differential equations

Let us fix a point x_0 and consider its motion under the action of the phase flow g^t. In other words, consider the mapping $\varphi : R \to M$ defined as follows:

$$\varphi(t) = g^t x_0 \tag{4}$$

Theorem 2.1: *The mapping φ is solution of the differential equation $x' = v(x)$ with initial condition $\varphi(0) = x_0$.*

Proof: Let

$$\varphi'(t) = \frac{d}{dt}\varphi(t) \tag{5}$$

be the first derivative of φ at the point t. We can also write it as:

$$\varphi'(t) = \frac{d}{d\tau}\Big|_{\tau=t}\varphi(\tau) \tag{6}$$

According to the definition of φ we obtain:

$$\frac{d}{d\tau}\Big|_{\tau=t}\varphi(\tau) = \frac{d}{d\tau}\Big|_{\tau=t} g^{\tau} x_0 \tag{7}$$

Introducing a new variable $u = \tau - t$ we obtain the expression:

$$\frac{d}{du}\Big|_{u=0}(g^{u+t}x_0) = \frac{d}{du}\Big|_{u=0}(g^u g^t x_0) = \frac{d}{du}\Big|_{u=0} g^u (g^t x_0) \tag{8}$$

According to (1), the last expression is equal to

$$v\left(g^t x_0\right) = v\left(\varphi(t)\right) \tag{9}$$

So, $\varphi(t)$ is the solution of the equation $x' = v(x)$.

About the initial condition,

$$\varphi(0) = g^0 x_0 = x_0 \tag{10}$$

thus we conclude that the initial condition is satisfied, too. □

Remark 2.1: *The converse is also true, i.e. the solution of differential equation $x' = v(x)$ with initial condition $\varphi(0) = x_0$ has the form $\varphi(t) = g^t x_0$. The proof follows directly from the existence and uniqueness theorem for the solution of first order differential equation which satisfies given initial condition.*

Thus, for each one-parameter diffeomorphism group there is associated differential equation, determined by the phase velocity vector field, which solution is a motion of the phase points under the action of the phase flow. If the phase flow describes any process with arbitrary initial conditions, then the differential equation defined by its phase velocity vector field determines the local low of evolution of the process. Knowing this local low of evolution, the theory of differential equations is supposed to reconstruct the past and predict the future. Establishing any low in the nature in a form of a differential equation reduces any problem about the evolution of the process (physical, chemical, ecological, biological process etc.) to a geometric problem for the behavior of the phase curves of given vector field in the corresponding phase space.

The phase flow of the differential equation $x' = v(x)$ is the one-parameter diffeomorphism group such that v is its phase velocity vector field.

Finding the phase flow of a differential equation, it suffices to find the solution of that equation. $g^t x_0$ is the value of the solution φ at the moment t with initial condition $\varphi(0) = x_0$.

Let $\{g^t \mid t \in R\}$ be a one-parameter group of linear transformations. Consider the motion $\varphi : R \to R^n$ of a point $x_0 \in R^n$. Let $A : R^n \to R^n$ be a linear operator defined by the relation

$$Ax = \frac{d}{dt}\Big|_{t=0} (g^t x), \quad \forall x \in R^n \tag{11}$$

Then, $\varphi(t)$ will be the solution of a differential equation $x' = Ax$ with the initial condition $\varphi(0) = x_0$. So, for describing a one-parameter group of linear transformations it is enough to explore the solutions of the linear equation $x' = Ax$ (the correspondence between one parameter group of linear transformations an differential equations is one-to-one and onto: each operator $A : R^n \to R^n$ defines a one-parameter group $\{g^t\}$).

Remark 2.2*: Let $A : R^n \to R^n$ be a linear operator. The family of all linear operators $e^{tA} : R^n \to R^n$, $t \in R$ (A is fixed) is one-parameter group of linear transformations, i.e.*

$$e^{(t+s)A} = e^{tA}e^{sA} \tag{12}$$

$$\frac{d}{dt}\left(e^{tA}\right) = Ae^{tA} \tag{13}$$

This can easily be proved just using the definition of operator e^{A} with an exponential series.

Theorem 2.2: *The solution $x = \varphi(t)$ of the equation $x' = Ax$ with initial condition $\varphi(0) = x_0$ has the form*

$$\varphi(t) = e^{tA}x_0 \tag{14}$$

Proof:

$$\varphi'(t) = \frac{d\varphi}{dt} = Ae^{tA}x_0 = A\varphi(t) \tag{15}$$

$$\varphi(0) = e^{0}x_0 = x_0 \tag{16}$$

Thus the theorem is proved. □

Theorem 2.3: *Let $\{g^{t} : R^{n} \to R^{n}\}$ be a one-parameter group of linear transformations. There exist a linear operator $A : R^{n} \to R^{n}$ such that*

$$g^{t} = e^{tA} \tag{17}$$

Proof: Set

$$A = \frac{dg^{t}}{dt}\Big|_{t=0} = \lim_{t\to 0}\frac{g^{t} - E}{t} \tag{18}$$

According to Definition 1.11 and Theorem 2.1, the motion $\varphi(t) = g^{t}x_0$ is a solution of the equation $x' = Ax$ with initial condition $\varphi(0) = x_0$. Then, according to the Theorem 2.2 we have

$$\varphi(t) = e^{tA}x_0 \tag{19}$$

and we now obtain

$$g^{t}x_0 = e^{tA}x_0 \tag{20}$$

i.e. $$g^{t} = e^{tA}$$ □

So, using this approach, we stated a correspondence between linear differential equations $x' = Ax$ and their flows $\{g^{t}\}$.

3. Conclusion

The notion of one-parameter group of transformations is actually a geometrization of the solution of system of differential equations. This could be particularly useful in the qualitative theory of differential equations which explores the behavior of systems in the phase space, instead of finding the explicit solution to them. If we consider a non-linear vector field with small non-linearity, we can linearized it if we expand it in a Taylor series in a neighborhood of the equilibrium point and omit the non-linear terms. That way we omit infinitely small terms of higher order, thus we can consider that the behavior of linearized and non-linear system in a neighborhood of the equilibrium point are closely related [7].

References:

[1] B. Piperevski, E. Asprovska, M. Nikolovska: *About one-parameter group of linear transformations.* Symposium on Differential equations 2010, Strumica, June 2010.

[2] E. Asprovska, B. Piperevski. *About stability of the solution of one class linear autonomous systems*. Symposium on Differential equations 2010, Strumica, June 2010.

[3] E. L. Ince (1956): *Ordinary Differential Equations*. Dover Publications, Inc. New York.

[4] G. Ioss, D. D. Joseph (1980): *Elementary Stability and Bifurcation Theory*. Springer-Verlag, New York, Heidelberg, Berlin.

[5] G. F. Torres del Castillo (2012): *Differentiable Manifolds*. Springer Science+Business Media, LLC

[6] M. Brin, G. Stuck (2002): *Introduction to Dynamical Systems*. Cambridge, University Press.

[7] M. Nikolovska (2011): *Models of Lorenz and its applications.* MSc thesis, Faculty of Electrical Engineering and Information Technologies, Skopje.

[8] S. Smale (1963): *Stable manifolds for differential equations and diffeomorphisms*. Annali della Scuola Normale Superiore di Pissa, Classe di Scienze, 3^{e} serie, Tome 17, No 1-2 pp.97-116

[9] S. Sastry (1999): *Nonlinear Systems, Analysis, Stability and Control*. Springer

[10] V. I. Arnold (1978): *Ordinary Differential Equations*. MIT

THE BLACK-SCHOLES MODEL AND VALUATION OF THE EUROPEAN CALL OPTION

Limonka Lazarova[1], Marija Miteva[2] and Natasa Stojkovik[3]

[1] limonka.lazarova@ugd.edu.mk [2] marija.miteva@ugd.edu.mk
[3] natasa.maksimova@ugd.edu.mk

Faculty of computer science, University “Goce Delcev” – Stip

Abstract: In this paper will be considered the simple continuous time model of Black-Scholes. The Black-Scholes formula for valuation of the European Call Option will be shown. It will be given a review of the background of this model and also the basic concepts of stochastic or Ito calculus that are necessary to explore the model.

Keywords and Phrases: Geometric Brownian motion, Ito integral, Ito formula, martingale, Black-Scholes formula.
Mathematics Subject Classification 2010: 91G80.

1. Introduction

The Black-Scholes Model was first discovered in 1973 by Fischer Black and Myron Scholes who developed a formula for valuation of European contingent claims based on geometric Brownian motion model for the stock price process. Robert Merton developed another method to derive the formula with more applicability and generalized the formula in many directions. It was for the development of the Black-Scholes Model that Scholes and Merton received the Nobel Prize of Economics in 1997 (Black had passed away two years earlier). The idea of the Black-Scholes Model was first published in "The Pricing of Options and Corporate Liabilities", of the Journal of Political Economy by Fischer Black and Myron Scholes, [4] and then elaborated in "Theory of Rational Option Pricing" by Robert Merton in 1973. Within six months of the publication of the Black-Scholes Model article, Texas Instruments had incorporated the Black-Scholes Model into their calculator, announcing the new feature with a half-page ad in The Wall Street Journal. The three young Black-Scholes Model researchers, which were still in their twenties, set about trying to find an answer to derivatives pricing using mathematics, exactly the way a physicist or an engineer approaches a problem. They had shown that mathematics could be applied using a little known technique known as stochastic differential equations and that discovery led to the development of the Black-Scholes Model that we know today.

Stochastic calculus or Ito calculus is one of the basic and main tools in finance, especially in the construction of the finance models in the theory of options. By using of the theory of probability and stochastic processes and by introducing of coincidence in the coefficients of differential equations is derived more realistic mathematical models. In [1], Bernt Oksendal elaborates some examples of stochastic models.

In order to describe the Black-Scholes model, the following definitions given in [6], [7] and [10] are necessary.

The stochastic process will be considered in complete filtrate space $(\Omega, \Im, P, (\Im_t, t \in T))$.

Definition 1.1 *The real valued stochastic process M is called martingale if:*

i) $(\forall t \geq 0),\ \ \exists E(M_t)$,

ii) $s < t \ \Rightarrow\ E(M_t \mid \Im_s) = M_s$.

X is semi martingale if $X = X_0 + M + A$, where X_0 is $\Im_0$ - measurable random variable, M is local martingale with value 0 in 0 and A is adapted process with continuous trajectories on the right with value 0 in 0 and paths are with finite variation.

Definition 1.2 *The real valued stochastic process $B = (B_t \mid t \in [0, +\infty))$ is called Brownian motion if:*

i) *B is adapted with a filtration $(\Im_t, t \in [0, +\infty))$;*

ii) *B has independent increments i.e.*
$\forall s,t\ (0 \leq s < t)$: $P(B_t - B_s \in A \mid \Im_s) = P(B_t - B_s \in A)$ *for every Borel set B;*

iii) *B has stationary increments i.e.*
$\forall s,t\ (0 \leq s < t)$: $B_t - B_s$ *has normal distribution* $N(\mu(t-s), \sigma^2(t-s))$

iv) $P(B_0 = x) = 1,\ \ (x \in R)$.

The most important Brownian motion for modeling of the financial models is geometric Brownian motion.

Definition 1.3 *If* $\{B(t),t \geq 0\}$ *is Brownian motion, then stochastic process* $\{Y(t),t \geq 0\}$*, defined by* $Y(t) = e^{B(t)}$ *is geometric Brownian motion.*

The fact that traditional differentiation and integration could not be applied in stochastic calculus implies finding new methods and procedures of differentiation and integration. These new tools were developed for the first time by Ito (1944), who proved Ito lemma and Ito formula. This formula is very important in stochastic calculus, especially in stochastic models in the finance.

The following definitions are given in [5].

Definition 1.4 *Let* $f(t,\omega):[0,\infty)\times\Omega \to R$ *, such hat* $f(t,\omega)$ *e* $B\times\Im$ *- measurable (*B *is Borel* σ *- algebra on* $[0,\infty)$*),* $f(t,\omega)$ *is* $\Im_t$ *- adapted and*

$$E\left[\int_0^t f(s,\omega)^2 ds\right] < \infty .$$

Ito integral to the function f *is defined by:*

$$\int_0^t f(s,\omega)dB_s(\omega) = \lim_{n\to\infty}\int_0^t H_n(s,\omega)dB_s(\omega) , \qquad \text{(limit in } L^2 \text{)}$$

(1)

Where (H_n) *is sequence elementary function, for which:*

$$E\left[\int_0^t (f(s,\omega) - H_n(s,\omega))^2 ds\right] \to 0, \quad when\ \ n \to \infty .$$

The Ito integral is very important in financial mathematics. For example, if stochastic process Z_t is price of the stock, then stochastic integral $\int_0^t H_s dZ_s$ is showing the gain or the loss at the disposal with H_s shares of the stock at time s .

Definition 1.5 *Let* $f:R\to R$ *is* C^2 *- function and* B_t *is Brownian motion. The one dimensional Ito formula is given by:*

$$f(B_t) - f(B_0) = \int_0^t f'(B_s)dB_s + \frac{1}{2}\int_0^t f''(B_s)dB_s \qquad (2)$$

2. The Black Scholes continuous time model

The most famous model, which is used in finance, long time ago is the model in which the stock price can be described with Brownian motion. At the beginning this model, in which the stock price is described with many Brownian motions, was not accepted because of two reasons. One of the reasons is that the Brownian motion can receive a negative value, but the option price cannot be negative. The other reason we can see in the following example: if an investor invests 10000$ on sale of shares of the stock, each of 100$ and if the stock price is increased to 200$, then the investor will have profit 10000$. Also, if that 10000$ are invested on sale of shares, each of the stock 1000$, and then the price is increased on 2000$, so in this case the investor will have the same profit of 10000$. It follows that there are proportional increments, but the Brownian motion has stationary and independent increments. Because of that, the random variables $\frac{\Delta S_t}{S_t}$ can be described with the process of Brownian motion, where S_t is stock price process.

The different stocks have different volatility σ. It is expected that the rate of return μ is greater than risk free rate r, because every investor expects higher profit, with which would be recover the takeover risk.

For modeling stock price it will be used stochastic differential equation $\frac{dS_t}{S_t} = \sigma dB_t + \mu dt$, or equivalent integral form:

$$S_t = S_0 + \int_0^t S_s \sigma dB_s + \int_0^t S_s \mu ds \quad , \qquad (3)$$

where B_t is Brownian motion.

This stochastic differential equation can be solved explicitly, and its solution is given in the following theorem:

Theorem 2.1 *The solution of the stochastic differential equation* $dS_t = \sigma S_t dB_t + \mu S_t dt$ *is given with process of geometric Brownian motion.*

Proof: From [12], is following that there is at most one solution of $dS_t = \sigma S_t dB_t + \mu S_t dt$.

We assume that the stock price in initial moment 0 is $S_0 = 1$. We will apply the one-dimensional Ito formula (2) to the function $f(x) = e^x$, so we get

$$S_t = e^{X_t} = e^{X_0} + \int_0^t e^{X_s} dX_s + \frac{1}{2}\int_0^t e^{X_s} d\langle X\rangle_s = 1 + \int_0^t S_s \sigma dB_s + \int_0^t S_s\left(\mu - \frac{1}{2}\sigma^2\right)ds + \frac{1}{2}\int_0^t$$

$$= 1 + \int_0^t S_s \sigma dB_s + \int_0^t S_s \mu ds.$$

[

Ve assume that the interest rate r e 0, without loss of generality. Let s vestor buys Δ_0 shares of stock at time t_0 .The investing in shares of tne sτocκ at time t_1 has changed to Δ_1 shares of the stock, Δ_2 shares of the stock at time t_2 etc. In this case, the investor’s wealth at time t is given by:

$$X_{t_0} + \Delta_0\left(S_{t_1} - S_{t_0}\right) + \Delta_1\left(S_{t_2} - S_{t_1}\right) + \ldots + \Delta_i\left(S_{t_{i+1}} - S_{t_i}\right) \qquad .$$

(4)

That means that at the time t_0 the investor has an initial wealth X_{t_0} . If investor buys Δ_0 shares of stock and each of the share with price S_{t_0} , it will cost $\Delta_0 S_{t_0}$ and if at the moment t_1 , buys Δ_0 shares of the stock by price S_{t_1} , then the investor’s wealth will be $X_{t_0} + \Delta_0\left(S_{t_1} - S_{t_0}\right)$. This procedure continues in the other time points $t_1, t_2, \ldots$ so we get the relation (4). The relation (4) can be written in the form:

$$X_{t_0} + \int_0^t \Delta(s) dS_s \qquad ,$$

(5)

where $t \geq t_{i+1}$ and $\Delta(s) = \Delta_i$ for $t_i \leq s < t_{i+1}$. The wealth of the investor is given by Ito integral (1) in terms of the stock price. The integrand must be adapted process with respect to the filtration on the probability space $(\Omega, \Im, P)$, because the number of shares of the stock which investor posses at time s cannot be based on future information.

Next, we will consider the case when interest rate r is not equal to 0. Let $P_t = e^{-rt} S_t$ is current stock price, and let $P_0 = S_0$. If we have Δ_i shares of the stock in the time period $[t_i, t_{i+1})$, the wealth of the investor will be $\Delta_i\left(P_{t_{i+1}} - P_{t_i}\right)$. So the process of investor’s wealth will be:

$$X_{t_0}+\int_{t_0}^{t}\Delta(s)dP_s\,.$$

If we apply the Ito product formula given in [8], [11], we derive the stochastic differential equation

$$dP_t=\sigma P_t dB_t+(\mu-r)P_t dt \qquad (6)$$

and its solution $P_t=P_0\exp\left(\sigma B_t+\left(\mu-r-\frac{\sigma^2}{2}\right)t\right)$ is similar with the solution to the equation (3).

The following theorem shows the completeness of the continuous time model, [9].

Theorem 2.2 *If* P_t *is geometric Brownian motion and if the price of option* V *is* $\Im_t$ *- measurable and square-integrable, then there is a constant* c *and adapted process* K_s *, such that* $V=c+\int_0^t K_s dP_s$ *. Moreover there is a probability measure* $\overline{P}$ *in terms of which* P_t *is martingale.*

Proof: Let P_t is geometric Brownian motion and let $P_t=P_0\exp\left(\sigma B_t+\left(\mu-r-\frac{\sigma^2}{2}\right)t\right)$, i.e. in differential form $dP_t=\sigma P_t dB_t+(\mu-r)P_t dt$. We define a new probability measure $\overline{P}$ with:

$$\frac{d\overline{P}}{dP}=M_t=\exp\left(aB_t-\frac{a^2t}{2}\right).$$

From Girsanov theorem [9], $\widetilde{B}_t=B_t-at$ is Brownian motion with respect to the probability measure $\overline{P}$. It follows that:

$$dP_t=\sigma P_t d\widetilde{B}_t+\sigma a P_t dt+(\mu-r)P_t dt\,.$$

If we choose that $a = -\frac{(\mu - r)}{\sigma}$, we obtain:

$$dP_t = \sigma P_t d\widetilde{B}_t \quad . \tag{7}$$

$\widetilde{B}_t$ is Brownian motion with respect to the probability measure $\overline{P}$, so it follows that P_t is martingale, because it is presented as Ito integral, which is martingale. The equation (7), can be written as

$$d\widetilde{B}_t = \sigma^{-1} P_t^{-1} dP_t \quad . \tag{8}$$

If the price of the option V is $\Im_t$ - measurable, from the martingale representation theorem in [2] it follows that exists adapted process H_s such that $\int_0^t H_s^2 ds < \infty$ and $V = c + \int_0^t H_s d\widetilde{B}_s$. By using to the equation (8) follows that:

$$V = c + \int_0^t H_s \sigma^{-1} P_t^{-1} dP_s \ . \qquad \square$$

3. Valuation of the European Call Option with Black Scholes formula

We will derive a formula for valuation of the arbitrary option. Let $T \geq 0$ is fixed real number. If the price of arbitrary option V is $\Im_T$ - measurable, then from theorem 2.2, it follows that

$$V = c + \int_0^t K_s dP_s . \tag{9}$$

and with respect to the probability measure $\overline{P}$, the process P_t is martingale.

Theorem 3.1 *The price of the option* V *is* $\overline{E}V$ *.*

Proof: This is no arbitrage principle (risk-free profit). Suppose that the price of the option$V$, in initial time is W_0. If investor starts with 0$, then he can sell the option V for W_0 dollars and to use this money to buy and trade with shares of stock. If he uses c dollars of this income and if invests in accordance with the strategy of owning K_s shares of stock at time s , then at the time of maturity of the option V , i.e. at time T will be:

$e^{rT}(W_0 - c) + V$ $.

At the time of maturity$T$, the buyer of the option V uses the option and the seller of the option used V dollars to fulfill his obligation. In this way the profits of the seller of the option would be $e^{-rT}(W_0 - c) + V$ if $W_0 > c$, without risk. From here it follows that$W_0 \leq c$. If $W_0 < c$, then the opposite happens, i.e. the investor buys option instead of to sell the option and to own $-K_s$ shares of the option at the time s . Since we cannot have a risk-free profit, it is following that $W_0 \geq c$ or$W_0 = c$.

With respect to the probability measure $\overline{P}$, the process P_t is martingale. The mathematical expectation of the expression (9) is:

$$\overline{E}V = \overline{E}\left[c + \int_0^t K_s dP_s\right] = c = W_0 = V \qquad .$$

□

For valuation of the arbitrary option, the formula (9) is not appropriate. Suppose that V is standard European call option, where

$$V = e^{-rt}(S_t - K)^+ = \left(e^{-rt}S_t - e^{-rt}K\right)^+ = \left(P_t - e^{-rt}K\right)^+ .$$

With respect to the probability measure $\overline{P}$, the stock price is given by $dP_t = \sigma P_t d\widetilde{B}_t$, where $\widetilde{B}_t$ is Brownian motion with respect to the probability measure $\overline{P}$. It follows that for the stock price we have $P_t = P_0 \exp\left(\sigma\widetilde{B}_t - \left(\frac{\sigma^2}{2}\right)t\right)$. It follows that:

$$\overline{E}V=\overline{E}\left[\left(P_T-e^{-rT}K\right)^+\right]=\overline{E}\left[\left(P_0\exp\left(\sigma\widetilde{B}_T-\left(\frac{\sigma^2}{2}\right)T\right)-e^{-rT}K\right)^+\right].$$

(10)

Because $\widetilde{B}_T$ is process of the Brownian motion, i.e. its increments are random variables with normal distribution, it follows that the density function is given by $p_{\widetilde{B}_T}=\frac{1}{\sqrt{2\pi T}}e^{-\frac{y^2}{(2T)}}$.

If we do some calculations we can obtain the Black-Scholes formula:

$$W_0=x\Phi(g(x,T))-Ke^{-rT}\Phi(h(x,T)),$$

where $\Phi(z)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z}e^{-\frac{y^2}{2}}dy,\quad x=P_0=S_0$.

$$g(x,T)=\frac{\log\left(\frac{x}{K}\right)+\left(r+\frac{\sigma^2}{2}\right)T}{\sigma\sqrt{T}},\qquad h(x,T)=g(x,T)-\sigma\sqrt{T}.$$

The Black-Scholes formula depends of the volatility σ, but it does not depend of the rate of return μ. The stock price is given by $dP_t=\sigma P_t d\widetilde{B}_t$, where $\widetilde{B}_t$ is Brownian motion with respect to the probability measure $\overline{P}$. It follows that for the stock price the equation $P_t=P_0\exp\left(\sigma\widetilde{B}_t-\left(\frac{\sigma^2}{2}\right)t\right)$ hold. The rate of return μ is not present in this expression, because when the Girsanov theorem is applied, we have probability $\overline{P}$, which is risk neutral.

From the equation (10) we obtain:

$$\overline{E}V=\overline{E}\left[\left(P_T-e^{-rT}K\right)^+\right]=$$

$$=\overline{E}\left[\left(P_0\exp\left(\sigma\widetilde{B}_T-\left(\frac{\sigma^2}{2}\right)T\right)-e^{-rT}K\right)^+\right]=\overline{E}\left[\left(x\exp\left(\sigma\widetilde{B}_T-\left(\frac{\sigma^2}{2}\right)T\right)-e^{-rT}K\right)^+\right]$$

where $\tilde{B}_t$ is Brownian motion with respect to the probability measure $\overline{P}$. Instead of $S_0 = P_0$ we will use x. Because $\tilde{B}_T$ is normal random variable with mathematical expectation 0 and variance T, then we can write as $\sqrt{T}Z$ where Z is random variable with standard normal distribution i.e. with mathematical expectation 0 and variance 1.

Because the expression $$x\exp\left(\sigma\tilde{B}_T - \left(\frac{\sigma^2}{2}\right)T\right) > e^{-rT}K$$

hold, if and only if: $$\log x + \sigma\sqrt{T}Z - \left(\frac{\sigma^2}{2}\right)T > -rT + \log K$$

or: $$Z > \left(\frac{\sigma^2}{2}\right)T - rT + \log K - \log x,$$

then if we write $z_0 = \left(\frac{\sigma^2}{2}\right)T - rT + \log K - \log x$, and if we consider that for Φ $\Phi(-z) = 1 - \Phi(z)$, hold, we will have:

$$\overline{E}V = \overline{E}\left[\left(P_T - e^{-rT}K\right)^+\right] =$$

$$= \overline{E}\left[\left(P_0\exp\left(\sigma\sqrt{T}z - \left(\frac{\sigma^2}{2}\right)T\right) - e^{-rT}K\right)^+\right] = \overline{E}\left[\left(x\exp\left(\sigma\sqrt{T}z - \left(\frac{\sigma^2}{2}\right)T\right) - e^{-rT}K\right)^+\right] =$$

$$= \frac{1}{\sqrt{2\pi}}\int_{z_0}^{\infty}\left(x\exp\left(\sigma\sqrt{T}z - \left(\frac{\sigma^2}{2}\right)T\right) - e^{-rT}K\right)^+ \exp\left(-\frac{z^2}{2}\right)dz =$$

$$= x\frac{1}{\sqrt{2\pi}}\int_{z_0}^{\infty}\exp\left(-\frac{1}{2}\left(z^2-2\sigma\sqrt{T}z+\sigma^2T\right)\right)dz-e^{-rT}K\int_{z_0}^{\infty}\exp\left(-\frac{z^2}{2}\right)dz$$

$$= x\frac{1}{\sqrt{2\pi}}\int_{z_0}^{\infty}\exp\left(-\frac{1}{2}\left(z-\sigma\sqrt{T}\right)^2\right)dz-e^{-rT}K\left(1-\Phi(z_0)\right)=$$

$$= x\frac{1}{\sqrt{2\pi}}\int_{z_0-\sigma\sqrt{T}}^{\infty}\exp\left(-\frac{1}{2}y^2\right)dy-e^{-rT}K\Phi(-z_0)=$$

$$= x\left(1-\Phi\left(z_0-\sigma\sqrt{T}\right)\right)-e^{-rT}K\Phi(-z_0)=x\Phi\left(\sigma\sqrt{T}-z_0\right)-Ke^{-rT}\Phi(-z_0).$$

The last formula is formula for valuation of the European call option with strike price K and time to maturity T, if $\sigma\sqrt{T}-z_0=g(x,T)$ and $-z_0=h(x,T)$.

4. Conclusion

In this paper we have reviewed the Black-Scholes model and we have applied Black-Scholes formula for valuation of European Call Option. It is shown that the Brownian motion can be used for modeling stock price from some financial data. We can conclude that despite their popularity and wide spread use, the model is built on some non-real life assumptions about the market, [3]. It assumes stocks move in a manner referred to as a random walk, risk free rate, no transaction costs and it assumes European-style options which can only be exercised on the expiration date.

References

[1] B. Oksendal, Stochastic differential equation. An introduction with applications, 5th. ed. Springer-Verlag Heidelberg New York,(2000) p. 1-4.

[2] D. Nularet , Stochastic Processes, p.68-113.

[3] D. Teneng, Limitations of the Black-Scholes Model, International Research Journal of Finance and Economics

ISSN 1450-2887 Issue 68 (2011), © EuroJournals Publishing, Inc. 2011

[4] F.Black, M. Scholes, The Pricing of Options and Corporate Liabilities, The Journal of Political Economy, Volume 81, Issue 3, (May-June, 1973), p.637-654.

[5] E.Allen, Modelling with Ito Stochastic Differential Equations, Springer (2007),

[6] I. Karatzas and S. Shreve. Brownian Motion and Stochastic Calculus. Springer. 1998, p.1-22

[7] J. Janssen, R. Manca, E. Volpe di Prignano, Mathematical Finance, Deterministic and Stochastic Models, p.517-540, 641-672

[8] R. F. Bass, The Basics of Financial Mathematics, Department of Mathematics, University of Connecticut, (2003), p.1-43

[9] R.J. Williams. Introduction to the Mathematics of Finance. American Mathematical Society. 2006

[10] S. M. Ross, Stochastic Processes, University of California, Berkeley, John Wiley \& Sons, Inc (1996), p.295-405

[11] S.Shreve, Stochastic Calculus and Finance, Carnegie Mellon University, (1997), p.153-175.

[12] T. G. Kurtz, Lectures on Stochastic Analysis, Departments of Mathematics and Statistics University of Wisconsin - Madison (2009), p.42-53

BITCOIN SCHEMES- INOVATION OR A THREAT TO FINANCIAL STABILITY?

Violeta Madzova PhD[23]

Abstract:

A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. The recent developments in widely spread internet and data mining activities, highlighted the issue of accepting and using virtual currencies for different purposes, including, buying commodities or services, saving, as well as converting into real currencies, such as US dollars, euro or other currencies.

One of the most controversial and the most advanced virtual currency scheme to date is the one so-called Bitcoin, designed and implemented by the Japanese programmer Satoshi Nakamoto in 2009. Although the use of Bitcoin might have positive impact on financial innovation and the provision of additional payment alternatives to consumers, it also might increase the risks in financial payments, exchange rates of real currencies, as well as increase the possibility of money laundering, using them for illegal deeds.

Therefore , the purpose of this paper to clarify the main characteristic of Bitcoin, and analyze its positive aspects as well as the threats that may occur to the modern world economy , in case the usage of this money , significantly increases .

Keywords: virtual currency ,e-money, financial and price stability, risks

Introduction

Money is a social institution: a tool created and marked by society’s evolution, which has exhibited a great capacity to evolve and adapt to the character of the times .Economists differentiate among three different types of money:**commodity money, fiat money**, and **bank money.** While **commodity money** (such as gold coins) is no longer performing its originate function , so called **“fiat money”** [24] , as well as **bank money** (checks issued by banks) have took its place and are widely used in all modern economies.

[23] Author is assistant professor at the University “Goce Delcev”-Faculty of Economics-Stip, e-mail:violeta.madzova@ugd.edu.mk

[24] Fiat money is a good, the value of which is less than the value it represents as money. Dollar bills and banknotes are examples of fiat money

Being issued by the central banks, people have accepted fiat money in exchange for goods and services, simply because they trust this central authority which is crucial element of any fiat money system.

Additional reason for wide acceptance of fiat money is of course, possibility to unite three different money functions into one, i.e. money can be:

-used as a mean of exchange -intermediary in trade to avoid barter system,
-used as a standard numerical unit for the measurement of value .
-saved and used as a store of value for the future times.

Due to the recent technological developments and especially high penetration of the internet, there has also been a development of virtual communities in recent years. A virtual community [25] is to be understood as a place within cyberspace where individuals interact and follow mutual interests or goals. In some cases, these virtual communities have created and circulated their own digital currency for exchanging the goods and services they offer, thereby creating a new form of digital money . These money can have positive aspects if they contribute to financial innovation and provide additional payment alternatives to consumers.

However, it is clear that they can also pose risks for their users, especially in view of the current lack of regulation.In fact, virtual currencies act as a medium of exchange and as a unit of account within a particular virtual community. The question then arises as to whether they also fulfil the “store of value” function in terms of being reliable and safe, or whether they pose a risk not only for their users but also the wider economy.

Virtual currency schemes in the new e-communities

A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.

The virtual currency schemes are still new and there is still vague understanding of their nature, thus mix them with so called “electronic money”. Namely, as it is stated in the Electronic Money Directive (2009/110/EC), “electronic money” is monetary value as represented by a claim on the issuer which is: stored electronically; issued on receipt of funds of an amount not less in value than the monetary value issued; and accepted as a means of payment by undertakings other than the issuer.

[25] There are many examples of virtual economies, in terms of social networks(Facebook, MySpace, Twitter), knowledge virtual community (Wikipedia), or those that create a virtual world (Second Life) or create an online environment for gambling (Online Vegas Casino).

Although some of these criteria are also met by virtual currencies, a clear distinction should be made between virtual currency schemes and electronic money. i.e:

- In electronic money schemes the link between the electronic money and the traditional money format is preserved and has a legal foundation, as the stored funds are expressed in the same unit of account (e.g. US dollars, euro, etc.).
- In virtual currency schemes the unit of account is changed into a virtual one.
- Electronic money schemes are regulated and electronic money institutions that issue means of payment in the form of electronic money are subject to prudential supervisory requirements. This is not the case for virtual currency schemes.
- Electronic money is primarily subject to the operational risk associated with potential disruptions to the system on which the electronic money is stored.
- Virtual currencies are not only affected by credit, liquidity and operational risk without any kind of underlying legal framework, these schemes are also subject to legal uncertainty and fraud risk, as a result of their lack of regulation and public oversight.

It is important to underline that, there three types of virtual currency schemes which depens on their interaction with traditional, “real” money and the real economy:[26]

- **Type 1**, which is used to refer to closed virtual currency schemes, basically used in an online game;

- **Type 2** virtual currency schemes have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can subsequently be used to buy virtual goods and services, but exceptionally also to buy real goods and services;

-**Type 3** virtual currency schemes have bidirectional flows, i.e. the virtual currency in this respect acts like any other convertible currency, with two exchange rates (buy and sell), which can subsequently be used to buy virtual goods and services, but also to purchase real goods and services.

One of the most typical and developed “type 3” virtual currency is so called Bitcoin. In fact Bitcoin shares characteristics of both commodity money and fiat money, but does not fit properly in either category. Bitcoin supersedes

[26] See more : BRODBECK, Simon “Virtual money – A new form of privately issued money in the money market”, European School of Management, Paris, May 2007.

commodity money in value density, recognizability and divisibility. It also resembles commodity money in that, at least during the expansion of the Bitcoin base, its value, assuming competing suppliers, is equal to its marginal cost of production. However, unlike commodity money, bitcoins, which exist only as numbers in a computer, have zero value as a commodity in the real world. On the other hand, fiat money commands a value far higher than its costs of production, which raises the risk of mismanagement by their monopolistic suppliers.

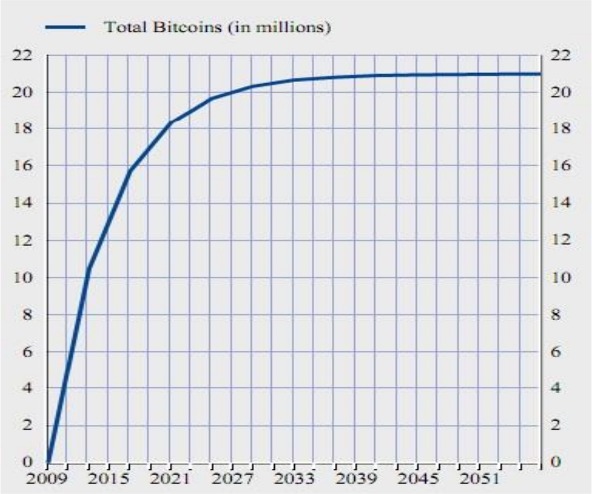
The nature of a Bitcoin as a virtual currency scheme

Bitcoin is decentralized virtual currency , which is traded on line and is exchanged into US dollars or other currencies. Bitcoin , allows users to mine buy, sell or accept bitcoins from anywhere in the world. However , no matter how much worldwide bitcoin community is spread over , it doesn’t have centralized data base or authority, but a peer to peer network. It enables creation of bitcoins through mining process and validates the transactions. According to the latest information there are over 8,8 million coins in circulation[27]. Estimating the bitcoin price at the level of 4-5US dollar/per 1 Bitcoin , the Bitcoin community value is estimated between 35-44 million US dollars.

According to Bitcoin, the scheme has been technically designed in such a way that the money supply will develop at a predictable pace. The number of Bitcoins generated per block isset to decrease geometrically, with a 50% reduction every four years. The result is that the number of Bitcoins in existence will reach 21 million in around 2040. (see: Table 1)\

[27] European Central Bank, “Virtual currency schemes “October 2012, pg 18 http://www.ecb.europa.eu/home/html/index.en.htm

Table 1: Trend of bitcoin over time



Source : http://www.ecb.int/pub/pdf/other

Bitcoins are not pegged to any real-world currency. The exchange rate is determined by supply and demand in the market.

There are several exchange platforms for buying Bitcoins that operate in real time, such as Mt.Gox which is the most widely used currency exchange platform and allows users to trade US dollars for Bitcoins and vice versa.

In order to start using Bitcoins, users need to download the free and open-source software. Purchased Bitcoins are thereafter stored in a digital wallet on the user's computer. Consequently, users face the risk of losing their money if they don't implement adequate antivirus and back-up measures.

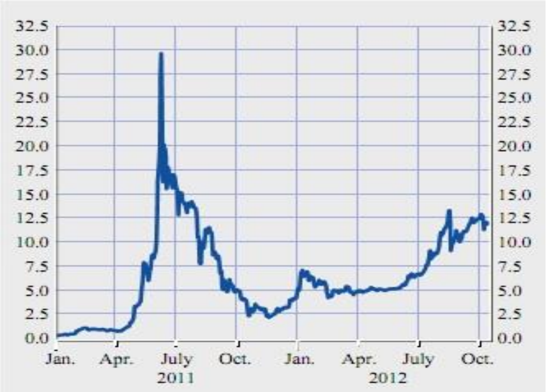
However, it is also true that the system demonstrates a clear case of information asymmetry. It is complex and therefore not easy for all potential users to understand. At the same time, users can easily download the application and start using it even if they do not actually know how the system works and which risks they are actually taking. This fact, in a context where there is clear legal uncertainty and lack of close oversight, leads to a high-risk situation.

The turbulent path of a Bitcoin

Bitcoin, the infamous pseudonymous cryptocurrency with no centralized authority, has had a tumultuous history so far.In 2008, Satoshi Nakamoto selfpublished a paper outlining his work on The Cryptography Mailing list at metzdowd.com and then on 3 January 2009 released the open source project called Bitcoin and created the first block, called the "Genesis Block"[28]. Through 2009 and early 2010, bitcoins had no value at all, and for the first six months after they started trading in April 2010, the value of one bitcoin stayed below 14 cents. Then, as the currency gained viral traction in summer 2010, rising demand for a limited supply caused the price on online exchanges to start moving so by November 2010 , it surged to 36 cents , while in February 2011, it rose again and it hit USD 1,06 before settling in at roughly 87 cents. From early April 2011 to the end of May 2011, the going rate for a bitcoin rose from 86 cents to USD 8,89. The highest pic was reached at the beginning of June when the market value of all bitcoins in circulation has tripled and was approaching USD 130 million. Then , cyberattack perpetrated on 20 June 2011, managed to decrease the value of the currency down from USD 17,50 to USD 0,01 within several minutes. According to currency exchange Mt.Gox platform , one account with a lot of Bitcoins was compromised and the stolen lot was first sold out and then bought back again, with the intention of withdrawing the coins. The USD 1,000/day withdrawal limit was active for this account and the hacker was only able to exchange USD 1.000 worth of Bitcoins. Apart from this, no other accounts were compromised, and nothing was lost. The price dramatically dropped down , but it quickly drove it back up, limiting the thief's haul to only around 2.000 bitcoins. The exchange ceased operations for a week and rolled back the post-crash transactions, but the damage had been done as the bitcoin never got back above $17. [29] (see Table 2)

[28] Benjamin Wallace, "The rise and fall of a BITCOIN"; November 23,2011, pg2

Table 2:Bitcoin exchange rate over time



source: htpp://bitcoincharts.com /charts

Monetary aspects of the Bitcoin virtual currency scheme

As the Bitcoin scheme is designed as a decentralized system where no central monetary authority is involved, the supply of money does not depend on the monetary policy of any virtual central bank, but rather evolves based on interested users performing a specific activity.

Therefore, users have several incentives to use Bitcoins.

1. Transactions are anonymous, as accounts are not registered and Bitcoins are sent directly from one computer to another.
2. Users have the possibility of generating multiple Bitcoin addresses to differentiate or isolate transactions.
3. Transactions are carried out faster and more cheaply than with traditional means of payment. Transactions fees, if any, are very low and no bank account fee is charged.

Bitcoin users buy and sell the currency among themselves without any kind of intermediation and therefore, it seems that nobody benefits from the system, apart from those who benefit from the exchange rate evolution (just as in any other currency trade) or those who are hard-working “miners” and are therefore rewarded for their contribution to the security and confidence in the system as a whole.Also, the scheme does not promise high returns to anybody. Although some Bitcoin users may try to profit from exchange rate fluctuations, Bitcoins are not intended to be an investment vehicle, just a medium of exchange.

However there are still concerns if the Bitcoin schemes might generate potential risks regarding payment or even financial stability in the modern economies. Having in mind the small scope of all virtual currency

schemes including Bitcoins, these risks do not affect anyone other than the users of the schemes. But, it can be expected that the growth of virtual currencies will most likely continue, triggered by several factors:
a) the growing access to and use of the internet and the growing number of virtual community users,
b) the increase of electronic commerce and in particular digital goods, which is the ideal platform for virtual currency schemes;
c) the higher degree of anonymity compared to other electronic payment instruments that can be achieved by paying with virtual currencies;
d) the lower transaction costs, compared with traditional payment systems;
e) the more direct and faster clearing and settlement of transactions, which is needed and desired in virtual communities.
Therefore, by assuming that Bitcoin as virtual currency scheme will continue to grow, periodical examination of the developments is needed in order to consider the potential risks more carefully.

What types of risks might occur ?

Bitcoin as a virtual currency payment arrangement has evolved into “real” payment systems within the specific virtual community. In contrast to traditional payment systems, it ise not regulated or closely overseen by any public authority. Participation in this scheme exposes their users to credit, liquidity, operational and legal risks within the virtual communities; but no systemic risk outside these communities can be expected to materialise in the current situation.

More precisely the following types of risks might occur by using the Bitcoin currency scheme[30]:
-*Credit risk*-Users are exposed to credit risk in relation to any funds
held on the virtual accounts, as it cannot be guaranteed that the settlement institution is able to fully meet its financial obligations when these are due or at any time in the future.
-*Liquidity risk* -Users are also exposed to liquidity risks if the settlement institution fails to meet any commitments it has made to provide liquidity to the participants as and when expected.In this regard, virtual currency schemes are very illiquid as a result of the low volumes traded.In the event of security incidents, the conversion of users’ funds into real money would probably not occur quickly without a significant material loss in value.

[30] See :BIS, “The role of central bank money in payment systems”, CPSS Publications, No 55,August 2003

-*Operational risk*-Both payer and payee need to have accounts with the settlement institution and are therefore reliant on the soundness of its operational and business continuity.
-*Legal risk*-There are many legal uncertainties regarding virtual currency schemes. In virtual currency schemes, the lack of a proper legal framework substantially exacerbates the other risks. Even more, the legal uncertainty surrounding these schemes might constitute a challenge for public authorities, as these schemes can be used by criminals, fraudsters and money launderers to perform their illegal activities.
-*Reputation risk* -If the use of virtual currency schemes grows considerably, incidents which attract press coverage could have negative impacts on the reputations of central banks, if the public perceives theincidents as being caused, in part, by central banks not doing their jobs properly. As a consequence, this risk should be considered when assessing the overall risk situation of central banks.

If the Bitcoin might be consider as threat to price, financial and the payment stability of the modern economies?

Bitcoin as virtual currency scheme may be inherently unstable. But, due to its limited connection to the real economy, the low volumes traded and the lack of wide user acceptance for the time being, it seems that it still doesn’t jeopardise financial stability of the economies which citizens use Bitcoin as a means of exchange or payment.

The limited volume of a Bitcoin in circulation also doesn’t pose a risk for price stability at this stage, provided that the issuance of money continues to be as stable as it seems to be at present. In the short to medium term, no significant impact can be expected on the velocity of money. However, it is probably worth monitoring the interaction between virtual currencies and the real world.

Bitcoin schemes do not allow borrowing or lending. But this may change in the future. There is even speculation on how Bitcoin could evolve. Banks could, for instance, act as a depository for the wallet files that contain users’ Bitcoins. The banks could then pay interest to those who hold the virtual currency with them. Alternatively the Bitcoin system could even start working as a fractional reserve system, extending credit over and above its actual reserves. However, the scheme’s supporters are clearly opposed to this. These developments, if they came to pass, could indeed have a certain impact on financial stability in the future.

In the particular case of Bitcoin, which is a decentralised peer-to-peer virtual currency scheme, there is not even a central point of access, i.e. there is no server that could be shut down if the authorities deemed it necessary. As a consequence, governments and central banks would face serious difficulties if they tried to control or ban any virtual currency scheme, and it is not even clear to what extent they are permitted to obtain information from them.

Therefore, the main activities to prevent negative impact of the Bitcoin schemes might be seen in constant monitoring of the Bitcoin development and well as in creating a proper legal basis for virtual currency schemes in general. The legal basis of a payment system consists of framework legislation, as well as specific laws, regulations, and agreements governing both payments and the operation of the system. Bitcoin need to have proper legal framework, as well as a clear definition of rights and obligations for the different parties. Furthermore, the global scope that most of these virtual communities enjoy not only hinders the identification of the jurisdiction under which the system’s rules and procedures should eventually be interpreted.

Conclusions

In the traditional markets , central governments manage the currencies and their performance based on a number of factors often questionable. However the introduction of the virtual currency schemes , especially the wider use of the most popular and the same time the most controversial virtual currency scheme called Bitcoin is characterized with the absence of central government whom decisions could induce phenomena of inflation or deflation and the anonymity of the transfer between entities in the network. In an extreme case, this virtual currency could have a substitution effect on central bank money if they become widely accepted.

The increase in the use of virtual money might lead to a decrease in the use of “real” money, thereby also reducing the cash needed to conduct the transactions generated by nominal income. In this regard, a widespread substitution of central bank money by privately issued virtual currency could significantly reduce the size of central banks’ balance sheets, and thus also their ability to influence the short-term interest rates.

The substitution effect would also make it more difficult to measure monetary aggregates ,which might pose further risks to price and financial stability in the medium to longer term. Since there is still a limited volume of a Bitcoin in circulation, the usage of Bitcoin can't be seen as a threat to the financial, payment and price stability worldwide.

Yet, the growing trend of wider use of Bitcoin currency requires continuous monitoring of its development and creating a proper legal basis for virtual currency schemes in general.

Bibliography

BALL, James , “Bitcoins: What are they, and how do they work?”, *The Guardian*, 22 June ,2011.

European Central Bank, “Virtual currency schemes “October 2012, http://www.ecb.europa.eu/home/html/index.en.htm

Benjamin Wallace, “The rise and fall of a BITCOIN”; November 23, 2011, .

BBC (2009), “Sales of virtual goods boom in US”, - http://news.bbc.co.uk/2/hi/technology/8320184.stm, *BBC News*, October 2009.

BELLER, Matthew (2007), “The Coming Second Life Business Cycle”, *Ludwig von Mises Institute*,2 August.

BIS, “The role of central bank money in payment systems”, *CPSS Publications*, No 55,August 2003.

BRODBECK, Simon “Virtual money – A new form of privately issued money in the moneymarket”, *European School of Management*, Paris, May 2007.

JAVA IDEs FOR EASILY LEARNING AND UNDERSTANDING OBJECT ORIENTED PROGRAMMING

Aleksandra Stojanova[1], Natasha Stojkovic[2] and Dusan Bikov[3]

[1]aleksandra.stojanova@ugd.edu.mk
[2]natasa.maksimova@ugd.edu.mk
[3]dusan.bikov@ugd.edu.mk

Abstract: Introduction to object-oriented programming (OOP) can be difficult for beginners in programming, especially if only pure code is used. To facilitate learning and understanding the concept of OOP many Java Integrated Development Environments (IDEs), that contains a lot of visual elements, are developed. Adding the visualization make programming easier, more interesting and interactive for users. These environments help to decrease the age of programming beginners. In this paper it will be given a brief overview of some of these environments. It will be done a comparison between them emphasizing differences among them, their advantages and disadvantages.

Keywords: object-oriented programming (OOP), Integrated Development Environment (IDE), visualization, Java.

1. Introduction

The learning and teaching of programming remains a challenging topic in the field of computer science education [2]. Working environments are very important in the study of programming, especially if it is an object-oriented programming. When the environments enriched with visualization and interaction, programming introduction becomes less abstract and less theoretical [5]. Java programming language is used worldwide in universities for learning basic concepts of OOP. Therefore many IDEs based on Java, are developed. The main purpose of Java IDEs is making process of programming easier, faster with more visual elements and less code writing [1]. In this paper we will start with introduction to Java IDEs, like BlueJ[12], Alica[11] and Greenfoot[14].We will shortly describe each of these environments and their constituent integrated elements. We also will describe and their way of working and their way of creating and presenting objects and classes. We will give the reason of using these IDEs, and target age group of users. Then, we will make comparison among these tree IDEs and we will emphasize their pros and cons.

2. Examples of IDEs for easily learning of object oriented concepts

In this paper three integrated development environments are reviewed. These environments are Alice, Greenfoot and BlueJ. They have the same goal and that is to help understanding object concepts, but they use different ways to accomplish the goal.

2.1. Alice

Alice is an IDE specifically designed as a learning tool to enable young programmers to create animations and games using 3D worlds. Alice use program visualization and enables users to see how their animation programs run. Programming visualization environment offered through Alice might be highly motivating to college students, especially for today's generation of video games and animated films [1].

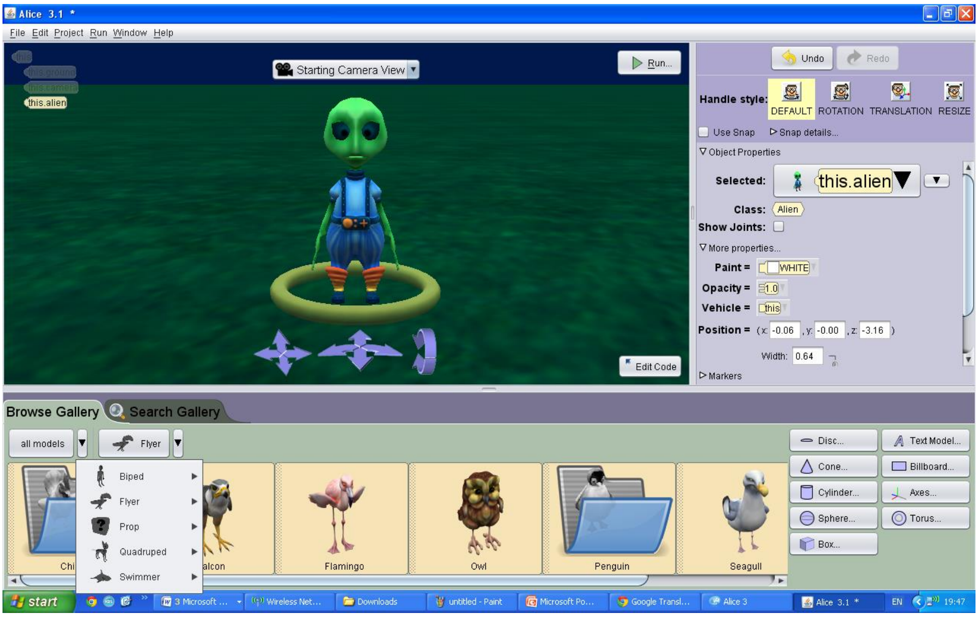
It uses drag-and-drop interface, and no text entry, to make the learning fun and interesting. This Alice's feature prevents users from making syntax errors, which are very common for beginners. It is intended for beginners in object-oriented programming, and it is easy and fun way to begin learning the Java language. Working with Alice provides fast visual feedback of the program and easy understanding of its object oriented structure and relationship between each programming statement and the corresponding behavior of objects in their animation [3].

Its 3D modeled classes and instantiated objects provide concrete picture of the concept of an object [16].

Alice’s library contains hundreds of 3D models which are provided in a gallery of Java classes. These models help virtual world to be enriched and populated. The user can create animations using these models that can move around a virtual world.

There are two types of animations in Alice: movie (passive animations) and interactive. The users immediately can see how their animation program runs [3].

Working in Alice consists of two phases: creating a scene and scripting (editing the code). The user can easily select new objects from a gallery that contains predefined objects, and can give the object functionality by using primitive methods from drop-down menus or by writing new functions. (Figure 1)



Selected: this.alien
Class: Alien
Show Joints: □
Paint = WHITE
Opacity = 1.0
Vehicle = this
Position = (x: -0.06 , y: -0.00 , z: -3.16)
Width: 0.64

Figure 1. Screenshot from Alice interface.

The language presented to the user in Alice, could be with the all Java syntax details but still it is drug and drop and not standard Java text-editor environment. This environment can be used as plugin in NetBeans [10] and Alice users can easily transfer their Alice project directly into Java text editor environment [3].

2.2 Greenfoot

Greenfoot is another integrated environment for learning programming. The program language that is used in this environment is Java too. Unlike Eclipse [13] or NetBeans [10] that also are Java IDEs and are using visual elements, this environment is more interactive and needs less previous theoretical knowledge for programming. But Greenfoot is also different from Alice because it needs more writing java code for making programs, and the language exposed to the users is Java. Greenfoot is Java two dimensional environment and is specialized for development of animations, simulations and games. It is designed for using in height schools and first programming courses in universities. [7]

This environment is a full interactive world of objects. It is a self-contained system that provides a full IDE, including integrated editor, compiler and debugger on source level and also contains build in classes and objects and allows creation of new classes and object [5, 6].

Its runtime environment and compiler uses standard Java. Also classes that are used there are pure Java classes and the syntax is also the same of standard java syntax.

Some of the advantages of Greenfoot are: easy way of making programming and giving visual feedback to the user. Scenarios are flexible and offer different level of complexity that makes this system usable in different age group categories. Greenfoot give very clear way of presenting object oriented concepts like (class, objects, inheritance etc.) It allows easy development of different scenarios and games with a little previous theoretical knowledge background, and also allows interaction with objects and easy control of their behaviors. Another advantage of this environment is the existence of an easy way of migration to other Java environments. Greenfoot is easy way to start programming games and simulations complete with 2D graphics and sound. But the support for text is very poor and is not using 3D [8,6].

Greenfoot user interface consist of the world (the background of the scene) and actors (Greenfoot objects). The two superclasses in the Greenfoot are World and Actor and they are always present in the scenario. All other classes are sub classes and derived from these two superclasses. One scenario of Greenfoot is presented in Figure 2.

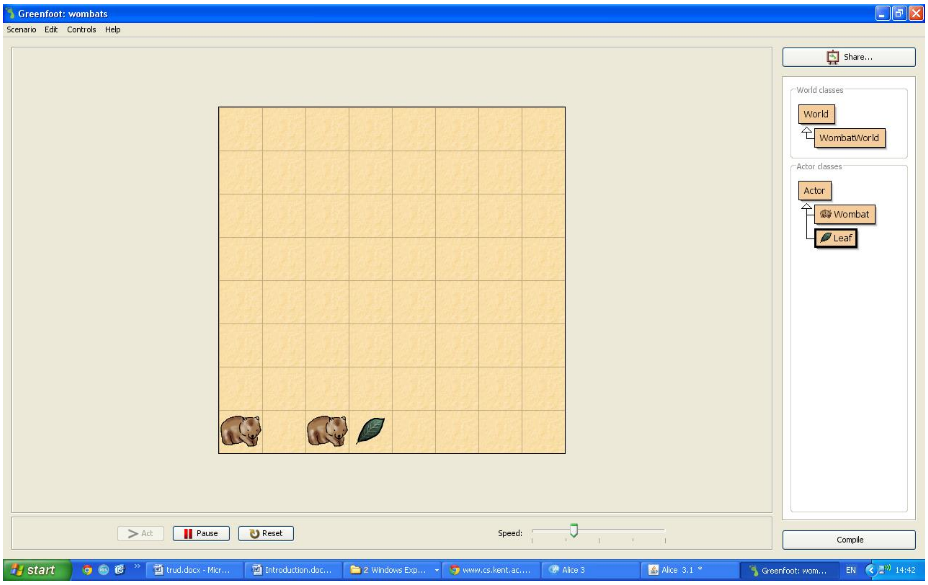


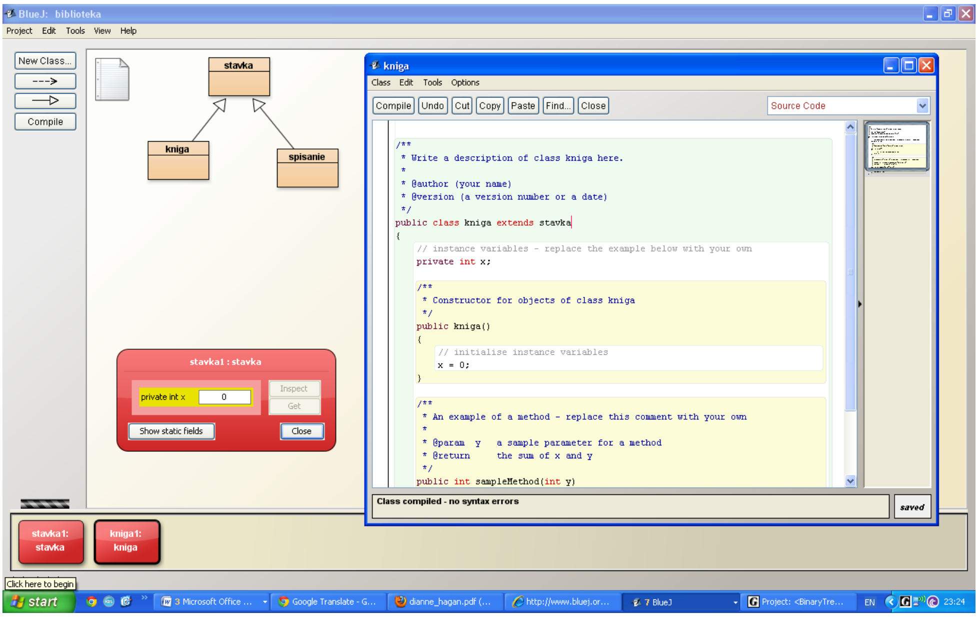
Figure 2. Screenshot from Greenfoot interface.

Greenfoot has build in predefined classes, objects and methods but also give a user a chance to create new classes objects and functions that give functionality of the instances (actors). The classes can be edited, compiled and instantiated. At any moment user can see the hierarchy structure of classes. The code of each class can be seen in code editor where the user can edit the existing code and add new code. The explanation of each class can be seen in the documentation [14].

2.3 BlueJ

BlueJ is specifically developed for the purpose of teaching object oriented programming with Java and it is free and open source software. This environment can run on all platforms supporting a recent Java virtual machine [11,13]. BlueJ is fully integrated environment. It supports graphical visualization of class structure and also a textual editing. It have built-in editor, compiler, virtual machine and debugger therefore it offers easy-to-use interface ideal for beginners.

BlueJ provides clear separation of the concepts of classes and objects. Classes and object in this environment are visually represented as UML (Unified Modeling Language) class diagrams (Figure 3) [6]. In this kind of visualization, hierarchy among classes can be clearly seen, but BlueJ does not provide direct visualization of any the object's state or behavior.



private int x 0

```
/**
 * Write a description of class kniga here.
 *
 * @author (your name)
 * @version (a version number or a date)
 */
public class kniga extends stavka
{
    // instance variables - replace the example below with your own
    private int x;

    /**
     * Constructor for objects of class kniga
     */
    public kniga()
    {
        // initialise instance variables
        x = 0;
    }

    /**
     * An example of a method - replace this comment with your own
     *
     * @param  y   a sample parameter for a method
     * @return     the sum of x and y
     */
    public int sampleMethod(int y)
```

Class compiled - no syntax errors

Figure 3. Screenshot from BlueJ interface

It allows easy making of classes and when the classes is added and compiled, the user can interactively instantiate objects and execute their methods through a sequence of pop-up menus. This allows users to immediately see the effect of a method invocation on that object and also simplifies the debugging process [9].

This environment uses the standard javac compiler, that gives users exposure to the exact same language, and the same compiler error messages that they might get when they leave BlueJ and move on to other tools. These kind error messages are not always helpful, especially to beginner programmers, so BlueJ provides extended help text for better understanding. This environment allows compilation and running the program without any main methods, but does not support as much features as professional IDEs, like NetBeans [10], Eclipce[13] or JBuilder[15] does.

BlueJ allows easy migration from educational tool to professional Java IDE, because in NetBeans IDE exists BlueJ plug-in that can help the migration [10].

3. Making comparison

All these three IDEs are used for easily learning of object oriented programming but still, they are different. They are different from commonly used IDEs for Java, like Eclipse and NetBeans. On one hand, these three environments can be used for learning Java by users who have very little theoretical knowledge of programming, and on the other hand Eclipse and NetBeans are environments that are used for professional development of complex Java programs.

Target group of users of all three environments are novices programmers, but Alice is named for younger beginners. It can be used in first classes of introduction in programming. In Alice object are presented in 3D and are more realistic and more fun to animate the beginners. Greenfoot is 2D environment but still similar to Alice because it uses defined set of classes, object and methods, and all objects are presented with adequate pictures.

In BlueJ environment classes a visually presented as UML diagrams, and not as pictures. All three environments provide interactivity to user.

Alice does not use text editing at all, methods and objects are made using drag-and-drop interface and pop-up-menus. Greenfoot and BlueJ on the other side have text editors where the user can write his own code.

Language presented to the user in Alice is not standard Java allowing the user to avoid making syntax errors. In Greenfoot and BlueJ, language exposed to the user is standard Java, to make better approach to professional Java IDEs.

All three environments offer way for migration to professional IDE for programming. Alice and Greenfoot are more game oriented and might be used as a tools for easy making games and animation.

According the features they offer for learning programming Greenfoot is in the middle between Alice and BlueJ. So in the learning chain novices programmers might begin with Alice then migrate to Greenfoot and then to BlueJ. BlueJ is most closely resembled with professional IDEs and its migration to professional environment is the easiest one.

4. Conclusion

Because object-oriented programming is quite abstract and complex, beginner-students often have trouble with learning the basic concepts of object–oriented programming. Furthermore, students often do not understand the reason for learning and advantages of using the object-oriented approach to software development.

Professional IDEs are not always adequate for learning basics of object oriented programming because these environments usually are not object oriented also they can be very complex and focused on building graphical user interface[9].

Alice, Greenfoot and BlueJ, make programming easier than other commonly available tools. They easily can be used from young people, non-engineering, undergraduates with little or no-programming experience. They use visual elements to represent the object concepts and allows interactivity to user. Using visualization and interaction provides a sense of reality for objects.

Alice, Green and BlueJ, are environments that allow users to focus on the concepts of objects like encapsulation or inheritance rather than dealing with syntax errors. So, these three environments can be used as impressive introduction to a professional IDEs.

Our purpose was to present these little-known environments for Java and to clarify their pros and cons. They might be used for adding efficiency in the process of learning.

Refernces

[1] B. Moskal, D. Lurie and S. Cooper (2004): *Evaluating the Effectiveness of a New Instructional Approac.* ACM SIGCSE '04, New York, NY, USA ©2004 pp. 75-89

[2] D. McCall, M. Kölling and P. Henriksen (2010): *Motivating Programmers via an Online Community.* Journal of Computing Sciences in Colleges, 25(3): pp. 82-93, January 2010

[3] D. Culbya, D. Cosgrove, Don Slater and Wanda Dann (2012): *Mediated Transfer: Alice 3 to Java*. In SIGCSE'12. 2012. Raleigh, North Carolina, USA: ACM. pp. 141-146

[4] D. Hagan, and S. Markham (2000) Teaching Java with the BlueJ Environment, Australian Society for Computers in Tertiary Education - ASCILITE ,

[5] M. Klling and P. Henriksen (2005): *Game Programming in Introductory Courses With Direct State Manipulation*. In ITiCSE 2005 Proceedings, pp 59-63

[6] M. Kölling and Poul Henriksen (2004): *greenfoot:Combining Object Visualisation with Interaction.* ACM 2004 Article, New York, NY, USA ©2004, pp. 73-82

[7] M. Kölling (2009): *Introduction to Programming with Greenfoot*. Pearson Education, Upper Saddle River, New Jersey, USA

[8] M. Kölling (2010). *The greenfoot programming environment*. ACM Transactions on Computing Education (TOCE) Vol 10, Issue 4,Article 14 (November 2010)

[9] M.Kölling (2008) *Using BlueJ to Introduce Programming* ,Reflections on the Teaching of Programming, Springer-Verlag Berlin, Heidelberg ©2008 pp. 98 – 115

[10] NetBeans IDE, official pages. Read on November, 2012. http://edu.netbeans.org/bluej/

[11] Official website of Alice. Read on November, 2012. http://www.alice.org/

[12] Official website of BlueJ. Read on November, 2012. www.bluej.org/

[13] Official website of Eclipse Read on November, 2012 http://eclipse.org/

[14] Official website on Greenfoot. Read on November, 2012. http://www.greenfoot.org/

[15] Official website of JBuilder, Read on November, 2012
http://www.embarcadero.com/products/jbuilder

[16] S. Cooper, W. Dann and R. Pausch (2003): *Teaching objects-first in introductory computer science*, n SIGCSE'03, New York, NY, USA: ACM.pp.191-195

STUDENTS' KNOWLEDGE TEST CONTROL – METHODS AND RESULTS' INTERPRETATION

Ludmila Stoyanova[1], Daniela Minkovska[2]

[1] Technical University of Sofia, Bulgaria, lstoyanova@tu-sofia.bg
[2] Technical University of Sofia, Bulgaria, daniela@tu-sofia.bg
** Corresponding author's mail: lstoyanova@tu-sofia.bg, daniela@tu-sofia.bg*

Abstract: This paper reveals some popular methods and types of test approach for students' knowledge and skills assessment that have been used in the machine engineering faculties. The received test results from conducted experiments have been analyzed and interpreted by the means of statistical methods. Definite conclusions have been made concerning the efficiency of appliance of different test approaches.

Keywords: assessment, tests, E-learning, programming

1. Introduction

In the modern forms of education, conducted with the help of multimedia technology, the introduction of e-learning systems, various test control and assessment systems of students' knowledge is exceptionally significant.

Important parameter among the general characteristics in the process of learning is the assessment. For the process of checking the obtained students' knowledge different methods might be used - traditional examination by writing an essay to a definite question, the oral answer to a problem, or the usage of previously drawn test' variants. The test method for assessment offers many advantages over the other methods, such as shortening of the time control, covering larger amount of the material, and the ease of interpretation and analysis of the results.

The goal of the experiment has been to reveal the advantages and disadvantages of the already used methods for one and the same discipline in one and the same direction at the Technical University of Sofia, Bulgaria.

That was necessary when the directions as a number of definite faculties have been introduced where the study of the same discipline have to be on the same level. In order to compare the level of students' knowledge the comparison began from the testing methods.

2. A brief overview of some methods for structuring the test questions

The usage of a test method for control and assessment of students' knowledge involves structuring the entire learning material in an appropriate sequence, selection of appropriate types of test questions and creation of relevant evaluation criteria.

The most convenient tests from the getting a “correct” image of learning process’ results point of view are the didactic tests. They measure the received results in the learning process of definite curricula in an organized learning process. The didactic tests are two types:

- Normative – they establish the personal achievements of each tested student by comparison to everyone else who worked on this test. The level of these achievements always ends with an assessment.
- Criteria – they measure the student’s achievements according to the standards already set in the curriculum. This type of tests are also standardized tests.

Both types of tests should not be opposed, because they have common characteristics, such as using the same type of test questions, the same properties (validity, reliability, difficulty, etc.), the evaluation requires a sample of test questions and others [1].

The construction of didactic tests requires the following:

- questions must be clearly and concisely written;
- the proposed options for answer must be unambiguous;
- the learners must have limited (but sufficient) time to think over the answer;
- the student have to work almost without need of supplies;
- limited ability for random guess of the correct answer;
- opportunity to receive immediate evaluation after the test.

The didactic tests allow the usage of two main types of test questions - open type and closed type.

- Open type - these are the questions and problems with free response in which students themselves can formulate their answer. In them, the students can apply, analyze and present their knowledge and related skills.
- Closed type - these are the questions and tasks with the so called structured response in which students choose an answer, their ability for response is limited or is one among many alternatives. This type of questions can possess different structure:

- dichotomous tests (type true-false-items) – these questions consist from one statement or proposition that is offered to the student for assessment whether it is true or not. The advantage of this type is that the tests are composed relatively quickly and require less time. They allow quick processing and analysis of test results. The results are not affected much by the chance that one answer might be selected randomly. Deficiencies are associated primarily with the students possibility to guess 50% of the responses completely random, even without thinking;
- tasks with multiple response (type multiple-choice items) - the most commonly used type of questions in didactic tests. They have two parts - a base (specific task formulated as a question or incomplete statement) and alternatives (possible answers or statements, only one of which is correct). Alternatives must be not less than three, in the best case, four or five possible answers. Each test question should contain only one accurate, correct and unambiguous answer. The advantage is that by the means of that type of questions complete learning content can be covered and the verification of responses is relatively quick. The disadvantage is that the possibility of guessing the correct answer depends on the number of offered variants for answer;
- tasks for comparison - allow to assess students' understanding of the interrelationships between words and definitions, events and dates, categories and examples etc. In this case to one set of information is proposed a definite common set of answers. The question usually is given in two columns. The student is required to relate the elements from one column to the elements in the second column. The advantage of this type is that it allows relatively quick checking of the utilization of relatively large amounts of factual information. Assessment is objective and independent and the evaluation can be performed automatically. Disadvantages – questions are hard to understand [2];

The latest trend in education is the application of the so-called adaptive tests (tailored-tests). They implement the strategy whereby questions have been chosen according the appropriate student’s level of preparation. At the beginning, the student undergoes diagnostic test questions, and then depending on his results the proposed test questions are tougher or lighter. The construction of such tests is a complicated and long research process, which is based on the latest theories in the field of testing with probabilistic and informational technique nature, such as probabilistic theory or called. Poisson - D. Raash model, the theory of "Maximum-Likelihood-Shatzung" of RA Fisher, the three parametric model of Birnbaum and some other [3].

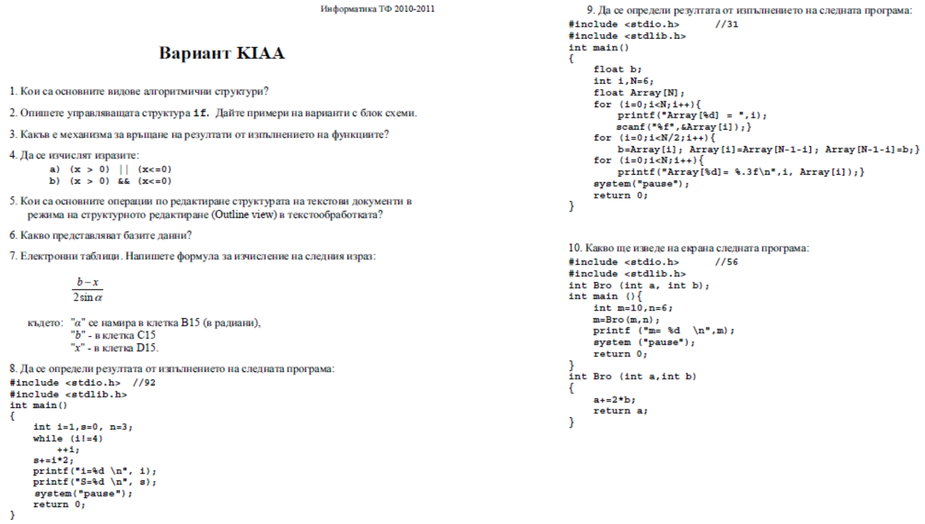
The usage of the test method for monitoring and assessment of students' knowledge is an innovative method that enables the increase of the cognitive activity of the students, and self-diagnosis of their achievements. With its help, the lecturer can make a quick and easy statistical and/or probabilistic analysis of the results and reliable conclusions about the quality of the learning process.

3. Description of experiments with different types of tests

In the machine engineering faculties mainly two types of tests have been used.

The first type of test is the one that contains only the short answer type of questions [4]. This type of test has been used without computer, just on paper. The usage of computer assisted testing may be introduced successfully but the checking of students' answers will still remain without computer help. That is so because the short answer questions are similar to essay. The student gives his answer without any kind of hints. The questions have to be constructed in a clear form [2] and they should require a short answer. Still it is a free constructed answer and the computer assisted checking of such answers is not on the appropriate or better to say desired level. From another side their checking would be considered much easier than the essay. As the praxis has proven the checking and proofing of such type of questions is really timesaving if the required answers are short and clear. And depending on the question formulation the spent time for checking and proofing is comparable to the time of the manual checking and proofing of multiple choice type of questions.

Sometimes the short answer questions are neglected because of their general usage to require the exact reproduction of knowledge, e.g. "Define the element of the …" or “List the elements that….” However, this disadvantage can be overcome by the usage of questions of higher levels according the Bloom’s theory, e.g. “What is the difference between…”, “Analyze the advantages of the usage of element …”, “Categorize the elements according…”and so on. In this way, the student has to prove his understanding of knowledge or even more his ability to comprehend, analyze or evaluate (Fig. 1).



Информатика ТФ 2010-2011

Вариант KIAA

1. Кои са основните видове алгоритмични структури?

2. Опишете управляващата структура **`if`**. Дайте примери на варианти с блок схеми.

3. Какъв е механизма за връщане на резултати от изпълнението на функциите?

4. Да се изчислят изразите:

```
a) (x > 0) || (x<=0)
b) (x > 0) && (x<=0)
```

5. Кои са основните операции по редактиране структурата на текстови документи в режима на структурното редактиране (Outline view) в текстообработката?

6. Какво представляват базите данни?

7. Електронни таблици. Напишете формула за изчисление на следния израз:

$$\frac{b-x}{2\sin\alpha}$$

където: "α" се намира в клетка B15 (в радиани),
"b" - в клетка C15
"x" - в клетка D15.

8. Да се определи резултата от изпълнението на следната програма:

```
#include <stdio.h>  //92
#include <stdlib.h>
int main()
{
    int i=1,s=0, n=3;
    while (i!=4)
        ++i;
    s+=i*2;
    printf("i=%d \n", i);
    printf("S=%d \n", s);
    system("pause");
    return 0;
}
```

9. Да се определи резултата от изпълнението на следната програма:

```
#include <stdio.h>      //31
#include <stdlib.h>
int main()
{
    float b;
    int i,N=6;
    float Array[N];
    for (i=0;i<N;i++){
        printf("Array[%d] = ",i);
        scanf("%f",&Array[i]);}
    for (i=0;i<N/2;i++){
        b=Array[i]; Array[i]=Array[N-1-i]; Array[N-1-i]=b;}
    for (i=0;i<N;i++){
        printf("Array[%d]= %.3f\n",i, Array[i]);}
    system("pause");
    return 0;
}
```

10. Какво ще изведе на екрана следната програма:

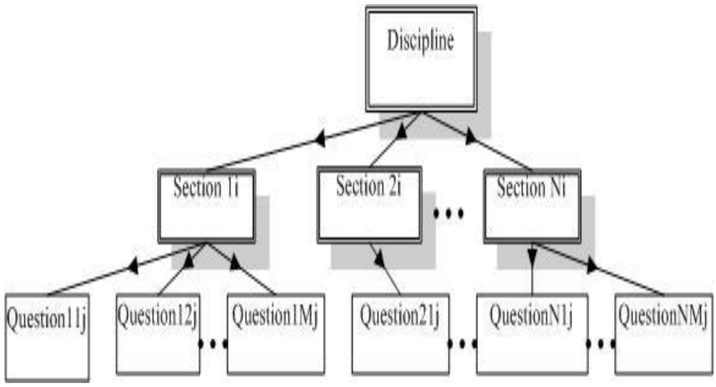
```
#include <stdio.h>      //56
#include <stdlib.h>
int Bro (int a, int b);
int main (){
    int m=10,n=6;
    m=Bro(m,n);
    printf ("m= %d  \n",m);
    system ("pause");
    return 0;
}
int Bro (int a,int b)
{
    a+=2*b;
    return a;
}
```

figure 1 Test with short answer type questions

This method for test construction requires that the discipline or the part of discipline on which a test will be constructed have to be presented as a set of sections (Fig. 2). On figure 2 the sections are named from Section 1i to Section Ni, where i depicts the appropriate cognitive level according to the Bloom’s taxonomy.

Each section includes a number of questions over a part of the curricula. Every section corresponds to a certain cognitive level in Bloom’s taxonomy. The questions to each section may refer to the lowest level in the taxonomy up to the level of the section.

Of course, it depends on the author of the test, but in such way, the students will be tested and assigned to the cognitive level, which correspond to their assessed knowledge and skills. The construction of a definite variant of the test should contain questions at different cognitive levels that are equal or lower than the level of corresponding section.



Legend:

i – cognitive level of the section

N - number of the section

M – number of the question in the section

j – cognitive level of the question

figure 2 Test structure

By this kind of tests, the correct answer to each question brings the student 3 points. Each test variant consists of 10 questions. The distribution of questions over the cognitive levels brings to the correct correlation between the assessed knowledge and skills and the gathered points from the test.

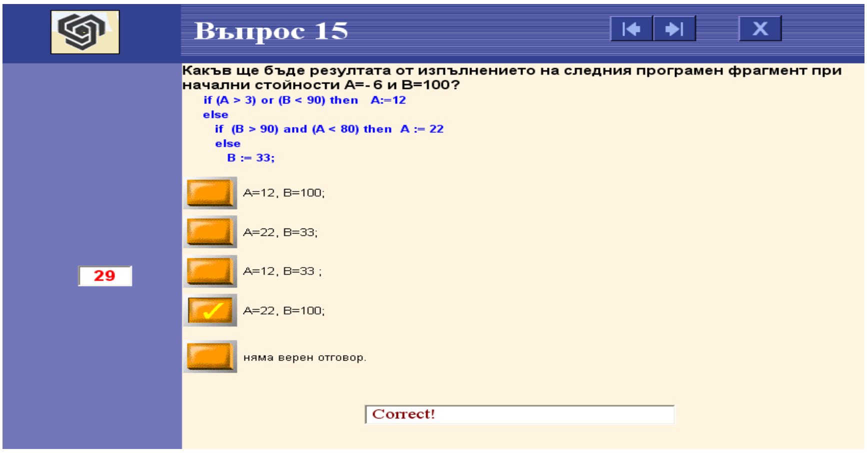
The described test type has been experimented for the knowledge and skills' assessment of one group of 112 students twice per one semester and another group of 182 students also tested twice per one semester.

At the same time another type of testing has been used for control and assessment of another group of students.

The second type of tests consists of questions of multiple choice type. These students have been tested twice per semester with this kind of tests.

During the real implementation in the learning process of this type of test control, the students' answers to the same number of questions, uniformly distributed, at the learner material [5]. All questions are stored in one unified database; the questions are generated according to the basic topics on the studied material separately, through random method [6]. All generated tests' variants have the same characteristics, for example: united structure of the proprieties part with the same number for choice, as one of them is true, difficulty, the same points for a correct answer, they have equal time for implementing of the control and one and same predefined grade scale [7]. In that way the students are stationed in equal conditions, because they have possibility decide equal by difficulty, but different by content tests (Fig. 3).

For getting of assessment for mean level (3) on the first and second test' control, it is necessarily the students to obtain 30 percent of correct answers [8]. Evaluation with higher marks is respectively with the criteria of ECTS (European Credit Transfer System) (Fig. 4) [9].



Какъв ще бъде резултата от изпълнението на следния програмен фрагмент при начални стойности A=-6 и B=100?

```
if (A > 3) or (B < 90) then   A:=12
else
  if  (B > 90) and (A < 80) then  A := 22
  else
    B := 33;
```

A=12, B=100;

A=22, B=33;

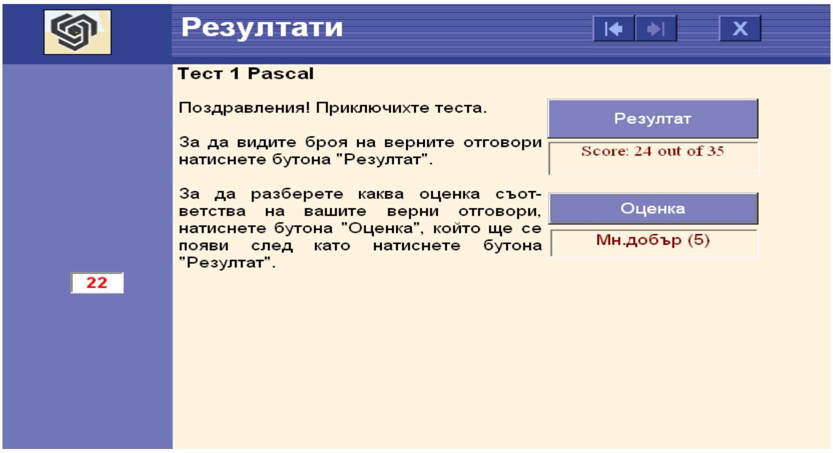
A=12, B=33 ;

✓ A=22, B=100;

няма верен отговор.

Correct!

figure 3 Page with a multiply type question



Тест 1 Pascal

Поздравления! Приключихте теста.

За да видите броя на верните отговори натиснете бутона "Резултат".

Score: 24 out of 35

За да разберете каква оценка съответства на вашите верни отговори, натиснете бутона "Оценка", който ще се появи след като натиснете бутона "Резултат".

Мн.добър (5)

22

figure 4 Final page from the continue control system

The previous experiments [5, 6, 7, 8] have proved that this type of questions and respectively tests give the most exact correspondence of students’ knowledge and skills and the gathered points (or the mark).

The time spent for the checking of these types of tests is quite short.

On the base of the gathered results, some quite useful histograms (bars) could be presented. They allow the comparison of empirical distribution of students’ results according the two investigated educational years for each of investigated faculty:

- Faculty of Power Engineering and Power Machines (FPEPM) – (Fig. 5);
- Faculty of Transport (FT) – (Fig. 6).

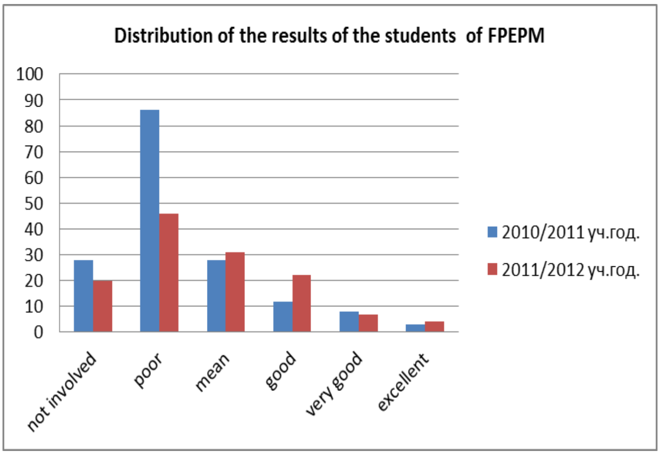


figure 5 Distribution of students' results of Faculty of Power Engineering and Power Machines (FPEPM)

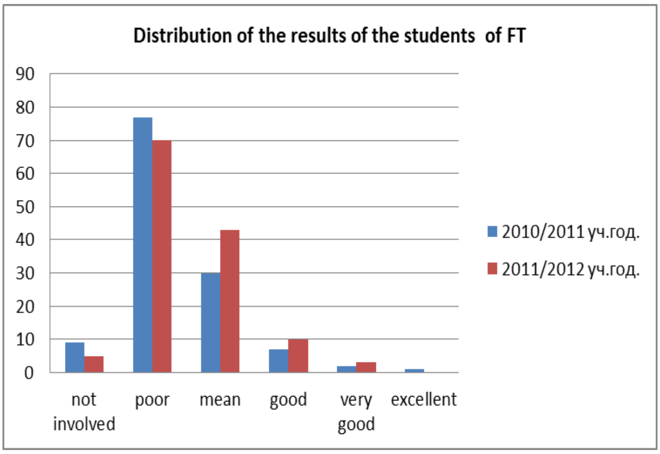


figure 6 Distribution of students' results of Faculty of Transport (FT)

The students' results of Faculty of Power Engineering and Power Machines (FPEPM – fig. 5) have undergone the second test type – multiple choice test type and the students from the Faculty of Transport (FT – fig. 6) have conducted the tests from the first type – the short answer type. The distribution of the students' results is similar for both faculties and this points that both test types measure in equally correct way the received knowledge and skills.

4. Conclusion

The experiments for the two types of testing have been conducted in two successive years during the first semester and for a discipline that have been studied in one semester in both faculties. The chosen faculties are the Faculty of Transport and the Faculty of Power Engineering and Power Machines - both in the machine engineering direction.

The experiments have established that the both types of testing bring to correct correlation between the assessed knowledge and skills and the received marks from the test.

The short answer types of questions develop the students' ability to construct answers, to present ideas and so on, and this is very important in this age of electronic devices.

The second type of tests is much more suitable for the lecturers and instructors because it is timesaving.

From these results, we can draw the conclusion that the usage of the test method for control of the learning or the e-learning processes is an effective instrument for measurement and assessment of the level of the knowledge and skills of the students, being educated. It gives the teachers the opportunity to acquaint themselves with the results during the learning process and in this way allow them to change or adjust the learning material according the students' level. The usage of the two different forms and the test methods themselves have not played significant role for the assessment of the students. Their differences have been much more significant to the teachers in the timesaving aspect.

5. References

1. Тупаров Г., Дурева Д., *Електронно обучение – технологии и модели*, изд. „Неофит Рилски“, Благоевград, 2008, ISBN:978-954-680-533-1
2. Желев Г., *Методи за управление на диалога и адаптацията на потребителите*, PhD thesis, Leningrad, Rusia
3. Георги Бижков, *Теория и методика на дидактическите тестове*, Просвета София, 1992
4. Методология и технология электронного обучения, last viewed 09.11.2012, http://cnit.ssau.ru/ do/index.htm
5. Jelev G., Minkovska D., *Approaches for Definition the Validity of the Results of the Test for Knowledge Mastering*., Proceedings, International Scientific Conference, Computer Science, FKSU, TU, Sofia, 2004;
6. Jelev G., Minkovska D., *An Approach for Improving of Test Environment for the Knowledge Mastering*, Proceedings, International Scientific Conference “Computer Science'2005”, Chalkidiki, Greece, 2005;
7. Jelev G., Minkova Y., *Determination of Representative Sample Size*, Computer Science conference, FKSU, TU, Sofia, 2004;
8. Jelev G., Minkovska D., *Results Analysis of Test Control on the Knowledge of the Students*, Proceedings, International Scientific Conference “Computer Science'2006”, Istanbul, Turkey, 2006;
9. Practical guide of ECTS, ECTS, 1995

WEB SERVICE FOR AMBIGUOUS TRANSLITERATION OF FULL SENTENCES FROM LATIN TO CYRILLIC ALPHABET

Stojance Spasov[1] *stojance.spasov@ugd.edu.mk*

Zoran Zdravev[1] *zoran.zdravev@ugd.edu.mk*

[1]Faculty of Computer Science, University “Goce Delcev” - Stip

Abstract

Introduction to transliteration as a process discovers the ability to differ and convert symbols from one language with different meaning to other languages. The intelligent algorithm for detecting Latin and Cyrillic alphabet has a need of minimal steps for transliteration, in the cases when the words from one language can have more than one meaning. This paper pays attention to the forms of transliteration of full sentences, which shall be used for Macedonian texts written in Latin alphabet on social networks, web-sites, old magazines etc.

Keywords: algorithm, Macedonian texts, Latin and Cyrillic alphabet, more than one meaning.

Introduction

The transliteration is a process used for mapping of words from one system of writing to another. This procedure is widely applied in Macedonian alphabet that uses Cyrillic letters, due to the circumstances when the writing of letters in Latin alphabet is required. With the assistance of modern techniques and technologies, the process of easier and faster transliteration under standard circumstances is enabled. But under non-standard circumstances, common for Macedonian area, together with the grammar rules, there is often a misunderstanding, especially regarding the meaning and ambiguity of words. For example from “kuka” we derive “кука” or "куќа”, from “sok” we derive “сок' or "шок" and so on. It mostly happens in international communication, where different technologies, without Cyrillic input language, are used for sending messages and mails from mobile phones, writing on social networks etc. Therefore, regarding transliteration with different meanings, researches of the purpose and meaning of the words in the sentence are required as well as algorithm that will solve this problem. This could greatly contribute to Macedonian alphabet, especially for terms written in Latin alphabet. The purpose of this research is creating a web based service i.e. defining an intelligent algorithm that will enable transliteration of full sentences from Latin to Cyrillic alphabet as well as transliteration upon request of other applications.

Transliteration

The words from any language should sometimes be written in other alphabet. Mostly this happens under Macedonian circumstances as well, when the words are written in Latin alphabet. This is due to the fact that communication devices do not have Cyrillic input language. When sending an email from mobile phone written in Latin alphabet for example. The transliteration may be reversible and convert terms from one alphabet to another. The transliteration is not always a simple process for realization, because there is not a difference drawn between writing Macedonian alphabet with Latin letters. Therefore, there are rules according to several standards. The Macedonian transliteration is standardized with ISO R9:1968. This system was adapted and adopted in 1970 by the Macedonian Academy of Sciences and Arts and it is considered as officially accepted in the Republic of Macedonia. There are so far transliteration algorithms invented that work perfectly under standard circumstances. Standard circumstances are those when the writing of the texts follows already established standards such as „ѓ=gj“, „ж=zh“, „ѕ=dz“, „њ=nj“, „ќ=kj“, „ч=ch“, „џ=dj“ и „ш=sh“. This presentation of the letters and diagraphs is simpler. However, there is other type of writing in which letters are called diacritics presented with a special sign, for example for letters ѓ, ќ, ч, ж, ш, ѕ, џ - (ǵ, ḱ, č, ž, š, dz, dž). This is demonstrated in *Table 1.*

Table 1*.* Transliteration from Cyrillic to Latin alphabet under standard circumstances

Cyrillic	*Latin*	*Process of transliteration*	
А а	A a	авантура	avantura
Б б	B b	борба	borba
В в	V v	вести	vesti
Г г	G g	град	grad
Д д	D d	дрво	drvo
Ѓ ѓ	Gj gj	ѓавол	gjavol
Е е	E e	елен	elen
Ж ж	Zh zh	жонглер	zhongler
З з	Z z	збор	zbor
Ѕ ѕ	Dz dz	ѕид	dzid
И и	I i	имот	imot
Ј ј	J j	јубилеј	jubilej
К к	K k	коска	koska
Л л	L l	леден	leden
Љ љ	Lj lj	љубичица	ljubichica
М м	M m	манастир	manastir
Н н	N n	нога	noga
Њ њ	Nj nj	коњ	konj

Table 2*.* Ambiguous Transliteration f Cyrillic to Latin alphabet under non-stanc circumstances

Cyrillic	*Latin*	*Process of transliteratio*	
А а	A a	авантура	avant
Б б	B b	борба	borb
В в	V v	вазна	vazn
Г г	G g	град	grad
Д д	D d	дрво	drvo
Ѓ ѓ	Gj gj	ѓавол	gavol
Е е	E e	елен	elen
Ж ж	Z z	жонглер	zongl
З з	Z z	збор	zbor
Ѕ ѕ	Z z	ѕид	zid
И и	I i	имот	imot
Ј ј	J j	јубилеј	jubile
К к	K k	коска	kosk
Л л	L l	леден	leden
Љ љ	L l	љубичица	lubici
М м	M m	манастир	man
Н н	N n	нога	noga
Њ њ	Nj nj	коњ	konj

О о	O o	облека	obleka
П п	P p	песна	pesna
Р р	R r	разговор	razgovor
С с	S s	соба	soba
Т т	T t	торба	torba
Ќ ќ	Kj kj	ќумур	kjumur
У у	U u	умерено	umereno
Ф ф	F f	форма	forma
Х х	H h	хумор	humor
Ц ц	C c	цвеќе	cvekje
Ч ч	Ch ch	човек	chovek
Џ џ	Dj dj	џамија	djamija
Ш ш	Sh sh	шеќер	shekjer

О о	O o	облека	oblek
П п	P p	песна	pesn
Р р	R r	разговор	razg
С с	S s	соба	soba
Т т	T t	торба	torba
Ќ ќ	K к	ќумур	kumu
У у	U u	умерено	umer
Ф ф	F f	форма	form
Х х	H h	хумор	hum
Ц ц	C c	цвеќе	cvek
Ч ч	C c	човек	cove
Џ џ	J j	џамија	jami
Ш ш	S s	шеќер	seke

Under non-standard circumstances, very common in Macedonian area, the writing of letters in Latin alphabet can have two meanings in Cyrillic alphabet. So, for the Latin “s” we have Cyrillic “ш” or “с” and for Latin “z” we can have Cyrillic “з” or “ж”. Hence, the sentence is unclear. This is demonstrated in *Table 2.*

Therefore, the end results are usually words with different meanings. For example, from “vesti” we derive “вешти" or “вести”, from "dokazi" we derive "докази" or "докажи". There are a lot of other examples too. This instances are called “ambiguous transliteration”.

Ambiguous transliteration

This paper is consisted of two smaller researches of ambiguous transliteration of full sentences from Latin to Cyrillic alphabet. The first research regards finding words that can have more than one meaning in the given alphabet. For that purpose we use a given base (dictionary) with

251460 words of Macedonian language including: verbs, names of locations and people, adjectives, nouns and other terms, and with the assistance of elaborated transliteration algorithm we obtained more than 5000 words with ambiguous transliteration.

Result

This means that more than 2 % of the words in the dictionary written in Latin alphabet have more than one meaning when transliterated in Cyrillic alphabet. This result of transliterated words has a great contribution to the structure of the language itself. When browsing those words in the given web service that makes difference between Cyrillic and Latin alphabet, the different meanings of the words is shown (for example забар, зелен, сок etc.). We will explain the procedure of transliteration of individual non-standard words with the following example. They should go through all these steps of transliteration demonstrated in diagram 1 and the obtained result shall be the ambiguous word.

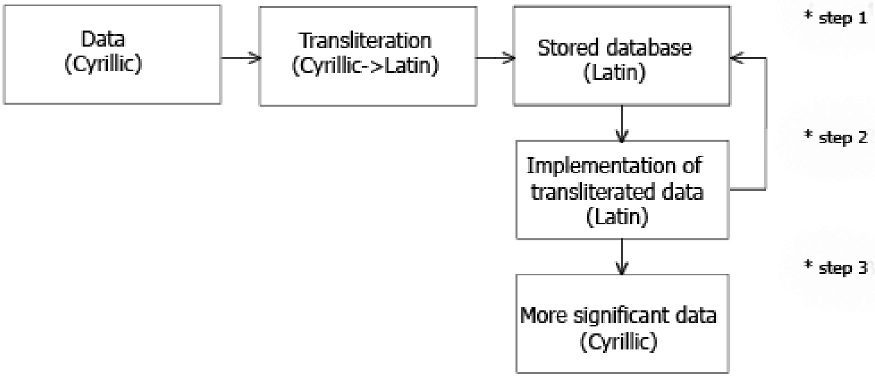


Diagram 1. Transliteration of individual words

Step 1: In the beginning, the transliteration of every data from the given dictionary commences. Let’s take the noun {забар} that should be transliterated in Latin alphabet. This means that each character of the data is transliterated in the other alphabet {з,а,б,а,р -z,a,b,a,r) and it is saved in the database with its own unique key. This step is repeated for all words in the dictionary.

Step 2: Each transliterated word, transformed to Latin alphabet, is further selected and compared to the following transliterated word from the database in order to check its ambiguity. It can be achieved by repeating the word {zabar} more than once.

Step 3: In this case the word {zabar} is placed in position of two nouns, which means that the end result has the following order {zabar}->{забар, жабар}. We can conclude that the final step enables a view of ambiguous term which basically is given in Cyrillic alphabet.

That is the part that we shall work on in order to properly transliterate full sentences and to obtain the real meaning of the full sentence. When transliterating only one word, the ambiguity of the words written on Latin alphabet cannot be resolved. However, when transliterating full sentences, a solution can be found.

Table 3. Overview of words with two meaning obtained by the steps of transliteration

Id	**Ordinal number of the dictionary**	**Cyrillic**	**Latin**	**Words with two meaning**
280	9279	бас	bas	bas(бас) - бас, баш
586	18295	важна	vazna	vazna(важна) - важна, вазна
667	20687	вести	vesti	vesti(вести) - вести, вешти
2110	42856	докази	dokazi	dokazi(докази) - докажи, докази
2355	53109	жаби	zabi	zabi(жаби) - жаби, заби
2472	54909	забар	zabar	zabar(забар) - жабар, забар
2836	69526	звуци	zvuci	zvuci(звуци) - звуци, звучи
2876	71706	знаци	znaci	znaci(знаци) - знаци, значи
3157	94910	каса	kasa	kasa(каса) - каса, каша
3262	97909	кожа	koza	koza(кожа) - кожа, коза
4304	175440	попусти	popusti	popusti(попусти) - попусти, попушти
4677	223624	сефот	sefot	sefot(сефот) - сефот, шефот

Solving ambiguous transliteration

We suggest one algorithm for intelligent solution of transliteration which can work under circumstances of full sentences transliteration. It is created in order to properly show the words with two meanings, obtained by transliteration under non-standard circumstances, in accordance with the grammar rules. In order to prove its practicability, another research was conducted related to transliteration of certain number of sentences downloaded from the Internet. These sentences contain different terms, adjectives, nouns, conjunctions etc. This is only part of the solution with particular steps required for resolving the existing problem i.e. the ambiguity of words. Firstly, a calculation of the **K_i**-coefficient of words is conducted. Two formulas of ambiguity are used for that purpose. The first formula calculates the parameters which are not divided with 10%, whereas the second formula is with 10% The parameters are simple and are equally applied in the two formulas which are: the total number of sentences that contain one or more of the ambiguous words, the number of repetitions of all words in the sentence, the total number of all sentences that use ambiguous words. There are tests of 29 downloaded sentences conducted in the research. Those sentences contain the ambiguous word in Latin alphabet as “vesti” and “вести” or “вешти” in Cyrillic alphabet.

Formula 1. ***Parameters without 10%***	*Formula 2.* ***Parameters with 10%***
$K_i = P / S_1 + S_1 / S_2$	$K_i = (P / S_1 + S_1 / S_2) * 0,10$

In the following two table those 29 sentences are demonstrated, i.e. 16 sentences that contain the word "вешти" or 13 sentences that contain the word "вести". Using the given formulas we obtain results for the parameters of each word that are explained in details with the following 7 steps.

Table 4. Overview of 24 sentences that contain the word “вешти”

вешти	**16**	**Repetitions**	**Sentences**	**Total sentences**	**Coefficient**
вешти	на	12	0,75	0,55	1,30
вешти	минатата	1	0,06	0,55	0,61

вешти	забава	1	0,06	0,55	0,61
вешти	во	10	0,63	0,55	1,18
вешти	Скопје	1	0,06	0,55	0,61
вешти	овие	2	0,13	0,55	0,68
вешти	жени	4	0,25	0,55	0,80
вешти	им	1	0,06	0,55	0,61
вешти	помагаа	1	0,06	0,55	0,61
вешти	болните	1	0,06	0,55	0,61
вешти	од	5	0,31	0,55	0,86
вешти	дневниот	1	0,06	0,55	0,61

Table 5. Overview of 24 sentences that contain the word “вести”

вести	**13**	**Repetitions**	**Sentences**	**Total sentences**	**Coefficient**
вести	најнови	3	0,23	0,448275862	0,68
вести	од	6	0,46	0,448275862	0,91
вести	Македонија	3	0,23	0,448275862	0,68
вести	и	5	0,38	0,448275862	0,83
вести	светот	4	0,31	0,448275862	0,76
вести	спортски	1	0,08	0,448275862	0,53
вести	забавни	1	0,08	0,448275862	0,53

вести	анализи	1	0,08	0,448275862	0,53
вести	интервјуа	1	0,08	0,448275862	0,53
вести	видео	1	0,08	0,448275862	0,53
вести	ги	1	0,08	0,448275862	0,53

This is followed by the steps for calculating **K_i** coefficient:

Step 1: Entering sentences in database, 29 sentences in this case.

Step 2: Sorting all words from all sentences where words can be repeated more than once.

Step 3: Calculation of **P -** parameter for repetition i.e. repetition of the words in the database.

Step 4: Calculation of only **S_1 -** number of sentences that contain the word “вешти” with previously appeared repetitions.

Step 5: Calculation of only **S_2 -** the total number of sentences that contain the words with two meanings “вешти” and “вести”.

Step 6: Here the **K_i -** coefficient is calculated as summary of step 4 and step 5.

Step 7: Then, we write Macedonian sentences shown in Latin alphabet. In this case we have the sentence “Najnovi vesti od Makedonija i svetot". Each word of the sentences has its own coefficient. The summary of the coefficients gives the right word for transliteration.

All these steps described above regard table 4 and table 5, whereas the result of step 7 is obtained by these two tables.

Result

Out of the coefficients’ sum for “вешти” we obtain the result 1,97 and for "вести" it is 3,86. This means that the sum with greater value represents the right word in some sentence or it gives the meaning of the whole sentence.

Table 6. Data for sentences of the word with two meanings

Najnovi vesti od Makedonija i svetot. (with sentences)

вешти	sentences (вешти)	вести	sentences (вести)
најнови	0	најнови	0,23
од	0,31	од	0,46
Македонија	0	Македонија	0,23
и	0,56	и	0,38
светот	0	светот	0,31
	0,87		1,61

Table 7. Data for coefficient of the word with two meanings in full sentences

Najnovi vesti od Makedonija i svetot. (with coefficient)

вешти	coefficient (вешти)	вести	coefficient (вести)
најнови	0	најнови	0,68
од	0,86	од	0,91
Македонија	0	Македонија	0,68
и	1,11	и	0,83
светот	0	светот	0,76
	1,97		3,86

For testing, a simple algorithm is elaborated which gives satisfactory results for determining the sense of the sentence and hence, it gives successful transliteration of full sentences. This is only one part of the solution which needs to be realized for transliteration of the words’ meanings.

Conclusion

Based on the results obtained from conducted research, the following conclusions can be drawn.

The transliteration as reversible process enables individual transformation of letters from one alphabet to another. Due to the inability of several digital devices to use Cyrillic alphabet for writing of digital text, certain standards are used. Under some circumstances, there are words with two or more meanings, and therefore, that produces obscurity in the meaning of the sentence. For that purpose, algorithm which can distinguish these words and calculate the coefficient for transliteration of words is used. This solution is possible if transliteration is applied for full sentences. So far, the calculation of the coefficient was not performed in digital form, for that reason the future job shall regard creating algorithm for transliteration of ambiguous words which can provide coefficient of words and with that the proper meaning of the full sentences as well. The application shall be the most useful in web services for transliteration of non-standard digital texts written in Latin to Cyrillic alphabet.

References

[1] Virga, Paola, and Sanjeev Khudanpur. "*Transliteration of proper names in cross-lingual information retrieval.*" Proceedings of the ACL 2003 workshop on Multilingual and mixed-language named entity recognition-Volume 15. Association for Computational Linguistics, 2003.

[2] Šimičević, Greta, and Ana Marija Boljanović. "*Transcription and Transliteration in a Computer Data Processing.*"

[3] *TRANSKRIPCIJA, TRANSLITERACIJA* I. "RASPRAVE ZJ, SV. 13 (1987), ZAGREB, 19-30 YU ISSN 0351—434x." Rasprave Zavoda za jezik IFF. 13 (1987): 19.

[4] Kuo, Jin-Shea, Haizhou Li, and Ying-Kuei Yang. "*Learning transliteration lexicons from the web.*" ANNUAL MEETING-ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. Vol. 44. No. 2. 2006.

[5] Sherif, Tarek, and Grzegorz Kondrak. "*Substring-based transliteration.*" ANNUAL MEETING-ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. Vol. 45. No. 1. 2007.

[6] Lin, Wei-Hao, and Hsin-Hsi Chen. "*Backward machine transliteration by learning phonetic similarity.*" proceedings of the 6th conference on Natural language learning-Volume 20. Association for Computational Linguistics, 2002.

[7] Antoniou, Grigoris, and Frank Van Harmelen. "*A semantic web primer.*" MIT press, 2004.

[8] Liyang, Yu. "*Introduction to the Semantic Web and Semantic Web Services.*" Taylor & Francis Group, 2007.

[9] Leon, Atkinson. "*Core PHP Programming.*" Prentice Hall PTR, ISBN: 0-13-089398-6, Second Edition, 2000.

[10] Vikram, Vaswani. "*PHP Programming Solutions.*" ISBN-10: 0-07-148745-X. McGraw-Hill, 2007.

ON THE APPLICATION OF KEEDWELL CROSS INVERSE QUASIGROUP TO CRYPTOGRAPHY

Jaíyéọlá Tèmítọpé Gbọláhàn

jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng

Department of Mathematics, Faculty of Science, Obafemi Awolowo University, Ile Ife 220005, Nigeria

On the 50th Anniversary of Obafemi Awolowo University

Abstract: In 1999, A. D. Keedwell found cross inverse property quasigroups (CIPQs) applicable to J. H. Ellis's original schema for a public key encryption. The present study devices a mechanism of changing the use of the Keedwell CIPQs against attack on a system(as required by the author). This is done as follows. The holomorphic structure of automorphic inverse property quasigroups (loops) [AIPQs (AIPLs)] and cross inverse property quasigroups (loops) [CIPQs (CIPLs)] are investigated. Necessary and sufficient conditions for the holomorph of a quasigroup(loop) to be an AIPQ (AIPL) or CIPQ (CIPL) are established. It is shown that if the holomorph of a quasigroup(loop) is a AIPQ(AIPL) or CIPQ (CIPL), then the holomorph is isomorphic to the quasigroup(loop). Hence, the holomorph of a quasigroup(loop) is an AIPQ (AIPL) or CIPQ (CIPL) if and only if its automorphism group is trivial and the quasigroup(loop) is a AIPQ(AIPL) or CIPQ (CIPL). Furthermore, it is discovered that if the holomorph of a quasigroup(loop) is a CIPQ (CIPL), then the quasigroup (loop) is a flexible unipotent CIPQ(flexible CIPL of exponent 2). By constructing two isotopic quasigroups(loops) U and V such that their automorphism groups are not trivial, it is shown that U is a AIPQ or CIPQ (AIPL or CIPL) if and only if V is a AIPQ or CIPQ (AIPL or CIPL). Explanations are given on how these CIPQs can be incorporated into the encryption scheme of Keedwell for higher security using a computer.

Keywords: holomorph of loops, automorphic inverse property loops (AIPLs), cross inverse property loops (CIPLs), automorphism group, cryptography

1 Introduction and Preliminaries

Let L be a non-empty set. Define a binary operation ($\cdot$) on L. If $x\cdot y\in L$ for all $x,y\in L$, $(L,\cdot)$ is called a groupoid. If the equations: $a\cdot x=b \quad and \quad y\cdot a=b$

have unique solutions for x and y respectively, then $(L,\cdot)$ is called a quasigroup. Let J_ρ be a permutation on L with inverse mapping J_λ i.e. $J_\rho^{-1}=J_\lambda$ and for each $x\in L$, let $x^\rho=xJ_\rho$ and $x^\lambda=xJ_\lambda$. Also, let

$$x^{\lambda^i}=\underbrace{((x^\lambda)^\lambda)^{\cdots}}_{i-times}\ and\ x^{\rho^i}=\underbrace{((x^\rho)^\rho)^{\cdots}}_{i-times}\ for\ i\geq 1.$$

Now, if there exists a unique element $e\in L$ called the identity element such that for all $x\in L$, $x\cdot e=e\cdot x=x$, $(L,\cdot)$ is called a loop. Hence, in a loop, if x^ρ and x^λ obey the relations $xx^\rho=e$ and $x^\lambda x=e$ respectively, they are called the right and left inverses of x respectively.

For a loop $(L,\cdot)$, recall the classic definition of its Holomorph. Let $Hol(L)=L\times Aut(L)$ and with multiplication defined on it as follows:

$$(x,\alpha)(y,\beta)=(x\cdot\alpha(y),\alpha\beta).$$

But because we shall be mapping from the left, we shall adopt the definition of a loop in Bruck [8]. Let the set $H=H(L)=Hol(L)=Aut(L)\times L$. If we define ' $\circ$ ' on H such that $(\alpha,x)\circ(\beta,y)=(\alpha\beta,x\beta\cdot y)\,\forall\,(\alpha,x),(\beta,y)\in Hol(L)$, then $(Hol(L),\circ)$ is a loop as shown in Bruck [8] and is called the Holomorph of $(L,\cdot)$.

Definition 1. *A loop(quasigroup) is a weak inverse property loop (quasigroup)[WIPL(WIPQ)] if and only if it obeys the identity* $x(yx)^\rho=y^\rho \quad or \quad (xy)^\lambda x=y^\lambda$.

A loop(quasigroup) is a cross inverse property loop (quasigroup) [CIPL(CIPQ)] if and only if it obeys the identity

$$xy\cdot x^{\rho} = y \qquad or \qquad x\cdot yx^{\rho} = y \qquad or \qquad x^{\lambda}\cdot(yx) = yor \qquad x^{\lambda}y\cdot x = y.$$

A loop (quasigroup) is an automorphic inverse property loop (quasigroup) [AIPL(AIPQ)] if and only if it obeys the identity $(xy)^{\rho} = x^{\rho}y^{\rho}$ *or* $(xy)^{\lambda} = x^{\lambda}y^{\lambda}$

Consider $(G,\cdot)$ and $(H,\circ)$ been two groupoids (quasigroups, loops). Let A,B and C be three bijective mappings, that map G onto H. The triple $\alpha = (A,B,C)$ is called an isotopism of $(G,\cdot)$ onto $(H,\circ)$ if and only if $xA\circ yB = (x\cdot y)C\ \forall\ x,y\in G.$

If $(G,\cdot) = (H,\circ)$, then the triple $\alpha = (A,B,C)$ of bijections on $(G,\cdot)$ is called an autotopism of the groupoid (quasigroup, loop) $(G,\cdot)$. Such triples form a group $AUT(G,\cdot)$ called the autotopism group of $(G,\cdot)$. Furthermore, if $A = B = C$, then A is called an automorphism of the groupoid(quasigroup, loop) $(G,\cdot)$. Such bijections form a group $Aut(G,\cdot)$ called the automorphism group of $(G,\cdot)$.

As observed by Osborn [21], a loop is a WIPL and an AIPL if and only if it is a CIPL. The past efforts of Artzy [3, 6, 5, 4], Belousov and Curkan [7] and recent studies of Keedwell [17], Keedwell and Shcherbacov [18, 19, 20] are of great significance in the study of WIPLs, AIPLs, CIPQs and CIPLs, their generalizations(i.e m-inverse loops and quasigroups, (r,s,t)-inverse quasigroups) and applications to cryptography.

Interestingly, Adeniran [1] and Robinson [22], Adeniran et. al. [2], Chiboka and Solarin [10], Bruck [8], Bruck and Paige [9], Robinson [23], Huthnance [15] and Adeniran [1] have respectively studied the holomorphs of Bol loops, central loops, conjugacy closed loops, inverse property loops, A-loops, extra loops, weak inverse property loops, Osborn loops and Bruck loops. Huthnance [15] showed that if $(L,\cdot)$ is a loop with holomorph $(H,\circ)$, $(L,\cdot)$ is a WIPL if and only if $(H,\circ)$ is a WIPL. The holomorphs of an AIPL and a CIPL were first studied by Jaiyéọlá in [16].

For the purpose of applying CIPQs to cryptography, Keedwell [17] needed to construct CIPQs with long inverse cycles. He constructed the following CIPQ which we shall specifically call Keedwell CIPQ and explained in much detail how a CIPQ with a specified long inverse cycle may be constructed and stored economically in a computer.

Theorem 1. *(Keedwell CIPQ) Let $(G,\cdot)$ be an abelian group of order n such that $n+1$ is composite. Define a binary operation '$\circ$' on the elements of G by the relation $a\circ b=a^r b^s$, where $rs=n+1$. Then $(G,\circ)$ is a CIPQ and the right crossed inverse of the element a is a^u, where $u=(-r)^3$.*

The author also gave examples and detailed explanation and procedures of the use of this CIPQ for cryptography. Cross inverse property quasigroups have been found appropriate for cryptography because of the fact that the left(right) inverse of x^λ (x^ρ) is not necessarily x unlike in left and right inverse property loops where $(x^\lambda)^\lambda=x$ and $(x^\rho)^\rho=x$. Hence, this gave rise to what is called 'cycle of inverses' or 'inverse cycles' or simply 'cycles' i.e finite sequence of elements $x_1,x_2,\cdots,x_n$ such that $x_k^\rho=x_{k+1}\bmod n$. The number n is called the length of the cycle. The origin of the idea of cycles can be traced back to Artzy [3, 6] where he also found there existence in WIPLs apart form CIPLs. In his two papers, he proved some results on possibilities for the values of n and for the number m of cycles of length n for WIPLs and CIPLs. We shall call these "Cycle Theorems" for now.

In Keedwell [17], the author showed that a CIPQ provides a means of applying directly J. H. Ellis's original schema for a public key encryption system in which the receiver takes part in the encryption process. See J. H. Ellis [12], [13] and [14].

A few years later, the same idea was propounded by W. Diffie and M. E. Hellman [11]. Their work was probably independent of that of Ellis because Ellis was prevented by the Official Secrets Act from publishing his ideas or any of their proposed subsequent implementations described in [13]. On the other hand, the paper of Diffie and Hellman and the subsequent practical implementations of it are very well known.

We shall now highlight the relevant part of [13] as recorded by Keedwell [17]:

1. Suppose the recipient has two tables T_1 and T_3 while the sender has one, T_2. These machine tables are not secret and may be supposed to be

possessed by the interceptor. T_1 takes an input k and produces an output x . T_2 takes inputs x and p giving an output z . T_3 takes inputs z and k . All these quantities are large numbers of the same magnitude. We can think of T_1 as a linear table of simple list, while T_2 and T_3 are square tables.

2. In operation, p is the message which is to be sent and k is a random number, chosen by the recipient. He enciphers k by T_1 to get x which he sends. The sender uses x to encipher p with T_2 to get z , the cipher text, which he sends back. Now, the recipient uses k to decipher z by means of T_3 . It is clearly possible for the entries of T_3 to give p under these circumstances, we have achieved our objective.

3. If the numbers are large enough and T_1 and T_2 sufficiently random to avoid working backwards, p cannot be found without knowing k . In public encryption terms, x is the public encipherment key and k is the private decipherment key.

Let $(L,\circ)$ be a CIPQ with long inverse cycle $(a,a^{\lambda},a^{\lambda^2},a^{\lambda^3},\cdots,a^{\lambda^{t-1}})$ of length t and suppose that both the sender S and the receiver R are provided with apparatus which will compute $x\circ y$ for any given $x,y\in L$. The latin square representing this quasigroup acts as the look up tables T_2 and T_3 and the long inverse cycle of the quasigroup serves as the third look up table T_1 .

The receiver R selects randomly one element $a^{(u)}\in L$ of the long inverse cycle and uses it to obtain $a^{(u)}J^{-1}=a^{(u-1)}$ which he sends to S who has a message $m\in L$ which he wishes to transmit to R . S uses $a^{(u-1)}$ to encipher m as $a^{(u-1)}\circ m$ which he sends back to R . Now R uses $a^{(u)}$ to decipher $a^{(u-1)}\circ m$ as $(a^{(u-1)}\circ m)\circ a^{(u)}=m$. Here, $a^{(u-1)}$ is the public encipherment key, $a^{(u)}$ is the private decipherment key.

According to Keedwell [17], the systems described by Ellis is not a public key encryption system as presently understood because a new key k is chosen for each new message (or part massge) which is to be sent.

For a present-day public key implementation of the idea, the author found it necessary to keep secret the algorithm for obtaining the right cross inverse of each element of L. So the implementation might be carried out as follows:

A key distribution centre would be established. Each user would have a computer programmed to calculate $x \circ y$ for every pair $x, y \in L$. Only the key distribution centre would have knowledge of the long inverse cycle and would use it to distribute a public key $a_i^{(u)}$ and a private key $a_i^{(u+1)}$ to each user U_i. When user U_i wished to send a message m to user U_j, he would send $a_j^{(u)} \circ m$ which U_j could decipher using his private key $a_j^{(u+1)}$.

However, *this scheme is not very secure* unless a mechanism is set up by which the CIPQ $(L,\circ)$ is changed fairly frequently. The system is more effective if implemented as a one-time pad which is in effect what Ellis was describing. For example, it might be used

(i) for sending a message $m = m_1 m_2 \dots m_r$ in which each portion of the message has its own enciphering and deciphering keys; or

(ii) for key exchange without the intervention of key distribution centre in the following way:

The sender S selects arbitrarily(using physical random number generator) an element $a^{(u)}$ of the CIPQ $(L,\circ)$ and sends both $a^{(u)}$ and the enciphered key or message $a^{(u)} \circ m$. The receiver R uses his knowledge of the algorithm for obtaining $a^{(u+1)}$ from $a^{(u)}$ (as given in Theorem 1.1, for instance) and hence he computes $(a^{(u)} \circ m) \circ a^{(u+1)} = m$.

The aim of the present study is to device a mechanism of constructing a CIPQ which can be used fairly frequently to replace the CIPQ in the above encryption process in order for it to be well secured against attack. This is done as follows.

1. The holomorphic structure of AIPQs(AIPLs) and CIPQs(CIPLs) are investigated. Necessary and sufficient conditions for the holomorph of a quasigroup(loop) to be an AIPQ(AIPL) or CIPQ(CIPL) are established. It is shown that if the holomorph of a quasigroup(loop) is a AIPQ(AIPL) or

CIPQ(CIPL), then the holomorph is isomorphic to the quasigroup(loop). Hence, the holomorph of a quasigroup(loop) is an AIPQ(AIPL) or CIPQ(CIPL) if and only if its automorphism group is trivial and the quasigroup(loop) is a AIPQ(AIPL) or CIPQ(CIPL). Furthermore, it is discovered that if the holomorph of a quasigroup(loop) is a CIPQ(CIPL), then the quasigroup(loop) is a flexible unipotent CIPQ (flexible CIPL of exponent 2).

2. By constructing two isotopic quasigroups (loops) U and V such that their automorphism groups are not trivial and are conjugates, it is shown that U is a AIPQ or CIPQ (AIPL or CIPL) if and only if V is a AIPQ or CIPQ (AIPL or CIPL). Explanations and procedures are given on how these CIPQs can be incorporated into the above described encryption process of Keedwell for higher security using a computer.

2 Main Results

2.1 Holomorph of AIPLs and CIPLs

Theorem 2. *Let $(L,\cdot)$ be a quasigroup(loop) with holomorph $H(L)$. $H(L)$ is an AIPQ(AIPL) if and only if*

1. *$Aut(L)$ is an abelian group,*
2. *$(\beta^{-1},\alpha,I)\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$ and*
3. *L is a AIPQ(AIPL).*

Proof. A quasigroup(loop) is an automorphic inverse property loop(AIPL) if and only if it obeys the identity $(xy)^{\rho}=x^{\rho}y^{\rho}\ or\ (xy)^{\lambda}=x^{\lambda}y^{\lambda}$.

Using either of the definitions of an AIPQ(AIPL) above, it can be shown that $H(L)$ is a AIPQ(AIPL) if and only if $Aut(L)$ is an abelian group and $(\beta^{-1}J_{\rho},\alpha J_{\rho},J_{\rho})\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$. L is isomorphic to a subquasigroup(subloop) of $H(L)$, so L is a AIPQ(AIPL) which implies $(J_{\rho},J_{\rho},J_{\rho})\in AUT(L)$. So, $(\beta^{-1},\alpha,I)\in\square AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$.

Corollary 1. *Let $(L,\cdot)$ be a quasigroup(loop) with holomorph $H(L)$. $H(L)$ is a CIPQ(CIPL) if and only if*

1. *$Aut(L)$ is an abelian group,*
2. *$(\beta^{-1},\alpha,I)\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$ and*
3. *L is a CIPQ(CIPL).*

Proof. A quasigroup (loop) is a CIPQ (CIPL) if and only if it is a WIPQ (WIPL) and an AIPQ (AIPL). L is a WIPQ (WIPL) if and only if $H(L)$ is a WIPQ(WIPL).

If $H(L)$ is a CIPQ(CIPL), then $H(L)$ is both a WIPQ(WIPL) and a AIPQ(AIPL) which implies 1., 2., and 3. of Theorem 2. Hence, L is a CIPQ(CIPL). The c□nverse follows by just doing the reverse.

Corollary 2. *Let $(L,\cdot)$ be a quasigroup(loop) with holomorph $H(L)$. If $H(L)$ is an AIPQ (AIPL) or CIPQ (CIPL), then $H(L)\cong L$.*

Proof. By 2. of Theorem 2, $(\beta^{-1},\alpha,I)\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$ implies $x\beta^{-1}\cdot y\alpha=x\cdot y$ which means $\alpha=\beta=I$ by substituting $x=e$ and $y=e$. Thus, $Aut(L)=\{I\}$ and so $H(L)\cong L$.

Theorem 3. *The holomorph of a quasigroup (loop) L is a AIPQ (AIPL) or CIPQ (CIPL) if and only if $Aut(L)=\{I\}$ and L is a AIPQ(AIPL) or CIPQ (CIPL).*

Proof. This is established using Theorem 2, Corollary 1 and Corollary 2.

Theorem 4. *Let $(L,\cdot)$ be a quasigroups (loop) with holomorph $H(L)$. $H(L)$ is a CIPQ (CIPL) if and only if $Aut(L)$ is an abelian group and any of the following is true for all $x,y\in L$ and $\alpha,\beta\in Aut(L)$:*

1. $(x\beta\cdot y)x^{\rho}=y\alpha$. *2.* $x\beta\cdot yx^{\rho}=y\alpha$. *3.* $(x^{\lambda}\alpha^{-1}\beta\alpha\cdot y\alpha)\cdot x=y$.

4. $x^{\lambda}\alpha^{-1}\beta\alpha\cdot(y\alpha\cdot x)=y$.

Proof. This is achieved by simply using the four equivalent identities that define a CIPQ (CIPL):

$$xy\cdot x^{\rho}=y \quad or \quad x\cdot yx^{\rho}=y \quad or \quad x^{\lambda}\cdot(yx)=y \quad or \quad x^{\lambda}y\cdot x=y.$$

Corollary 3. *Let* $(L,\cdot)$ *be a quasigroups(loop) with holomorph* $H(L)$. *If* $H(L)$ *is a CIPQ (CIPL) then the following are equivalent to each other*

1. $(\beta^{-1}J_{\rho},\alpha J_{\rho},J_{\rho})\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$.

2. $(\beta^{-1}J_{\lambda},\alpha J_{\lambda},J_{\lambda})\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$.

3. $(x\beta\cdot y)x^{\rho}=y\alpha$. 4. $x\beta\cdot yx^{\rho}=y\alpha$.

5. $(x^{\lambda}\alpha^{-1}\beta\alpha\cdot y\alpha)\cdot x=y$. 6. $x^{\lambda}\alpha^{-1}\beta\alpha\cdot(y\alpha\cdot x)=y$.

Hence, $(\beta,\alpha,I),(\alpha,\beta,I),(\beta,I,\alpha),(I,\alpha,\beta)\in AUT(L)\,\forall\,\alpha,\beta\in Aut(L)$.

Proof. The equivalence of the six conditions follows from Theorem 4 and the proof of Theorem 2. The last part is simple.

Corollary 4. *Let* $(L,\cdot)$ *be a quasigroup(loop) with holomorph* $H(L)$. *If* $H(L)$ *is a CIPQ (CIPL) then,* L *is a flexible unipotent CIPQ (flexible CIPL of exponent* 2*).*

Proof. It is observed that $J_{\rho}=J_{\lambda}=I$. Hence, the conclusion follows. □

Example 2.1 *Let* $(L,\cdot)$ *be an abelian group with* $Inn_{\rho}(L)$*-holomorph* $H(L)$. $H(L)$ *is an abelian group.*

Proof. In an extra loop L, $Inn_{\rho}(L)=Inn_{\lambda}(L)\leq Aut(L)$ is a boolean group, hence it is abeilan group. An abelian group is a commutative extra loop. A commutative extra loop is a CIPL. So by Corollary 1, $H(L)$ is a CIPL. $H(L)$ is a group since L is a group. A group is a CIPL if and only it is abelian. Thus, $H(L)$ is an abelian group.

Remark 1. *The holomorphic structure of loops such as extra loop, Bol-loop, C-loop, CC-loop and A-loop have been found to be characterized by some special types of automorphisms such as*

1. *Nuclear automorphism(in the case of Bol-,CC- and extra loops),*
2. *central automorphism(in the case of central and A-loops).* □

By Theorem 2 and Corollary 1, the holomorphic structure of AIPLs and CIPLs is characterized by commutative automorphisms. The abelian group in Example 1 is a boolean group.

2.2 A Pair of AIPLs and CIPLs

Theorem 5. *Let* $U=(L,\oplus)$ *and* $V=(L,\otimes)$ *be quasigroups such that* $Aut(U)$ *and* $Aut(V)$ *are conjugates in* $SYM(L)$ *i.e there exists a* $\psi\in SYM(L)$ *such that for any* $\gamma\in Aut(V)$*,* $\gamma=\psi^{-1}\alpha\psi$ *where* $\alpha\in Aut(U)$*. Then,* $H(U)\cong H(V)$ *if and only if* $x\delta\otimes y\gamma=(x\beta\oplus y)\delta\,\forall\, x,y\in L,\beta\in Aut(U)$ *and some* $\delta,\gamma\in Aut(V)$ *. Hence:*

1. $\gamma\in Aut(U)$ if and only if $(I,\gamma,\delta)\in AUT(V)$.

2. if U is a loop, then; (a) $L_{e\delta}\in Aut(V)$. (b) $\beta\in Aut(V)$ if and only if $R_{e\gamma}\in Aut(V)$.

where e is the identity element in U and L_x, R_x are respectively the left and right translations mappings of $x\in V$.

3. if $\delta=I$, then $|\,Aut(U)\,|=|\,Aut(V)\,|=3$ and so $Aut(U)$ and $Aut(V)$ are boolean groups.

4. if $\gamma=I$, then $|\,Aut(U)\,|=|\,Aut(V)\,|=1$.

Proof.

1. Let $H(L,\oplus)=(H,\circ)$ and $H(L,\otimes)=(H,\text{e})$. $H(U)\cong H(V)$ if and

only if there exists a bijection $\phi : H(U) \to H(V)$ such that $[(\alpha,x)\circ(\beta,y)]\phi = (\alpha,x)\phi\text{e}(\beta,y)\phi$. Define $(\alpha,x)\phi = (\psi^{-1}\alpha\psi, x\psi^{-1}\alpha\psi)\,\forall\,(\alpha,x)\in(H,\circ)$ where $\psi \in SYM(L)$.

$H(U) \cong H(V) \Leftrightarrow (\alpha\beta, x\beta \oplus y)\phi = (\psi^{-1}\alpha\psi, x\psi^{-1}\alpha\psi)\text{e}(\psi^{-1}\beta\psi, y\psi^{-1}\beta\psi) \Leftrightarrow$

2. $(\psi^{-1}\alpha\beta\psi, (x\beta \oplus y)\psi^{-1}\alpha\beta\psi) = (\psi^{-1}\alpha\beta\psi, x\psi^{-1}\alpha\beta\psi \otimes y\psi^{-1}\beta\psi) \Leftrightarrow$
$(x\beta \oplus y)\psi^{-1}\alpha\beta\psi = x\psi^{-1}\alpha\beta\psi \otimes y\psi^{-1}\beta\psi \Leftrightarrow x\delta \otimes y\gamma = (x\beta \oplus y)\delta$
where $\delta = \psi^{-1}\alpha\beta\psi$, $\gamma = \psi^{-1}\beta\psi$.

3. Note that, $\gamma L_{x\delta} = L_{x\beta}\delta$ and $\delta R_{y\gamma} = \beta R_y \delta\,\forall\, x,y \in L$. So, when U is a loop, $\gamma L_{e\delta} = \delta$ and $\delta R_{e\gamma} = \beta\delta$. These can easily be used to prove the remaining part of the theorem.

Theorem 6. *Let $U = (L,\oplus)$ and $V = (L,\otimes)$ be quasigroups(loops) that are isotopic under the triple of the form $(\beta^{-1}\delta, \gamma, \delta)$ for all $\beta \in Aut(U)$ and some $\delta, \gamma \in Aut(V)$ such that their automorphism groups are non-trivial and are conjugates in $SYM(L)$ i.e there exists a $\psi \in SYM(L)$ such that for any $\gamma \in Aut(V)$, $\gamma = \psi^{-1}\alpha\psi$ where $\alpha \in Aut(U)$. Then, U is a AIPQ or CIPQ(AIPL or CIPL) if and only if V is a AIPQ or CIPQ(AIPL or CIPL).*

Proof. Let U be an AIPQ or CIPQ (AIPL or CIPL), then since $H(U)$ has a subquasigroup (subloop) that is isomorphic to U and that subquasigroup (subloop) is isomorphic to a subquasigroup(subloop) □ of $H(V)$ which is isomorphic to V , V is a AIPQ or CIPQ(AIPL or CIPL). The proof for the converse is similar.

2.3 Application to Cryptography

Let the Keedwell CIPQ be the quasigroup U in Theorem 5. Definitely, its automorphism group is non-trivial because as shown in Theorem 2 of Keedwell [17], for any CIPQ, the mapping $J_\rho : x \to x^\rho$ is an automorphism. This mapping will be trivial only if U is unipotent. For instance, in Example 2.1 of Keedwell [17], the CIPQ $(G,\circ)$ obtained is unipotent because it was constructed using the cyclic group $C_5 =< c : c^5 = e >$ and defined as $a \circ b = a^3 b^2$. But in Example 2.2, the CIPQ is not unipotent as a result of using the cyclic group $C_{11} =< c : c^{11} = e >$. Thus the choice of a Keedwell CIPQ which suits our purpose in this work for a cyclic group of order n is one in which $rs = n+1$ and $r+s \neq n$. Now that we have seen a sample for the choice of U, the quasigroup V can then be obtained as shown in Theorem 5. By Theorem 6, V is a CIPQ.

After the use of the latin square of the CIPQ U as look up tables T_2 and T_3 and its long inverse cycle T_1, for a guaranteed secured period of time, U needed to be changed according to Keedwell [17] for better security. So, we can now replace U with V which is also a CIPQ. This replacement can be computerized and incorporated into the computerization of encryption process with U since V is gotten from U via isotopy. Now, according to Theorem 5, by the choice of the mappings $\alpha, \beta \in Aut(U)$ and $\psi \in SYM(L)$ to get the mappings δ, γ, a CIPQ V can be produced following Theorem 5 using the isotopism $(\beta^{-1}\delta, \gamma, \delta)$ of Theorem 6. Note that the automorphism groups of $U = (L, \oplus)$ and $V = (L, \otimes)$ are not trivial since by Theorem 3, $H(U)$ is a CIPQ if and only if $Aut(U)$ is trivial and U is a CIPQ ($H(V)$ is a CIPQ if and only if $Aut(V)$ is trivial and V is a CIPQ). And in Theorem 5 and Theorem 6, we need just U being a CIPQ and $H(U) \cong H(V)$ but not $H(U)$ and $H(V)$ being CIPQs.

2.4 Concluding Remarks

The appropriateness of a CIPQ V to replace a CIPQ U follows from the fact that they are isotopic, which is a strong relation. The production of the new look up tables T_1, T_2 and T_3 from the new CIPQ V will be done by the key distribution centre. If the multiplication of elements x, y in $U = (L, \oplus)$ was $x \oplus y$, then the new multiplication of x, y in $V = (L, \otimes)$ will be $x \otimes y = (x\delta^{-1}\beta \oplus y\gamma^{-1})\delta \ where \ \beta \in Aut(U), \delta, \gamma \in Aut(V)$.

References

[1] J. O. Adeniran (2005): *On holomorphic theory of a class of left Bol loops*, Al.I.Cuza 51(1), pp. 23--28.

[2] J. O. Adeniran, Y. T. Oyebo and D. Mohammed (2011): *On certain isotopic maps of central loops*, Proyecciones Journal of Mathematics, 30(3), pp. 303-318.

[3] R. Artzy (1955): *On loops with special property*, Proc. Amer. Math. Soc. 6, pp. 448--453.

[4] R. Artzy (1959): *Crossed inverse and related loops*, Trans. Amer. Math. Soc. 91(3), pp. 480--492.

[5] R. Artzy (1959): *On Automorphic-Inverse Properties in Loops*, Proc. Amer. Math. Soc. 10(4), pp. 588--591.

[6] R. Artzy (1978): *Inverse-Cycles in Weak-Inverse Loops*, Proc. Amer. Math. Soc. 68(2), pp. 132--134.

[7] V. D. Belousov and B. F. Curkan (1969): *Crossed inverse quasigroups(CI-quasigroups)*, Izv. Vyss. Ucebn; Zaved. Matematika 82, pp. 21--27.

[8] R. H. Bruck (1944): *Contributions to the theory of loops*, Trans. Amer. Math. Soc. 55, pp. 245--354.

[9] R. H. Bruck and L. J. Paige (1956): *Loops whose inner mappings are automorphisms*, The annuals of Mathematics, 63(2), pp. 308--323.

[10] V. O. Chiboka and A. R. T. Solarin (1991): *Holomorphs of conjugacy closed loops*, Scientific Annals of Al.I.Cuza. Univ. 37(3), pp. 277--284.

[11] W. Diffie and M. E. Hellman, (1976): *New directions in cryptography*, IEE Trans. Inform. Theory IT-22, pp. 644--654.

[12] J. H. Ellis, (1970): *The possibility of secure non-secret digtal encryption*, CESG Report.

[13] J. H. Ellis (1987): *The story of non-secret digital encryption*, http://www.cesg.gov.uk/ellisdox.ps.

[14] J. H. Ellis (1987): *The history of Non-Secret Encryption*, http://www.cesg.gov.uk/about/nsecret.htm.

[15] E. D. Huthnance Jr.(1968): *A theory of generalised Moufang loops*, Ph.D. thesis, Georgia Institute of Technology.

[16] T. G. Jaiyé ọ lá (2008): *An holomorphic study of Smarandache automorphic and cross inverse property loops*, Proceedings of the 4th International Conference on Number Theory and Smarandache Problems, Scientia Magna Journal, 4(1), pp. 102--108.

[17] A. D. Keedwell (1999): *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin. 20, pp. 241—-250.

[18] A. D. Keedwell and V. A. Shcherbacov (2002): *On m-inverse loops and quasigroups with a long inverse cycle*, Australas. J. Combin. 26, pp. 99—-119.

[19] A. D. Keedwell and V. A. Shcherbacov (2003): *Construction and properties of* (r,s,t) *-inverse quasigroups I*, Discrete Math. 266, pp. 275—-291.

[20] A. D. Keedwell and V. A. Shcherbacov (2004): *Construction and properties of* (r,s,t) *-inverse quasigroups II*, Discrete Math. 288, pp. 61—71.

[21] J. M. Osborn (1961): *Loops with the weak inverse property*, Pac. J. Math. 10,pp. 295--304.

[22] D. A. Robinson (1964): *Bol loops*, Ph.D. thesis, University of Wisconsin, Madison, Wisconsin.

[23] D. A. Robinson (1971): *Holomorphic theory of extra loops*, Publ. Math. Debrecen 18, pp. 59--64.