
**УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП**
**ФАКУЛТЕТ ЗА ИНФОРМАТИКА**

ISSN:1857-8691

# ГОДИШЕН ЗБОРНИК
# 2013
# YEARBOOK
# 2013

**ГОДИНА 2** **VOLUME II**

**GOCE DELCEV UNIVERSITY - STIP**
**FACULTY OF COMPUTER SCIENCE**

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“ – ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА


# ГОДИШЕН ЗБОРНИК
# 2013
# YEARBOOK
# 2013

ГОДИНА 2 МАРТ, 2014 VOLUME II

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**

# CALCULATION OF MULTI-STATE TWO TERMINAL RELIABILITY

Natasha Stojkovic[1], Limonka Lazarova[2] and Marija Miteva[3]

[1]Faculty of Computer Science, “Goce Delcev” University– Stip
(natasa.maksimova, limonka.lazarova, marija.miteva)@ugd.edu.mk

**Abstract.** Traditionally, reliability of the transportation system has been analyzed from a binary perspective**.** It is assumed that a system and its components can be in either a working or a failed state. But, many transportation systems as: telecommunication systems, water distribution, gas and oil production and hydropower generation systems are consisting of elements that may operate in more than two states. The problem that we consider in this paper is known as the multi-state two terminal reliability computation. The multi – state two terminal reliability can be computed with the formula of inclusion and exclusion, if the minimal path vector or minimal cut vector are known.

**Keywords:** multi-state systems, network reliability, minimal path vectors, minimal cut vectors.

## 1 Introduction

Two-terminal network reliability for binary transportation system has been studied in various ways. For the binary network it is assumed that a whole system and its components can be in two states: working or failed state. However, the binary approach does not completely describe some transportation systems. Such systems are telecommunication systems, water distribution, gas and oil production and hydropower generation systems. These networks and its components may operate in any of several intermediate states and better results may be obtained using a multi-state reliability approach.[1]
The authors developed a multi-state approach for exact computation of multi-state two-terminal reliability at demeaned level $d$ ($M2TR_d$). The multi-state two terminal reliability is defined as the probability that a demand of $d$ units can be transmitted from source to sink nodes through multi-state edges [2]. The multi – state two terminal reliability can be computed if the minimal path vector or minimal cut vectors are known. In the literature many algorithms for calculating on minimal path or cut vectors are known.

Some algorithms for obtaining minimal path or cut vectors are given in [1], [2], [3] and [4]. In [1] is developed a multi-state approach for exact computation of multi-state two-terminal reliability. In the paper is proposed algorithm for obtaining minimal path vector. Disadvantage of this algorithm is that it gives candidates minimal path vectors that are not minimal. In [2] is proposed algorithm for obtaining minimal cut vectors for the multi-state two-terminal transportation system. The disadvantage of this algorithm is that it works only for weak homogeneous components. The components can have different number of state, but the first state of the components has to be the same. In [3]

is proposed algorithm for obtaining minimal path vectors. This algorithm has restriction for the values of capacities on the edges. The capacities on the edges can be only valued from the set of integer number. In [4], it is proposed an algorithm for obtaining the minimal path vector that does not require any restrictions for the values of the capacities of the links.

## 2 Basic definition

In this paragraph we will give some basic definitions for binary two terminal network.

Let $G(V,E)$ be a multi- state two terminal network. By $V$ the set of nodes is denoted, and by $E=\{e_i \mid 1\le i\le |E|\}$ the set of edges is denoted. Multi-state edge is defined as an edge of the system, which has a set of states $\{r\le \cdot 100\% \mid r\in[0,1]\}$. The state 0 is appropriate in case when there is no stream over the edge. The state 100% is appropriate on the state, when the edge works with full capacity. Intermediate states are all states in which could be found edge between the state 0 and the state in which the system works with total capacity. State space set is the vector which presents the state of the components.

For example, let the edge of the transport system has three different states: 0%, 50%, 100%. Then the vector $(0,0.5,1)$ is the vector of the states of that edge.

For any multi-state edge, the vector of the capacity **(Capacity Vector - Capacity State Set)** is obtained as a product of the full capacity of the edge and the vector of the state of that link. Let suppose that the edge described before, in perfect conditions could transfer flow equal to 8 units. The vector of the capacities, obtained in this way is equal to $S_i=(8\cdot 0,8\cdot 0.5,8\cdot 1)=(0,4,8)$.

**Capacity state set S,** as the set of the all possible capacities from the source to the sink, for the total system is defined. For some simplifications, the states could be numerated in different ways. For example, it can be supposed that the perfect state at the level 2,50% corresponds to 1, and the state of the total breakdown corresponds to 0. In this way, the vector (0, 1, 2) is obtained.

Let $x_i$ be the state of the link $e_i$. The vector $\vec{x}=(x_1,x_2,\ldots,x_n)$ which describes the states of all components of the system, is called **state vector.** The set of all state vectors is called state of the system $N=S_1\times S_2\times\ldots\times S_{|E|}$.

The function $\varphi: N\to S$ where $\varphi(\vec{x})$ is the potential capacity from the source to the sink. If the system is in the state $\vec{x}$, it is called **multi – state structural function.**

**Definition 1. Multi-state two terminal reliability for the level** $d$ (M2TR$_d$) is the probability of the event, that the flow is larger or equal to *d* and could be successfully transfered from the source to the sink.

$$M2TR_d = P\left(\varphi\left(\vec{x}\right) \geq d\right) \quad (1)$$

**Definition 2.** A vector $\vec{y}$ is said to be less than $\vec{x}$, $\vec{y} < \vec{x}$**,** (or dominated by $\vec{x}$ **)** if $\forall i$, $y_i \leq x_i$ and for some $k$, $y_k < x_k$.

**Definition 3.** A vector $\vec{x}$ is said to be a **minimal path vector to level** $d$ if $\varphi\left(\vec{x}\right) \geq d$ and if for every $\vec{y} < \vec{x}$, $\varphi\left(\vec{x}\right) < d$.

**Definition 4.** A vector $\vec{x}$ is said to be a **minimal cut vector to level** $d$ if $\varphi\left(\vec{x}\right) < d$ and if for every other $\vec{y} > \vec{x}$, $\varphi\left(\vec{x}\right) \geq d$. [4,5]

In order to determine the structure of the transport system we define binary path vector. We are considering multi-state transport system with set of the nodes $V$ and set of the edges $E = \{e_i \mid 1 \leq i \leq n\}$. We consider transportation system with the same nodes and edges. All the edges in this system are binaries, i.e. the set of the state of the links is {0,1}. Let $\vec{v}$ be the minimal path vector for this transportation system. We say that $\vec{v}$ is binary minimal path vector for the multi-state transport system. With BPV we denote the set of binary minimal path vectors.

With $TS = (V, E, BPV, S, VP)$, we denote the transportation system, where $V$ is the set of the nodes, $E$ is the set of the edges, $BPV$ is the set of binary minimal path vectors, $S$ is the set of capacity vectors of the components and $VP$ is the set of the probabilities on the level of the components, where $\vec{p}_i$ is vector of the probabilities on the $i$-th edges i.e. $p_{id} = P(x_i = d)$.

## 3 Calculating on the multi – state two terminal reliability

We will show how the reliability of multi state system, when the minimal path vectors are known, can be calculated. For the binary system, reliability could be solved by the following formula:

$$R = P\left(\bigcup_{h=1}^{j} \mathcal{P}_h\right) = \sum_{h=1}^{j} P(\mathcal{P}_h) - \sum_{h<k}^{j} P(\mathcal{P}_h \cap \mathcal{P}_k) + \ldots (-1)^j P(\mathcal{P}_1 \cap \ldots \cap \mathcal{P}_j).$$

(2)

where $j$ is a number of minimal paths, and $P_h$ is a $h$ - the minimal path [5].

This formula can be extended for the new structure of the vectors from the minimal sets. In the case of multi state system $M2TR_d$ can be obtained with the following modification of the formula of inclusion and exclusion

$$M2TR_d = \sum_{h=1}^{T} P\left(\vec{x} \geq \vec{y}_h\right) - \sum_{h<k}^{T} P\left(\vec{x} \geq \vec{y}_h \wedge \vec{x} \geq \vec{y}_k\right) + \ldots (-1)^T P\left(\vec{x} \geq \vec{y}_1 \wedge \ldots \wedge \vec{x} \geq \vec{y}_T\right)$$

(3)

where $T$ is number of the $MPV_d$ (minimal path vectors on level $d$) and $\vec{y}_h \in MPV_d$. By using of the notation

$$\max(\vec{z}_1, \ldots, \vec{z}_s) = (\max(z_1^{(1)}, \ldots, z_s^{(1)}), \ldots, \max(z_1^{(l)}, \ldots, z_s^{(l)}) \quad (4)$$

where $z_u^{(v)}$ is v-th coordinate of the coordinate $\vec{z}_u$, and the equation (3) can be written in the form:

$$M2TR_d = \sum_{h=1}^{T} P(\vec{x} \geq \vec{y}_h) - \sum_{h<k}^{T} P(\vec{x} \geq \max(\vec{y}_h, \vec{y}_k)) + \ldots (-1)^T P(\vec{x} \geq \max(\vec{y}_1, \ldots, \vec{y}_T))$$

(5)

**Algorithm for reliability calculating**

**Input:** Binary minimal path vectors $BPV$, set of the capacity vectors of the components *S*, and the set of the probabilities of the components levels $VP$.

**Output:** Reliabilities $M2TR_d$, for $m < d < M$, $m$ is the minimal level of the system work and $M$ is the maximal level of the system work.

**Step 1.** Finding the minimal path vectors for level $d$, $D = \left\{\vec{z}_1, \vec{z}_2, \ldots, \vec{z}_n\right\}$ with the algorithm proposed in [1-4].

**Step 2.** Finding all possible non empty subsets of the set *D*.

**Step 3.** For every subset $D_r$ $1 \le r \le 2^T - 1$ obtained in the step 2, it is find the supremum, $\vec{v}_r = \sup D_r$, according to the ordering relation $f$ given in definition 2, in this way every coordinate is equal to the maximum of the appropriate vector coordinates in that subset.

**Step 4.** Finding of the probabilities $P\left(\varphi(\vec{x}) \ge \vec{v}_r\right)$ and application of the formula 5 in order to obtain the reliability $M2TR_d$.

---

From the previous algorithm we can concluded that multi – state two terminal transportation system can be computed if minimal path vectors are given. In the Example 1, we will show minimal path vectors for level 1,2,3,4 for the system from Figure 1, and appropriate reliability.

**Example 1**. Let us consider the simple transportation system in Figure 1.

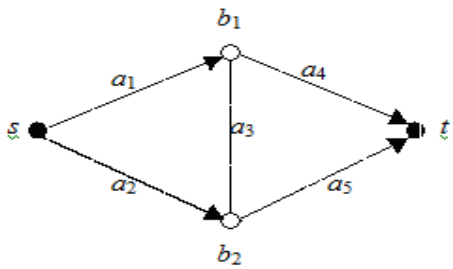



Figure 1. Two terminal transportation system

Capacities of the edges are $S_1$={0,1,2}, $S_2$={0,1,2}, $S_3$={0,1}, $S_4$={0,1} and $S_5$={0,1,2,3}. Probabilities that the edges can be in some state are: $p_1$=(0.1,0.1,0.8), $p_2$=(0.1,0.1,0.8), $p_3$=(0.1,0.9), $p_4$=(0.1,0.9) and $p_5$=(0.1,0.05,0.05,0.8).

The vector of maximal state will be *M*=(2,2,1,1,3).
We suppose that binary path vectors that are minimal path vectors to level 1 are known. With $MP_i$ we will denote minimal path vector to level $i$.

$MP_1$={(1,0,1,0,1), (1,0,0,1,0), (0,1,1,1,0), (0,1,0,0,1)}
$M2TR_1$=0.97686.
$MP_2$ = {(2,0,1,1,1), (1,1,0,1,1), (1,1,1,0,2), (0,2,1,1,1), (0,2,0,0,2)}
$M2TR_2$=0.84614

$MP_3$ = {(2,1,1,1,2), (1,2,0,1,2), (1,2,1,0,3)}
$M2TR_3$=0.64584

$MP_4$ = {(2,2,1,1,3)}
$M2TR_4$=0.3686

## 4 Conclusion

This paper presents an algorithm for calculating a multi-state two terminal reliability. With this algorithm reliability to level $d$ can be calculated when the minimal path vectors to level $d$ are known.

## References

[1] J.E. Ramirez-Marquez and D. Coit, D. (2003): *Alternative Approach for Analyzing Multistate Network Reliability*, *IERC Conference Proceedings* 2003

[2] J.E. Ramirez-Marquez, D. Coit, and M. Tortorella: *Multi-state Two-terminal Reliability: A Generalized Cut-Set Approach*, Rutgers University IE Working Paper 2004

[3] M. Mihova, M. and N. Synagina: *An algorithm for calculating multi-state network reliability using minimal path vectors*, The 6th international conference for Informatics and Information Technology (CIIT 2008)

[4] M. Mihova M, N. Maksimova, Z. Popeska: An algorithm for calculating multi-state network reliability with arbitrary capacities of the links”- Fourth International Bulgarian-Greek Conference Computer Science’2008 (170-175)

[5] Н. Максимова (2009): *Надежност на повеќе- состојбени двотерминални транспортни системи.* Магистерска теза, Институт за информатика, ПМФ Скопје

# INCREASING THE FLEXIBILITY AND APPLICATION OF THE B- SPLINE CURVE

**Julijana Citkuseva[1], Aleksandra Stojanova[1], Elena Gelova[1]**

**Faculty of computer science, "Goce Delcev" University, Stip, Macedonia**
(julijana.citkuseva, aleksandra.stojanova, elena.gelova)@ugd.edu.mk

**Abstract:** One of the main tasks of geometrical modelling is to find ways of designing and representing freeform curves and surfaces. One of well-known geometric modeling tools in computer aided geometric design are B-spline curves and surfaces. B-spline is smooth in parts of polynomial functions with reduced smoothness. In this article we will give ways of increasing the flexibility of the B - spline curve as well as its applications together with associated examples made using the program package Wolfram Mathematica 8.

**Keywords:** b-spline model, knot vector, control polygon, Bezier curve, multiple knot.

## 1. Introduction

A spline curve is a sequence of curve segments that are connected together to form a single continuous curve. B-spline curve addresses problems with the Bezier curve. It provides the most powerful and useful approach to curve design available today.

Freeform curves and surfaces have very broad application. Thus, Bezier-curves are used to draw the path of motion of a point (object). In 3D animations, these curves are used to determine the three-dimensional path and two-dimensional curve for interpretation of key segments. B –splines are used for modeling animation characters for the purposes of modeling animated movies and True Type fonts, as illustrated in this article.

B spline models were first mentioned by Schoenberg [19]. Initially, the practical application of B-spline curves and surfaces was limited by the instability of the algorithms for their calculation. This setback was resolved by Cox and de Boor [6] who proposed algorithm for numerical computation based on recursive template. Then, Reisenfeld [19] revealed that B-spline is a powerful tool for representing free-form shapes and applied B spline base for curves definitions.

### 1.1 Organization of the paper.

First we will give a brief overview of methods that are used for increasing flexibility of B-spline curves emphasizing two techniques: degree raising and knot inserting. Then, we give two examples of B-spline application.

## 1 Increasing the flexibility of the B- spline curve

If $\mathrm{S}_k = \left[ B_0^k(t) \;\; B_1^k(t) \;\ldots\; B_n^k(t) \right]^{\mathrm{T}}$ is B spline base defined in vector form, then,

$$\mathbf{S}_k(\mathrm{P};\mathrm{t}) = S_k^{\mathrm{T}} \cdot \mathbf{P} = \sum_{i=0}^{n} B_i^k(t)\mathrm{P}_i, \quad t \in [t_{k-1}, t_{n+1})$$

is B spline curve defined with vector $\mathbf{P} = [\mathrm{P}_0 \;\cdots\; \mathrm{P}_n]^{\mathrm{T}}$, where $\mathrm{P}_i$ are points of the control polygon for the curve.

It is clear that the choice of base functions and choice of knot vectors significantly affects the shape of the B-spline curve.

To obtain B-spline curve with greater flexibility two techniques are used:

- Raising the degree and
- Inserting knots (subdivision).

The advantage of raising a degree is that B-spline curve retains smoothness and while applying subdivision decreases differentiability of embedded knots, which depends on multiplicity of elements in the knot vector. If the knot vector doesn't have multiple elements, application of subdivision reduces differentiability to k-2 order.

By raising the degree of B-spline curve, the new curve should be identical to the original curve, i.e.

$$\mathbf{S}_k(\mathrm{P};\mathrm{t}) = \sum_{i=1}^{n+1} B_i^k(t)\mathrm{P}_i = \sum_{i=1}^{m+1} B_i^{k+1}(t)\mathrm{P}_i^*,$$

where $\mathrm{P}_i^*$ are points of the control polygon for the new curve.

By raising the degree or order of B-spline curve, it becomes smoother compared to the control polygon. Also, the appearance of multiple internal elements in the vector of knots for B spline base functions, means a reduction of continuity in the value for the knot, and drawing the resulting B-spline curve closer to a control polygon. These effects indicate that there are multiple internal elements in the knot vector.

The flexibility of B - spline curve also increases by inserting additional elements in the knot vector. Adding a single element in the knot vector is called knot insertion, and insertion of multiple elements in the knot vector is called a knot refining.

There are two basic methods of inserting knots. The first method contains the so-called Oslo algorithm developed by Cohen [19] and colleagues and Prautzch algorithm, and consists of simultaneously inserting multiple elements in the knot vector. The second method, developed by Boehm [19 ] consists of repeatedly inserting single element in the knot vector.

Let

$$\mathbf{S}_k(\mathrm{P};\mathrm{t}) = \sum_{i=1}^{n+1} B_i^k(t)\mathrm{P}_i$$

is an initial curve with the knot vector

$$\tau = [t_1 \;\; t_2 \;\; \cdots \;\; t_{n+k+1}].$$

The new curve, which is obtained after the insertion of knots is defined by

$$\boldsymbol{R}_k(\mathrm{P};s) = \sum_{j=1}^{m+1} M_j^k(s)\mathrm{C}_j$$

Where $\tau^* = [y_1 \;\; y_2 \;\; \cdots \;\; y_{m+k+1}]$, $m > n$ is the new knot vector and $\mathbf{S}_k(\mathrm{P};\mathrm{t}) = \boldsymbol{R}_k(\mathrm{P};s)$.

To determine the new points of the control polygon Oslo algorithm is used.

$$\mathrm{C}_j = \sum_{i=1}^{n+1} \alpha_{i,j}^k P_i \quad 1 \le i \le n, \quad 1 \le j \le m,$$

where $\alpha_{i,j}^k$ are given with recursive relation

$$\alpha_{i,j}^1 = \begin{cases} 1 & t_i \le y_j < t_{i+1} \\ 0 & \text{otherwise} \end{cases},$$

$$\alpha_{i,j}^k = \frac{y_{j+k-1} - t_i}{t_{i+k-1} - t_i}\alpha_{i,j}^{k-1} + \frac{t_{i+k} - y_{j+k-1}}{t_{i+k} - t_i}\alpha_{i+1,j}^{k-1},$$

where $\sum_{i=1}^{n+1} \alpha_{i,j}^k = 1$.

After inserting the value for the knot, if the original knot vector is uniform, periodic or open, then the end vector nodes are non-uniform. Uniform knot vector can be obtained by inserting multiple values for knot in the middle of each not null interval.

**Example 1.** Consider B spline curve of order k = 3 defined by four points of the control polygon

$$\mathrm{P}_1(0,0), \quad \mathrm{P}_2(1,4), \quad \mathrm{P}_3(3,2), \quad \mathrm{P}_4(4,3)$$

and open uniform knot vector $\tau = [0 \;\; 0 \;\; 0 \;\; 1 \;\; 2 \;\; 2 \;\; 2]$.

We will perform subdivision of curve, inserting the value 1 in the knot vector between knots 0 and 1, i.e. the knot vector is $\tau^* = [0 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 2 \;\; 2 \;\; 2]$. So, starting from uniform, non-uniform open knot vector with one double knot is obtained. Using the Oslo algorithm, the new control points of the polygon are obtained.

$\mathrm{C}_1 = \alpha_{3,1}^3\mathrm{P}_1 = \mathrm{P}_1 = (0,0),$
$\mathrm{C}_2 = \alpha_{3,2}^3\mathrm{P}_2 = \mathrm{P}_2 = (1,4),$
$\mathrm{C}_3 = \alpha_{2,3}^3\mathrm{P}_2 + \alpha_{3,3}^3\mathrm{P}_3 = \frac{1}{2}(\mathrm{P}_2 + \mathrm{P}_3) = (2,3),$
$\mathrm{C}_4 = \alpha_{3,4}^3\mathrm{P}_3 = \mathrm{P}_3 = (3,2),$
$\mathrm{C}_5 = \alpha_{4,5}^3\mathrm{P}_4 = \mathrm{P}_4 = (4,3).$

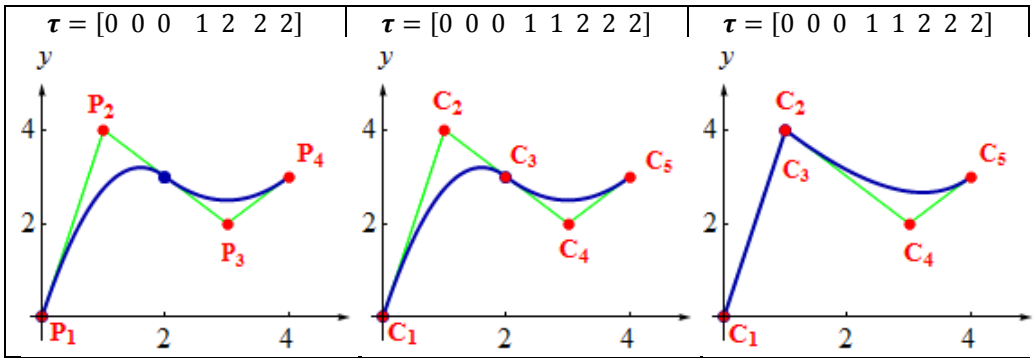



**Figure 1**. Impact of change in the control point polygon

**Figure 1:** Left, shows the B - spline curve obtained from the initial control polygon, with open uniform vector nodes. The graph in the middle shows the curve after the subdivision. We note that the curve does not change, but the control polygon is changed and now it has five points, and the knot vector is changed too. If points $C_3$ and $C_2$ match, then despite the double element in the knot vector corresponding to $C_2 = C_3$, there is a double point in the control polygon and the resulting curve will peak in the double knot , as presented in Figure 1 . Right.

## 2 Application of B-spline

B splines are very widely used in computer design. Below we give two examples of their application.

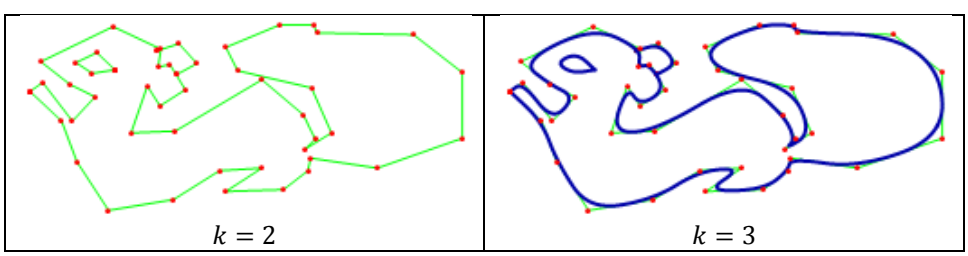
**Example 2.** B splines can be used for drawing animated characters for animated movie's needs. The draw for the various parts of the animated character required different control polygons. In this example the animated character of a squirrel is drawn, starting from three control polygons. The first caracter defines the body, the second the eye, and the third one defines the right ear of the squirrel:

**P-body** = {(8,138), (8,138), (22,148), (55,105), (80,132), (52,146), (20,171), (100,210), (153,185), (150,165), (163,168), (180,140), (152,122), (138,144), (120,92), (169,94), (265,151), (311,112), (324,85), (313,74), (342,92), (320,142), (238,161), (225,187), (285,212), (322,212), (326,203), (433,201), (487,159), (487,86), (393,53), (319,64), (316,50), (289,29), (225,27), (265,53), (218,50), (167,18), (95,6), (60,60), (43,105), (8,138), (8,138)};

**P- eye** = {(102,162), (102,162) ,(82,181), (59,170), (77,158), (102,162), (102,162)};

**P- ear** = {(148,183), (148,183), (173,191), (193,169), (171,157), (171,157)}.

In Figure 2, right in the front row a figure of a squirrel is presented derived from B-spline curve of order k = 2, (control polygons). The remaining graphs can be obtained when B-spline curves in order k = 3,4,5,6 and 7.



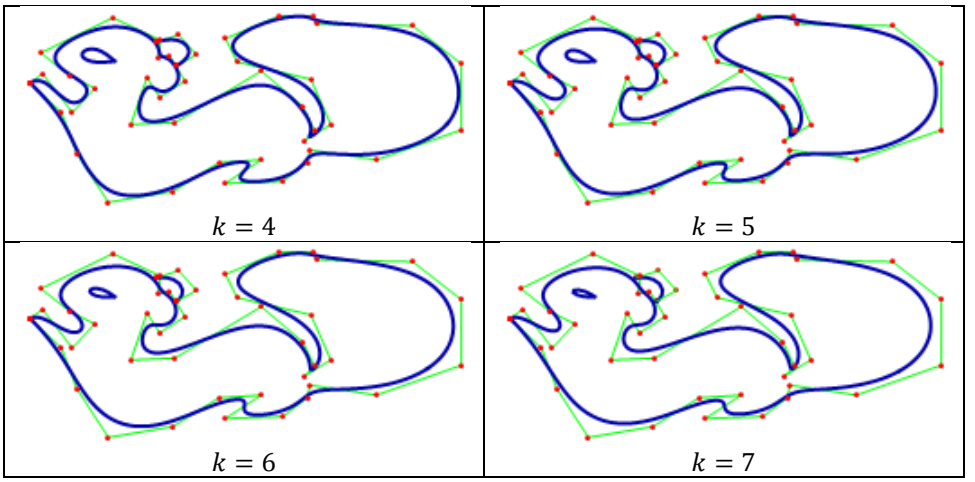


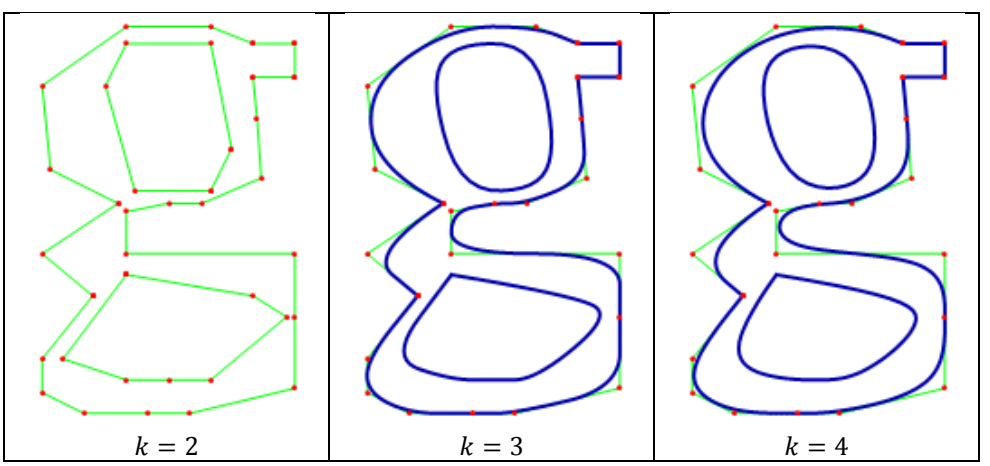

**Figure 2**. Application of B-splines for drawing squirrel

**Example 3**. This example will illustrate the application of B-spline for modeling True Type and Post Script fonts, modeling the letter g. First we define the control polygons:

**P1** = {(2.8, 5.2), (1, 4), (2.2, 3), (2.2, 3), (2.2, 3), (1, 1.5), (1, 0.7), (2, 0.2), (3.5, 0.2), (4.5, 0.2), (7, 0.8), (7, 2.5), (7, 4), (3, 4), (3, 5), (4, 5.2), (4.8, 5.2), (6.2, 5.8), (6.1, 7.2), (6, 8.2), (6, 8.2), (7, 8.2), (7, 8.2), (7, 9), (7, 9), (6, 9), (6, 9), (5, 9.4), (3, 9.4), (1, 8), (1.2, 6), (2.8, 5.2)};

**P2** = {(3, 3.5), (3, 3.5), (1.5, 1.5), (3, 1), (4, 1), (5, 1), (6.8, 2.5), (6, 3), (3, 3.5)};

**P3** = {(5, 5.5), (5.5, 6.5), (5, 9), (3, 9), (2.5, 8), (3.2, 5.5)}.



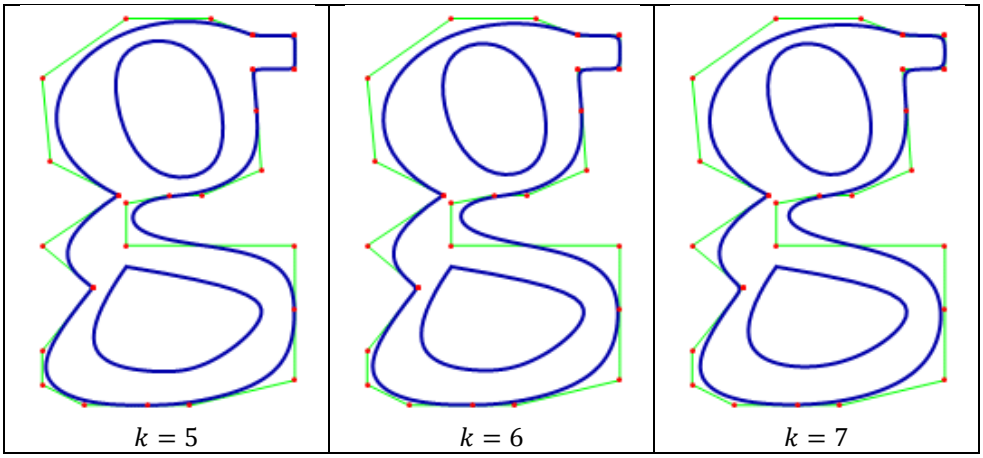



**Figure 4**. Application of B-splines for modeling fonts

**Figure 4:** Shows the obtained B-spline curves in order k = 2, 3, 4, 5, 6 and 7.

## 3 Conclusion

B-splines are not used very often in 2D graphics software but are used quite extensively in 3D modeling software. They have an advantage over Bézier curves, so that they are smoother and easier to control. B-splines consist entirely of smooth curves, but sharp corners can be introduced by joining two spline curve segments. The continuous curve of a b-spline is defined by control points. While the curve is shaped by the control points, it generally does not pass through them.

Application of the free-form curves is not limited to computer graphics, only. They have an important application in the calculation of optimal orbit and trajectory of aircraft flight. The most commonly used are Bézier and B-spline curves, but there are other splines as Hermit spline, Catmull-Rom spline and T-spline.

## References

[1] Anant U., *Shape-preserving Interpolation with Biarcs and NURBS*, Doctoral Thesis, Department of Computer Science University of Manitoba Winnipeg, Manitoba, Canada, 2009.

[2] Andersson F., *Bezier and B-SplineTechnology*, Umea university Sweden, 2003.

[3] Casiola G., Morigi S., *Reparametrization of NURBS curves*, International Journal of Shape Modelling, Vol. 2, No. 2&3 (1996), 103-116.

[4] Casiola G., *A System to Model and Render NURBS curves and Surfaces*, University of Bologna, 2000.

[5] Coxeter H.S.M., *Introduction to Geometry*, second edition, John Wiley & Sons, INC, 1969.

de Boor C., B-Spline Basics, web page http://128.105.2.28/debooron/bsplbasic.pdf.

[6] Dyn N., *Linear Subdivision Schemes for Refinement of Geometric Objects*, http://www.math.tau.ac.il/~niradyn/papers/final.pdf , 2002.

[7] Dyn N., Levin D., *Subdivision schemes in geometric modeling*, Acta Numerica, 11 , pp 73-144 doi:10.1017/S0962492902000028 (2002).

[8] Gallier J., *Geometric Methods and Applications for Computer Science and Engineering*, Springer-Verlag, TAM, Vol.38, 2000.

[9] Hu S. M., Li Y. F., Ju T., Zhu X., , *Modifying the shape of NURBS surfaces with geometric constrains*, Computer Aided Design 33 (2001) 903-912.

[10] Iglesias A., *B-splines and NURBS Curves and Surfaces,* http://etsiso2.macc.unican.es/~cagd.

[11] Iglesias A., Gutiérrez F., Gálvez A., *A Mathematica Package for CAGD and Computer Graphics*, web page http://education.siggraph.org/conferences/eurographics/gve-99/proceedings/papers/gve99-a-iglesias.pdf.

[12] Kocić Lj. M., *Geometrijsko modeliranje*, Univerzitet u Nišu, Elektronski Fakultet, 2010.

[13] Levin D., Dyn N., *Subdivison Schemes in Geometric Modelling*, Tel-Aviv University, Izrael, 2002.

[14] Lowther J., Houghton S., *Teaching B-splines Is Not Difficult*, Department of Computer Science Michigan Technological University MI 49931–1295.

[15] Mortenson M. E., *Geometric Transformations for 3D Modeling*, Industrial Press Inc., 2. Edition, 2007.

[16] Piegl L., Tiller W., *The NURBS Book*, Springer 1997.

[17] Piegl L., Tiller W., *Curve and surface constructions using rational B-splines*, Comput. Aided Design **19** (1987), No. 9, 485-498.

[18] Rogers D. F., *An Introduction to NURBS: with historical perspective*, Academic Press, 2001.

[19] Sederberg T. W., *Computer Aided Geometric Design Course Notes,* Department of Computer Science, Brigham Young University, 2011.

# WAVELET APPLICATION IN SOLVING ORDINARY DIFFERENTIAL EQUATIONS USING GALERKIN METHOD

**Jasmina Veta Buralieva [1,*], Sanja Kostadinova [2] and Katerina Hadzi-Velkova Saneva [3]**

[1]Faculty of computer science, “Goce Delcev” University -Stip, [2] Faculty of Electrical Engineering and Information Technologies, Skopje;
jasmina.buralieva@ugd.edu.mk, (ksanja, saneva)@feit.ukim.edu.mk;

**Abstract.** The Galerkin method is one of the most used methods for finding numerical solutions of ordinary and partial differential equations. Its simplicity makes it suitable for many applications. In this paper we show that the wavelet-Galerkin method is an improvement over the standard Galerkin method for ordinary differential equations.

**Keywords**. condition number, sparse matrix, wavelet, scaling function, wavelet-Galerkin method.

## 1. Introduction

The concepts of wavelet theory were provided by Meyer, Mallat, Daubechies, and many others, [4], [8], [10]. Since the beginning, the number of applications where wavelets have been used has exploded. In areas such as time-series analysis, approximation theory and numerical solutions of differential equations, wavelets are recognized as powerful weapons not just tools, [1], [2], [3], [7], [11], [12], [13].

In general, it is not always possible to obtain exact solution of an arbitrary differential equation. This necessitates either to go for discretization of differential equations leading to numerical (approximate) solutions, or for qualitative study which is concerned with deduction of important properties of the solutions without actually solving them. In the early nineties, scientists were very optimistic because it seemed that many fine properties of wavelets can be directly applied and would automatically lead to efficient numerical method for solving differential equations. The reason for this optimism was the fact that many nonlinear partial differential equations (PDEs) have solution containing local phenomena and interactions between several scales. Such solutions can be well represented in wavelet basis because of its satisfactory properties such as compact support (locality in time domain) and vanishing moments (locality in frequency domain).

The Galerkin method is one of the best known methods for finding numerical solutions of ordinary and partial differential equations. Its simplicity makes it perfect for many applications. The wavelet-Galerkin method is an improvement over the standard Galerkin method by using a compactly supported orthogonal functional basis, [2], [11], [12], [13]. The translates of a wavelet for all dilations form an unconditional orthonormal basis of $L^2(\mathbb{R})$ and the translates of a scaling function for all dilations form an unconditional orthonormal basis for $V_j \subset L^2(\mathbb{R})$, which is a great improvement over the standard polynomial basis or a trigonometric basis which not necessarily have to be unconditional.

The aim of this article is to throw some light on this aspect of wavelet analysis for numerical and qualitative analysis of ordinary differential equations. Section 2 is of preliminary character; we describe the spaces of functions that we use throughout this paper, we also recall some basic wavelet tools such as multiresolution analysis (MRA) and define the condition number of a matrix. In Section 3 we describe the classical Galerkin method for numerical solving of Sturm-Liouville differential equation which comes down to solve a linear system of equations, or equivalently, a matrix equation $AX = Y$. For numerical purposes, there are two properties that we would like the matrix $A$ to have. Firstly, we would like $A$ to have a small condition number, to obtain stability of the solution under small perturbations in the data. Secondly, for performing with $A$ quickly, we would like $A$ to be sparse, which means that $A$ should have a high proportion of entries that are 0. In this paper we show that the two desirable properties of matrix $A$ can be achieved if we use the wavelets as basis vectors.

## 2. Preliminaries and Notations

**2.1. Spaces of functions.** $L^2(\mathbb{R})$ is a Hilbert space of square integrable functions on the real line with the inner product $\langle f, g \rangle = \int_{\mathbb{R}} f(t)\overline{g}(t)dt$, where $\overline{g}(t)$ is a complex conjugate of $g(t)$. The Fourier transform of a function $f \in L^2(\mathbb{R})$ is given with

$$\hat{f}(\omega) = \int_{-\infty}^{\infty} f(t)e^{-i\omega t}dt.$$

The Hilbert space of square integrable functions on [0,1], with the inner product

$$\langle f, g \rangle = \int_0^1 f(t)\overline{g}(t)dt,$$

is denoted by $L^2([0,1])$. $\mathbb{C}^2([0,1])$ is the space of functions on $[0,1]$ with continuous derivatives up to order 2.

**2.2. The condition number of a matrix.** The methods for numerically solving linear ordinary differential equation often come down to solving a linear system of equations, or equivalently, the matrix equation $AX = Y$. Theoretically, such a system is well understood: for a square matrix $A$, there exists a unique solution $X$ for every $Y$ if and only if $A$ is an invertible matrix. However, in applications there are further issues that are of crucial importance. It is often observed that for two close values of $Y$, for example $Y'$ and $Y''$, the appropriate obtained solutions $X'$ and $X''$ are far apart. Such a linear system is called badly conditioned. In this situation, small errors in data $Y$ can lead to large error in the solution $X$. A measure of the stability of the linear system $AX = Y$ under perturbation of the data $Y$ is a condition number of a matrix $A$.

Let $A$ be a $n \times n$ matrix. The *operator norm*, or just *the norm* of $A$ is defined by

$$\|A\| = \sup \frac{\|Az\|}{\|z\|}, \tag{2.1}$$

where the supremum is taken over all nonzero complex vectors $z$ in $\mathbb{C}^n$.

Let $A$ be an invertible $n \times n$ matrix. A *condition number* $C_{\#}(A)$ of $A$, is defined by

$$C_{\#}(A) = \|A\| \|A^{-1}\|,$$

where $A^{-1}$ is the inverse matrix for *A*. It is clear that $C_{\#}(A) \geq 1$. It is known that if $A$ is normal invertible matrix then

$$C_{\#}(A) = \frac{|\lambda|_{\max}}{|\lambda|_{\min}} \tag{2.2}$$

where $|\lambda|_{\max} = \max\{|\lambda| : \lambda \text{ is an eigenvalue of A}\}$ and $|\lambda|_{\min} = \min\{|\lambda| : \lambda \text{ is an eigenvalue of A}\}$. If $A$ is unitary matrix, then $C_{\#}(A) = 1$. For irregular matrix A, $C_{\#}(A) = \infty$.

In applications, a small condition number (i.e. near 1) is desirable. In case when $C_{\#}(A)$ is high, the system $AX = Y$ can be replaced with the equivalent system $BAX = BY$, where $B$ is a preconditioning matrix such that $C_{\#}(BA) < C_{\#}(A)$. In theory this is always possible, i.e. for an invertible matrix $A$, $B = A^{-1}$.

**2.3. Wavelets and Multiresolution analysis (MRA).** Let $\psi_{a,b}$, $a > 0, b \in \mathbb{R}$ be a family of functions defined as translations (or shifting) by factor *b* and dilatation (or scaling) by factor *a* of the function $\psi \in L^2(\mathbb{R})$

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right).$$

The function $\psi \in L^2(\mathbb{R})$ (called a *wavelet* or *mother wavelet*) is assumed to satisfy the admissibility condition

$$C_\psi = \int_{-\infty}^{\infty} \frac{|\hat{\psi}(\omega)|^2}{|\omega|} d\omega < \infty,$$

which implies that

$$\hat{\psi}(0) = \int_{-\infty}^{\infty} \psi(t)dt = 0 \,. \tag{2.3}$$

One can prove that, if $\int_{-\infty}^{\infty} \psi(t)dt = 0$ and $\int_{-\infty}^{\infty} (1+|t|^{\alpha})|\psi(t)|dt < \infty$ for some $\alpha > 0$, then $C_{\psi} < \infty$, [1].

In most situations, it is useful to restrict $\psi$ to be well localized both in time and frequency domains. For time localization, $\psi(t)$ and its derivatives must decay very rapidly, while for frequency localization, $\hat{\psi}(\omega)$ must decay sufficiently fast as $|\omega| \to \infty$ and $\hat{\psi}(\omega)$ must become flat in the neighborhood of 0. The flatness is associated with the number of vanishing moments of $\psi(t)$ since

$$\int_{-\infty}^{\infty} t^k \psi(t)dt = 0 \Leftrightarrow \hat{\psi}^{(k)}(0) = 0 \tag{2.4}$$

for *k* = 0, 1, …, *n.* It means that larger number of vanishing moments more is the flatness $\omega$ is small.

The notion of multiresolution analysis (MRA) was introduced in 1988/89 by Mallat and Meyer as a natural approach to the wavelet orthonormal basis. One can easily obtain a wavelet basis associated to the particular multiresolution approximation as follows.

A *multiresolution analysis* (MRA) of space $L^2(\mathbb{R})$ consists of a sequence of closed subspaces $\{V_j\}_{j=-\infty}^{\infty}$ (called *approximation spaces*) with the following properties:

1. $V_j \subset V_{j+1}$, $j \in \mathbb{Z}$;
2. $\overline{\bigcup_{j\in\mathbb{Z}} V_j} = L^2(\mathbb{R})$; $\bigcap_{j\in\mathbb{Z}} V_j = \{0\}$;
3. $f(t) \in V_j \Leftrightarrow f(2t) \in V_{j+1}$;
4. $f(t) \in V_j \Leftrightarrow f(t-k) \in V_j$, $\forall k \in \mathbb{Z}$;
5. There exists a function $\phi$ (called *scaling function* or *father wavelet*) such that $\phi_{j,k}(t) = 2^{j/2}\phi(2^j t - k), k \in \mathbb{Z}$ constitute orthonormal basis for corresponding subspace $V_j$.

Let $\phi \in L^2(\mathbb{R})$ be compactly supported scaling function of MRA. Then

$$\int_{-\infty}^{\infty} \phi(t)dt \neq 0 \,, \tag{2.5}$$

and $\phi$ satisfies the following dilatation equation

$$\phi(t) = \sqrt{2}\sum_{k\in\mathbb{Z}} a_k \phi(2t-k) \tag{2.6}$$

where $a_k$ are real coefficients and $a_k \neq 0$ for only finitely many $k \in \mathbb{Z}$ (the number of nonzero coefficients $a_k$ in the series (2.6) is denoted by *L*). Since $\phi_{j,k}(t) = 2^{j/2}\phi(2^j t - k)$, $j,k \in \mathbb{Z}$ are orthonormal in $L^2(\mathbb{R})$, we have

$$\int_{-\infty}^{\infty} \phi(t-n)\phi(t-k)dt = \delta_{k,n} \tag{2.7}$$

where $\delta_{k,n}$ is the Kronecker delta function such that $\delta_{k,n} = 0$ for $n \neq k$ and $\delta_{k,n} = 1$ for $n = k$.

If $\phi \in L^2(\mathbb{R})$ be compactly supported scaling function of MRA, one can construct the wavelet $\psi$ such that $\psi_{j,k}(t) = 2^{j/2}\psi(2^j t - k), j,k \in \mathbb{Z}$ constitute an orthonormal basis for $L^2(\mathbb{R})$. It can be shown [4], that if $\hat{\phi}$ and $\hat{\psi}$ are the Fourier transforms of the scaling function and its corresponding wavelet, then, the following relation holds

$$\hat{\psi}(\omega) = \left( \left(\hat{\phi}(\omega/2)\right)^2 - \left(\hat{\phi}(\omega)\right)^2 \right)^{1/2} e^{i\omega/2}, \tag{2.8}$$

or equivalently,

$$\psi(t) = \sqrt{2}\sum_{k\in\mathbb{Z}} (-1)^k \overline{a_{-1-k}}\phi(2t-k). \tag{2.9}$$

The simplest example of MRA is the Haar multiresolution analysis. In this case

$$\phi(t) = \begin{cases} 1, & 0 \le t < 1 \\ 0, & \text{otherwise} \end{cases}. \tag{2.10}$$

Consequently to (2.8), we obtain that $\psi(t) = \phi(2t) - \phi(2t-1)$, that is

$$\psi(t) = \begin{cases} 1, & 0 \le t < \frac{1}{2} \\ -1, & \frac{1}{2} \le t < 1 \\ 0, & \text{otherwise} \end{cases}. \tag{2.11}$$

The Haar wavelet $\psi(t)$ is developed by Alfred Haar in 1910, long before anyone began speaking of wavelets.

3. Wavelet-Galerkin method for Sturm-Liouville equation

**3.1. Sturm-Liouville equation.** We consider the class of ordinary differential equations (known as Sturm-Liouville equations) of the form

$$Lu(t) = -\frac{d}{dt}\left( a(t)\frac{du}{dt} \right) + b(t)u(t) = f(t),\ 0 \le t \le 1, \tag{3.1}$$

with Dirichlet boundary conditions

$$u(0) = u(1) = 0. \tag{3.2}$$

Let $a(t)$, $b(t)$ and $f(t)$ be a real-valued functions, such that $f(t)$ and $b(t)$ are continuous functions and $a(t)$ has a continuous derivative on $[0,1]$. Note that *L* may be differential operator with variable coefficient because $a(t)$ and $b(t)$ are not necessarily constants. We assume that the operator *L* is *uniformly elliptic*, which means that there exist constants $C_1 > 0$, $C_2 > 0$ and $C_3 > 0$ such that

$$0 < C_1 \le a(t) \le C_2 \text{ and } 0 \le b(t) \le C_3 \text{ for all } t \in [0,1]. \tag{3.3}$$

By the theory of ordinary differential equations, it is known that there is a unique function *u* satisfying equation (3.1) and the boundary conditions (3.2).

**3.2. Galerkin method for ordinary differential equations.** For the Galerkin method [9], [12], we suppose that $\{v_j\}$ is a complete orthonormal system (orthonormal basis) for $L^2([0,1])$, and that every $v_j$ is $\mathrm{C}^2([0,1])$ function that satisfies

$$v_j(0) = v_j(1) = 0 .$$

We select some finite set $\Lambda$ of indices $j$ and consider the subspace

$$S = span\{v_j, j \in \Lambda\},$$

i.e. the set of all finite linear combination of the elements $\{v_j\}$, $j \in \Lambda$.

We look for an approximation $u_s$ of the exact solution $u$ of the equation (3.1) in the form

$$u_s = \sum_{k\in\Lambda} x_k v_k \in S ,$$

(3.4)

where the coefficients $x_k, k \in \Lambda$ are unknown. Our criterion for determining the coefficients $x_k$ is that $u_s$ should behave like the true solution $u$ on the subspace $S$, i.e.

$$\langle Lu_s, v_j \rangle = \langle f, v_j \rangle , \ \forall j \in \Lambda .$$

(3.5)

If we substitute equation (3.4) in equation (3.5) we obtain

$$\sum_{k\in\Lambda} \langle Lv_k, v_j \rangle x_k = \langle f, v_j \rangle , \ \forall j \in \Lambda .$$

(3.6)

Let $X$ denote the vector $(x_k)_{k\in\Lambda}$ and let $Y$ be the vector $(y_k)_{k\in\Lambda}$ where $y_k = \langle f, v_k \rangle$. Let $A = [a_{j,k}]_{j,k\in\Lambda}$ where $a_{j,k} = \langle Lv_k, v_j \rangle$. Thus, (3.6) is a linear system of equations

$$\sum_{k\in\Lambda} a_{j,k} x_k = y_j \quad j \in \Lambda$$

(3.7)

or,

$$AX = Y .$$

(3.8)

For each subset $\Lambda$ we obtain an approximation $u_s \in S$ to the true solution $u$, by solving the linear system (3.8) for $X$ and then we determine $u_s$ by equation (3.4).

We expect that as we increase our set $\Lambda$ in some systematic way, our approximations $u_s$ should converge to the true solution $u$. Now, our main concern is the nature of the linear system, resulting from the choice of wavelet basis as opposed to some other basis, for example, Fourier basis. For numerical purposes, there are two properties that we would like the matrix $A$ in the linear system (3.8) to have. First, we would like $A$ to have a small condition number, to obtain stability of the solution under small perturbations in the data. Second, for performing with $A$ quickly, we would like $A$ to be sparse, which means that $A$ should have a high proportion of entries that are 0. In the rest of the paper we will show that the two desire properties of matrix $A$ can be achieved if we use the wavelets as basis vectors.

**3.3. Wavelet-Galerkin method for ordinary differential equations**. As we emphasized, the family of wavelets $\psi_{j,k}(t) = 2^{j/2}\psi(2^j t - k), j,k \in \mathbb{Z}$ constitute an orthonormal basis for $L^2(\mathbb{R})$. We assume the possibility of modifying the wavelet system for $L^2(\mathbb{R})$, so as to obtain a complete orthonormal system $\{\psi_{j,k}\}_{(j,k)\in\Gamma}$ for $L^2([0,1])$. The set $\Gamma$ is a certain subset of $\mathbb{Z}\times\mathbb{Z}$ that we do not specify. The functions $\psi_{j,k}$ are not exactly the same functions as in a wavelet basis for $L^2(\mathbb{R})$, but they

are similar. In particular, $\psi_{j,k}$ has a scale of about $2^{-j}$, and is concentrated near the point $2^{-j}k$, and $\psi_{j,k}$ is 0 outside an interval centered at $2^{-j}k$ of length proportional to $2^{-j}$. Wavelets concentrated well into the interior of $[0,1]$ are nearly the same as usual wavelets, but those concentrated near the boundary points are substantially modified. After the modifications, $\forall(j,k)\in\Gamma$, $\psi_{j,k}$ should be $\mathbb{C}^2$ function and satisfy the boundary conditions

$$\psi_{j,k}(0)=\psi_{j,k}(1)=0.$$

Now, we rewrite the equations (3.4) and (3.6) using the fact that the wavelets are indexed by two integers, in the form

$$u_s=\sum_{(j,k)\in\Gamma}x_{j,k}\psi_{j,k},$$

and

$$\sum_{(j,k)\in\Gamma}\left\langle L\psi_{j,k},\psi_{l,m}\right\rangle x_{j,k}=\left\langle f,\psi_{l,m}\right\rangle,\ \forall(l,m)\in\Gamma. \tag{3.9}$$

We can still regard this, as a matrix equation $AX=Y$, where the vectors $X=(x_{j,k})_{(j,k)\in\Gamma}$ and $Y=(y_{j,k})_{(j,k)\in\Gamma}$, $y_{j,k}=\left\langle f,\psi_{j,k}\right\rangle$ are indexed by pairs $(j,k)\in\Gamma$, and $A=[a_{l,m;j,k}]_{(l,m);(j,k)\in\Gamma}$, $a_{l,m;j,k}=\left\langle L\psi_{j,k},\psi_{l,m}\right\rangle$. The pairs $(l,m)$ and $(j,k)$ represent row and column of $A$ respectively.

Next, we will prove that if the matrix $A$ does not have a low condition number or is not sparse, then the system $AX=Y$ can be replaced with the equivalent system $MZ=V$, for which the new matrix $M$ has the desire properties, i.e. $M$ is sparse matrix and has smaller condition number than *A*. Indeed, we define matrix $M=[m_{l,m;j,k}]_{(l,m),(j,k)\in\Gamma}$ by

$$M=D^{-1}AD^{-1}, \tag{3.10}$$

where $D=[d_{l,m;j,k}]_{(l,m),(j,k)\in\Gamma}$,

$$d_{l,m;j,k}=\begin{cases}2^j, & (l,m)=(j,k)\\ 0, & (l,m)\neq(j,k)\end{cases}$$

is diagonal matrix.

Since $\det(D)=2^{jn}$, its inverse matrix $D^{-1}$ is

$$D^{-1}=\frac{1}{\det(D)}adjD=\frac{1}{2^{jn}}\begin{bmatrix}2^{j(n-1)} & 0 & 0 & \dots & 0\\ 0 & 2^{j(n-1)} & 0 & \dots & 0\\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 2^{j(n-1)}\end{bmatrix}_{n\times n}=$$

$$=\frac{1}{2^{jn}}2^{j(n-1)}\begin{bmatrix}1 & 0 & 0 & \dots & 0\\ 0 & 1 & 0 & \dots & 0\\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1\end{bmatrix}_{n\times n}=\begin{bmatrix}2^{-j} & 0 & 0 & \dots & 0\\ 0 & 2^{-j} & 0 & \dots & 0\\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 2^{-j}\end{bmatrix}_{n\times n}.$$

Then, for the elements of matrix *M* we have

$$m_{l,m;j,k} = 2^{-l-j} a_{l,m;j,k} = 2^{-l-j} \left\langle L\psi_{j,k}, \psi_{l,m} \right\rangle \tag{3.11}$$

Since $AX = Y \Leftrightarrow D^{-1}AD^{-1}DX = D^{-1}Y$, setting $Z = DX$ and $V = D^{-1}Y$, we obtain the equivalent system $MZ = V$.

The matrix *M* is sparse, because of the good localization (compact support) of the wavelets. Namely, $\psi_{j,k}$ is 0 outside an interval of length $c2^{-j}$ around the point $2^{-j}k$, for some constant $c$ (depending on the choice of wavelet system). Because the operator $L$ involves only differentiation and multiplication by another function, it does not change this localization property. So, $L\psi_{j,k}$ is 0 outside this interval as well. Similarly, $\psi_{l,m}$ is 0 outside an interval of length $c2^{-l}$ around the point $2^{-l}m$. As $j$ and $l$ get large, fewer and fewer of these intervals intersect, so more and more of the matrix elements

$$m_{l,m;j,k} = 2^{-l-j} a_{l,m;j,k} = 2^{-l-j} \left\langle L\psi_{j,k}, \psi_{l,m} \right\rangle = 2^{-l-j} \int_0^1 L\psi_{j,k}(t)\, \overline{\psi_{l,m}(t)}\, dt$$

are 0. So *M* is sparse, which makes computation with it easier.

It is proved in [11] that if $\{\psi_{j,k}\}_{(j,k)\in\Gamma}$ is wavelet system, then there exist constants $C_4, C_5 > 0$ such that for all functions $g$ of the form $g = \sum_{(j,k)\in\Gamma} c_{j,k}\psi_{j,k}$ (the sum is finite), it holds

$$C_4 \sum_{(j,k)\in\Gamma} 2^{2j} \left|c_{j,k}\right|^2 \le \int_0^1 \left|g'(t)\right|^2 dt \le C_5 \sum_{(j,k)\in\Gamma} 2^{2j} \left|c_{j,k}\right|^2 . \tag{3.12}$$

The next proposition shows that the condition number of matrix *M* is bounded, independently of the set of indices, so the new equivalent system *MZ=V* is well conditioned.

**Proposition 3.1.** [11, Theorem 1.2] Let *L* be a uniformly elliptic Sturm-Liouville operator. Let $\{\psi_{j,k}\}_{(j,k)\in\Gamma}$ be a complete orthonormal system for $L^2([0,1])$ such that $\psi_{j,k}$ is in $C^2([0,1])$, satisfies $\psi_{j,k}(0) = \psi_{j,k}(1) = 0$ and (3.12) holds. Let $\Lambda$ be a finite subset of $\Gamma$.

Then the condition number of *M* defined by (3.10) satisfies the following inequality

$$C_{\#}(M) \le \frac{(C_2 + C_3)C_5}{C_1 C_4}$$

for any finite set $\Lambda$, where the constants $C_1, C_2, C_3$ are determined by (3.3), and $C_4, C_5$ by (3.12).

**Remark.** In most practical situations, it is usefully to restrict $\psi$ to have a larger number of vanishing moments (see eq. (2.4)). So, if *f* (*t*) is a polynomial, then $y_{j,k} = \left\langle f, \psi_{j,k} \right\rangle = 0$, i.e. *B* is a null-matrix. So, according to (2.5), it is much more suitable to work with the scaling function $\phi$ and not with the actual wavelet $\psi$.

In the next example, we will use the Haar scaling function and the corresponding wavelet. It will be shown that the numerical results obtained by using the Haar scaling function are better than the ones obtained by the Haar wavelet.

**Example.** We consider the differential equation

$$u''(t) - u(t) = t - 1,\ 0 \le t \le 1$$

with Dirihlet boundary conditions

$$u(0) = u(1) = 0\,.$$

Its exact solution is

$$u(t) = -\frac{1}{1-e^2}e^t + \frac{e^2}{1-e^2}e^{-t} - t + 1.$$

Now, we will obtain the approximate solution $u_s^1$ using a Haar wavelet (2.11). Let $\Gamma = \{(3,0);(3,1);(3,2);(3,3);(3,4);(3,5);(3,6);(3,7)\}$. The differential operator *L* is $Lu(t) = u''(t) - u(t)$, so we obtain

$$L\psi_{j,k} = -\psi_{j,k},\ \forall (j,k) \in \Gamma,\ \text{and}\ \ a_{l,m;j,k} = \left\langle L\psi_{j,k}, \psi_{l,m} \right\rangle = \begin{cases} -1, & (j,k) = (l,m) \\ 0, & (j,k) \neq (l,m) \end{cases}.$$

Since $y_{j,k} = \left\langle f, \psi_{j,k} \right\rangle$, we have

$$y_{3,k} = \left\langle f, \psi_{3,k} \right\rangle = -\frac{1}{64\sqrt{2}},\ \forall k = \overline{0,7}\,.$$

Solving the linear system $AX = Y$ where $X = (x_{j,k})_{(j,k)\in\Gamma}$, $Y = (y_{j,k})_{(j,k)\in\Gamma}$, and $A = [a_{l,m;j,k}]_{(l,m);(j,k)\in\Gamma}$, $a_{l,m;j,k} = \left\langle L\psi_{j,k}, \psi_{l,m} \right\rangle$ we get

$$x_{3,k} = \frac{1}{64\sqrt{2}},\ \forall k = \overline{0,7}$$

So the approximate solution is

$$u_s^1 = \sum_{(j,k)\in\Gamma} x_{j,k}\psi_{j,k} = 2^{3/2}\left(x_{3,0}\psi(2^3t) + x_{3,1}\psi(2^3t-1) + x_{3,2}\psi(2^3t-2) + x_{3,3}\psi(2^3t-3) + \right.$$

$$\left. + x_{3,4}\psi(2^3t-4) + x_{3,5}\psi(2^3t-5) + x_{3,6}\psi(2^3t-6) + x_{3,7}\psi(2^3t-7)\right).$$

In a similar way we obtain the approximate solution $u_s^2$ using the Haar scaling function (2.10).

Table 1. Comparison of the results using Haar wavelet and Haar scaling function

| $t$ | Exact solution $u$ | Numerical solution $u_s^1$ | Absolute error of $u_s^1$ | Numerical solution $u_s^2$ | Absolute error of $u_s^2$ |
|---|---|---|---|---|---|
| 0.0 | 0 | 0 | 0 | 0 | 0 |
| 0.1 | 0.0265183 | -0.03125 | 0.057768 | 0.09375 | 0.672317 |
| 0.2 | 0.0442945 | -0.03125 | 0.075545 | 0.08125 | 0.036956 |
| 0.3 | 0.0545074 | 0.03125 | 0.023257 | 0.06875 | 0.014243 |
| 0.4 | 0.0582599 | 0.03125 | 0.027009 | 0.05625 | 0.00201 |
| 0.5 | 0.0565906 | -0.03125 | 0.087841 | 0.05625 | 0.00034 |
| 0.6 | 0.0504834 | -0.03125 | 0.072128 | 0.04375 | 0.00673 |
| 0.7 | 0,0408782 | -0.03125 | 0.002570 | 0.03125 | 0.009628 |
| 0.8 | 0,0286795 | 0.03125 | 0.016484 | 0.01875 | 0.009929 |
| 0.9 | 0.0147663 | 0.03125 | 0.03125 | 0.00625 | 0.008516 |
| 1.0 | 0 | 0 | 0 | 0 | 0 |

**Remark.** Let us note that here we have used the simplest scaling function which is not even a smooth function. The results can be improved using scaling functions with better properties. For comparison, in [9],

the same equation is solved using the cubic spline scaling function and the obtained results are much better.

**References**

[1] A. H. Siddiqi. (2004). *Applied Functional Analysis: Numerical Methods, Wavelet Methods and Image Processing.* New York: Markel Dekker.

[2] C. Qian, J. Weiss (1993). Wavelets and numerical solution of partial deifferential equations. *Journal of Computational Physics, Vol.106, Issue 1, pp*.155-175.

[3] C. S. Salimath, *Wavelets in Numerical Analysis of Differential and Integral Equations.* Karnatak University Dharwad: Research Scholar Department of Mathematics.

[4] I. Daubechies, (1992). *Ten lecture of Wavelets.* Philadelphia: SIAM.

[5] G. G. Walter, X. Shen, (2000). *Wavelets and Other Orthonormal System with Application.* SRC Press, Secound Edition.

[6] M. W. Frazier, (1999). *An Introduction to Wavelets Through Linear Algebra.* New York: Springer-Verlag.

[7] R. T. Ogden, (1997). *Essential wavelets for Statistical Applications and Data Analysis.* Boston: Birkhauser.

[8] S. G. Mallat, (1989). Multiresolution approximations and wavelet orthonormal basis of $L^2(\mathrm{R})$, *Trans. Amer. Math. Soc., 315*, pp. 69-87.

[9] S. Kostadinova, J. Veta Buralieva, K. Hadzi-Velkova Saneva, (2013). Wavelet - Galerkin solution of some ordinary differential equations, *Proceedings of the XI International Conference ETAI 2013*, 26-28 September 2013, Ohrid, Macedonia.

[10] S. Mallat, (1989). Multiresolution approximation and wavelets. *Trans. Amer. Math. Soc., 315*, pp. 69-88.

[11] T. Lofti, K. Mahdiani. (2007). Numerical solution of baundary value problem by using wavelet-Galerkin methods. *Mathematical Sciences, Vol. 1, No. 3*, pp.7-18.

[12] U. Lepik, (2007). Application of Haar wavelet transform to solving integral and differential equations. *Proc. Estonian Acad. Sci. Phys. Math., Vol.56, no.1*, pp. 28-46.

[13] Vinod Mishra, Sabina, Wavelet Galerkin Solutions of ordinary differential equations. *Int. Journal of Math. Analysis, Vol. 5, 201, no. 9*, 408-424.

# ПРОИЗВОДИ НА ДИСТРИБУЦИИ ВО КОЛОМБООВА АЛГЕБРА

Марија Митева[1], Билјана Јолевска-Тунеска[2], Лимонка Лазарова[1]

[1] Факултет за информатика, Универзитет „Гоце Делчев“ - Штип
(marija.miteva, limonka.lazarova)@ugd.edu.mk
[2] Факултет за електротехника и информациски технологии, Скопје, Македонија
biljana j@feit.ukim.edu.mk

**Апстракт**

Во овој труд се добиени некои производи на дистрибуции. Резултатите се добиени во Коломбоова алгебра од обопштени функции, која се покажала како релевантна алгебарска структура за решавање на нелинеарни проблеми поврзани со дистрибуциите на Schwartz.

**Клучни зборови:** *дистрибуција, Коломбоова алгебра, обопштени функции на Colombeau, производ на дистрибуции.*

**Класификација на научни полиња:** 46F10, 46F30.

# PRODUCTS OF DISTRIBUTIONS IN A COLOMBEAU ALGEBRA

Marija Miteva[1], Biljana Jolevska-Tuneska[2], Limonka Lazarova[1]

[1]Faculty of computer science, Goce Delcev University, Stip, Macedonia
(marija.miteva, limonka.lazarova)@ugd.edu.mk
[2] Faculty of Electrical Engineering and Informational Technologies, Skopje, Macedonia
biljana j@feit.ukim.edu.mk

**Abstract**

In this paper some products of distributions are derived. The results are obtained in Colombeau algebra of generalized functions, which is most relevant algebraic construction for dealing nonlinear problems of Schwartz distributions.

**Keywords and Phrases:** *distribution, Colombeau algebra, Colombeau generalized functions, multiplication of distribution.*

**Mathematics Subject Classification 2010**: 46F10, 46F30.

## 1. Introduction

At the early fifty's of the last century, the French mathematician Laurent Schwartz invented his theory of generalized functions, also known today as a Theory of distributions, which has a big impact in a various fields of sciense and engineering, because of the techniques it provided when dealing with different non-linear problems that classical theory of distributions was unable to solve. One of the most useful aspects of Schwartz's theory of distributions in applications is that discontinuous functions can be handled as easily as continuous or differentiable functions which provides a powerful tool in formulating and solving many problems of various fields of maths, physics, ect. [12].

According to the distribution theory, we can distinguish two complementary points of view:

The first one is that distribution can be considered as a continuous linear functional $f$ acting on a smooth function $\varphi$ with compact support, i.e. we have a linear map

$$\varphi \to \langle f, \varphi \rangle$$

where $\varphi$ is called *test function*.

The second one is sequential approach: taking a sequence of a smooth functions $(\varphi_n)$ converging to the Dirac $\delta$ -function, we obtain a family of regularization $(f_n)$ by the convolution product

$$f_n(x) = (f * \varphi_n)(x) = \langle f(y), \varphi_n(x-y) \rangle$$

which converges weakly to the distribution $f$. We identify all the sequences that converge weakly to the same limit, we consider them as an equivalence class, so each distribution $f$ correspondes to such equivalence calss. We call the elements of each equivalence class *representatives* of the aproppriete distribution $f$. This way we obtain sequential reprezentation of distributions. Some authors use the equivalence calsses of nets of regularization, i.e. the $\delta$ -net $\left(\varphi_\varepsilon\right)_{\varepsilon>0}$ defined with

$$\varphi_\varepsilon = \frac{1}{\varepsilon}\varphi\left(\frac{x}{\varepsilon}\right)$$

But, two main problems when operating with distributions appear: not any two distributions can always be multiplied (the space of all distributions is not an algebra), and products of distributions not always satisfy the Leibniz rule for diferentiation. So, many attempts have been made to define products of distributions, or rather to enlarge the range of existing products [27]. Many attempts have been made to include the distributions into differential algebras (as an example one can see [25]).

The regularization method mentioned above is a result of a proposal for solving this problems: some modifications of functions are made in order to simlify them and make them more 'regular' (continuous, differentiable, finite, etc.). Actually, all the operations then are done with the regularized functions (the sequences of smooth functions; that's the meaning of the term '*operating in the sence of distributions*') and with the inverse process starting from the result, the function is returned from the regularization.

To overcome the problem with multiplication of distributions, the authors were searching for an associative and commutative algebra ($A(\Omega)$ *,* $+$, $\circ$), where $\Omega$ is an open set in $R^n$, satisfying following properties:

1) The space $D'(\Omega)$ of distributions over $\Omega$ is linearly embedded into $A(\Omega)$ and $f(x)\equiv 1$ is the unit in $A(\Omega)$;

2) There exist derivation operators $\partial i : A(\Omega) \to A(\Omega)$, $i = 1, 2, ..., n$, that are linear and satisfy the Leibnitz rule;

3) $\partial i|_{D'(\Omega)}$, $i = 1, 2, ..., n$, is the usual partial derivative;

4) $\circ|_{C(\Omega)\times C(\Omega)}$ is the usual product of functions.

Schwartz in his famous impossibility result [28] has shown that there isn't any algebra satisfying all these conditions. The optimal solution of this problem was offered by French mathematician Jean -Francois Colombeau who menaged to construct such an algebra in a way that the condition $C(\Omega)$ in the 4)th property above is replaced with $C^\infty(\Omega)$, i.e

4') $\circ|_{C^\infty(\Omega)\times C^\infty(\Omega)}$ is the usual product of functions

Colombeauin his books [3,1,2] described the problem of multiplication of distributions and introduced a differential algebra $G$, called Colombeau algebra, as a way for overcoming that problem. He introduced several variants of Colombeau algebras, but all of them with the property that $C^\infty$ functions are faithful differential subalgebra of $G$, something that Colombeau noticed as essential in overcoming Schwartz impossibility result. This new theory of generalized functions of Colombeau is more general then the theory of distributions. From the view point of diferentiation, these new generalized functions have the same properties as distributions. But, from the view point of product of distributions and non-linear operations, these new generalized functions have properties completly different from the properties of distributions: every finite product of generalized functions is generalized function, and moreover, the algebra of these generalized functions is closed under many non - linear operations, too. Also, every product of distributions is generalized function (in this new sense) and may not be a distribution.

In a few words, the differential Colombeau algebra $G$ as a powerful tool for treating linear and nonlinear problems including singularities has almost the optimal properties while the problem of multiplication of Schwartz distributions is concerned: it is an associative differential algebra of

generalized functions, contains the algebra of smooth functions as a subalgebra, the distribution space $\mathrm{D}'$ is linearly embedded in it as a subspace and the multiplication is compatible with the operations of differentiation and products with $C^\infty$-differentiable functions. The notion 'association' in $\mathrm{G}$ is a faithful generalization of the equality of distributions and enables obtaining results in terms of distributions again.

Colombeau's theory was primarly been used for dealing with nonlinear partial differential equations with singularities and was developed during the years and it has now a big appliance in a different fields (physics, geometry, etc. see [20, 13, 14, 21, 30, 18, 17, 26, 27, 16]).

About embedding of the space of distributions into the space of Colombeau generalized functions one can read papers [15, 25, 11, 29]. We can see some products of distributions in a Colombeau algebra in [10, 5, 6, 8, 9, 4, 7] and other papers written by this author.

Following this approach, we evaluate in this paper some product of distributions, as embedded in Colombeau algebra, in terms of associated distributions. Similar results are obtained in [23, 24, 19].

## 2 Colombeau algebra

In this section we will introduce basic notations and definitions from Colombeau theory.

N0 is the set of non-negative integers, i.e. N0 = N *{0}*.

For *q* N0 we denote

$$A_q(\mathbf{R}) = \left\{ \varphi(x) \in D(\mathbf{R}) \,\middle|\, \int_{\mathbf{R}} \varphi(x)\,dx = 1 \; and \int_{\mathbf{R}} x^j \varphi(x)\,dx = 0,\ j = 1,\ldots,q \right\}$$

where $\mathrm{D}(\mathbf{R})$ is the space of all $C^\infty$ functions $\varphi : \mathbf{R} \to \mathbf{C}$ with compact support. The elements of the set $A_q(\mathbf{R})$ are called *test functions*.

It is obvious that $A_1 \supset A_2 \supset A_3 \ldots$. Also, $A_k \neq \varnothing$ for all $k \in \mathbf{N}$ (this is proved in [3]).

For $\varphi \in A_q(\mathbf{R})$ and $\varepsilon > 0$ it is denoted $\varphi_\varepsilon = \frac{1}{\varepsilon}\varphi\left(\frac{x}{\varepsilon}\right)$ and $\overset{\vee}{\varphi}(x) = \varphi(-x)$.

Wanting to obtain an algebra containing the space of distributions, which elements could be multiplied and diferentiated as well as $C^\infty$ functions, Colombeau started with $\mathrm{E}(\mathbf{R})$, the algebra of functions $f(\varphi, x) : A_0(\mathbf{R}) \times \mathbf{R} \to \mathbf{C}$ that are infinitely differentiable with respect to the second variable, *x*. The embedding of distributions into such an algebra must be done in a way that the embedding of $C^\infty$ functions will be identity. Let $f$ and $g$ be $C^\infty$ functions. Taking the sequence $(f * \varphi_\varepsilon)_{\varepsilon>0}$, which converges to *f* in $\mathrm{D}'$, as a representative of *f*, we obtain an embedding of $\mathrm{D}'$ into $\mathrm{E}(\mathbf{R})$. So, if we consider *f* and *g* as a distributions, we look at the sequences $(f * \varphi_\varepsilon)_{\varepsilon>0}$ and $(g * \varphi_\varepsilon)_{\varepsilon>0}$. The product of $f$ and $g$ as a distributions not always coincide with their classical product considered as a distribution, i.e.

$$(f * \varphi_\varepsilon)(g * \varphi_\varepsilon) \neq (fg) * \varphi_\varepsilon$$

The idea therefore is to find an ideal $\mathrm{I}[\mathbf{R}]$ such that this diffrence will vanish in the resulting quotient. In order to determine $\mathrm{I}[\mathbf{R}]$ it is obviosly enough to find an ideal containing the differences $((f * \varphi_\varepsilon) - f)_{\varepsilon>0}$.

Expanding the last term in a Taylor series and having in mind propertis of $\varphi(x)$ as an element of $A_q(\mathbf{R})$ we can see that it will vanish faster then any power of ε, uniformly on compact

sets, in all derivatives. The set of these differences will not be an ideal in $\mathrm{E}(\mathbf{R})$ but in a set of a sequences which derivatives are bounded uniformly on compact sets by negative power of $\varepsilon$. These sequences are called 'moderate' sequences and the set containing them is denoted with $\mathrm{E}_M[\mathbf{R}]$.

Finaly, the generalized functions of Colombeau are elements of the quotient algebra

$$\mathrm{G} \equiv \mathrm{G}(\mathbf{R}) = \frac{\mathrm{E}_M[\mathbf{R}]}{\mathrm{I}[\mathbf{R}]}$$

where, as explained before, $\mathrm{E}_M[\mathbf{R}]$ is the subalgebra of 'moderate' functions such that for each compact subset *K* of R and any *p* N0 there is a *q* N such that, for each $\varphi \in A_q(\mathbf{R})$ there are *c*>0, $\eta$>0 and it holds:

$$\sup_{x \in K} \left| \partial^p f(\varphi_\varepsilon, x) \right| \le c\varepsilon^{-q}$$

for 0 <$\varepsilon$<$\eta$ and $\mathrm{I}[\mathbf{R}]$ is an ideal of $\mathrm{E}_M[\mathbf{R}]$ consisting of all functions $f(\varphi, x)$ such that for each compact subset *K* of R and any *p* N0 there is a *q* N such that for every *r*≥*q* and each $\varphi \in A_r(\mathbf{R})$ there are *c*>0, $\eta$>0 and it holds:

$$\sup_{x \in K} \left| \partial^p f(\varphi_\varepsilon, x) \right| \le c\varepsilon^{r-q}$$

for 0 <$\varepsilon$<$\eta$. Elements of $\mathrm{I}[\mathbf{R}]$ are also known as 'null' functions or 'negligible' functions.

The Colombeau algebra $\mathrm{G}(\mathbf{R})$ contains the distributions on R canonically embedded as a C-vector subspace by the map:

$$i : \mathrm{D}'(\mathbf{R}) \to \mathrm{G}(\mathbf{R}) : u \to i_0 = \left\{ i_0(\varphi, x) = \left( u * \check{\varphi} \right)(x) : \varphi \in A_q(\mathbf{R}) \right\}$$

where denotes the convolution product of two distributions and is given by:

$$(f * g)(x) = \int_{\mathbf{R}} f(y)\, g(x - y)\, dy$$

According to the above, we can also write: $i_0(\varphi, x) = \langle u(y), \varphi(y - x) \rangle$ where $\langle u, \varphi \rangle$ denotes the integral $\int_{\mathbf{R}} u(x)\varphi(x)\, dx$.

An element $f \in \mathrm{G}$ (a generalized function of Colombeau) is actually an equivalence class $[f] = [f_\varepsilon + \mathrm{I}]$ of an element $f_\varepsilon \in \mathrm{E}_M$ which is called *representative* of *f*. Multiplication and differentiation of generalized functions are performed on arbitrary representatives of the respective feneralized functions.

With the next two deffinitions, we introduce the notion of 'association'.

**Definition 2.1** *Generalized functions f, g* $\mathrm{G}(\mathbf{R})$ *are said to be associated, denoted f ≈g, if for some representatives* $f(\varphi_\varepsilon, x)$ *and* $g(\varphi_\varepsilon, x)$ *and arbitrary* $\psi(x) \in \mathrm{D}(\mathbf{R})$ *there is a* *q* N0 *such that for any* $\varphi(x) \in A_q(\mathbf{R})$

$$\lim_{\varepsilon \to 0_+} \int_{\mathbf{R}} \left| f(\varphi_\varepsilon, x) - g(\varphi_\varepsilon, x) \right| \psi(x)\, dx = 0 .$$

**Definition 2.2** *A generalizedfunction f* $\mathrm{G}(\mathbf{R})$ *is said to admit some u* $D^i(\mathrm{R})$ *as 'associated*

*distribution', denoted f ≈u, if for some representative* $f(\varphi_\varepsilon, x)$ *of f and any* $\psi(x) \in \mathrm{D}(\mathbf{R})$ *there is a q* N0 *such that for any* $\varphi(x) \in A_q(\mathbf{R})$

$$\lim_{\varepsilon \to 0_+} \int_{\mathbf{R}} f(\varphi_\varepsilon, x)\psi(x)dx = \langle u, \psi \rangle .$$

These definitions are independent of the representatives chosen and the distribution associated, if it exists, is unique. The association is a faithful generalization of the equality of distributions.

Myltiplying two distributions in $\mathrm{G}$ as a result it is in general obtained a generalized function which may not always be associated to the third distribution.

By *Colombeau product of distributions* is meant the product of their embedding in $\mathrm{G}$ whenever the result admits an associated distribution.

If the regularized model product of two distributions exists, then their Colombeau product also exists and it is same with the first one.

The relation $f \approx u$ is asymmetric, the distribution $u$ stands on the r.h.s.; the relation $f \approx u$ is an equivalent relation in $\mathrm{G}$ so it is symmetric in $\mathrm{G}$ and it can also be written as $f - u \approx 0$.

As a final conclusion of this introduction we have a fact that we operate with the elements of $\mathrm{G}$ exactly the same as with the $C^\infty$-functions, because we actually operate with their representatives which are $C^\infty$-functions.

## 3 Results on some products of distributions

In this part, we will obtain the product of distributions $x_+^p$ and $\ln x_+$ as embedded in Colombeau algebra.

For the embedding of the distribution $x_+^p$ using the embedding rule, we have:

$$\widetilde{x_+^p} = \int_0^\infty y^p \varphi_\varepsilon (y - x)dy = \frac{1}{\varepsilon}\int_0^\infty y^p \varphi\left(\frac{y-x}{\varepsilon}\right) dy$$

where $\varphi \in A_0(\mathbf{R})$. Without lost of generality we can take $\mathrm{supp}\varphi \subseteq [-l, l]$. Using substitution $v = \dfrac{y-x}{\varepsilon}$ we obtain the representative of $x_+^p$ in a Colombeau algebra:

$$\widetilde{x_+^p} = \int_0^\infty y^p \varphi_\varepsilon (y - x)dy = \frac{1}{\varepsilon}\int_0^\infty y^p \varphi\left(\frac{y-x}{\varepsilon}\right) dy$$

The same way

$$\widetilde{\ln x_+} = \int_0^\infty \ln y\, \varphi_\varepsilon (y - x)\, dy = \frac{1}{\varepsilon}\int_0^\infty \ln y \varphi\left(\frac{y-x}{\varepsilon}\right) dy$$

and with the substitution $u = \dfrac{y-x}{\varepsilon}$ we obtain:

$$\widetilde{\ln x_+} = \int_{-\frac{x}{\varepsilon}}^{l} \ln(x + \varepsilon u)\varphi(u)\, du$$

Now, for arbitrary $\psi(x)$ $\mathrm{D}(\mathbf{R})$ we have:

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}, \psi(x)\right\rangle =$$

$$= \int_{-\infty}^{\infty} \psi(x)\,dx \int_{-\frac{x}{\varepsilon}}^{l} (x+\varepsilon v)^p \varphi(v)\,dv \int_{-\frac{x}{\varepsilon}}^{l} \ln(x+\varepsilon u)\varphi(u)\,du$$

But $\psi$ ($x$) has also compact support, so we have:

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}, \psi(x)\right\rangle = \int_{-l\varepsilon}^{l\varepsilon} \psi(x)\,dx \int_{-\frac{x}{\varepsilon}}^{l} (x+\varepsilon v)^p \varphi(v)\,dv \int_{-\frac{x}{\varepsilon}}^{l} \ln(x+\varepsilon u)\varphi(u)\,du$$

Using substitution $w = -\frac{x}{\varepsilon}$, Taylor theorem for $\psi$ and changing the order of integration we obtain the integral:

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}, \psi(x)\right\rangle = \varepsilon^{p+1}\psi(0)\int_{-l}^{l}\varphi(v)\,dv\int_{v}^{l}\varphi(u)\,du\int_{v}^{u}(v-w)^p\ln(\varepsilon u-\varepsilon w)dw+O(\varepsilon)$$

With the new substitution $t = \frac{w-v}{u-v}$ we obtain

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}, \psi(x)\right\rangle =$$

$$= -\varepsilon^{p+1}\psi(0)\int_{-l}^{l}\varphi(v)dv\int_{v}^{l}(v-u)^{p+1}\varphi(u)du\left[\ln(\varepsilon u-\varepsilon v)\int_0^1(1-t)^p\,dt+\int_0^1(1-t)^p\ln t\,dt\right]+O(\varepsilon)$$

We know that $\int_0^1(1-t)^p\,dt = \frac{1}{p+1}$ and $\int_0^1(1-t)^p\ln t\,dt = -\frac{\sigma_{p+1}}{p+1}$ where $\sigma_p = \sum_{k=1}^{p}\frac{1}{k}$ for $p$ N and $\sigma_0 = 0$ so for the integral above we have:

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}, \psi(x)\right\rangle = -\frac{\varepsilon^{p+1}}{p+1}\psi(0)\int_{-l}^{l}\varphi(v)\,dv\int_{v}^{l}(v-u)^{p+1}\varphi(u)\ln(\varepsilon u-\varepsilon v)\,du$$

$$-\frac{\varepsilon^{p+1}\sigma_{p+1}}{p+1}\psi(0)\int_{-l}^{l}\varphi(v)dv\int_{v}^{l}(v-u)^{p+1}\varphi(u)du+O(\varepsilon)$$

By the properties of test functions, $\int u^k\varphi(u)du = 0$ for $k \geq 1$ and $\int\varphi(u)du = 1$, so the second integral above is zero and we have:

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}(\varphi_\varepsilon, x), \psi(x)\right\rangle = -\frac{\varepsilon^{p+1}}{p+1}\psi(0)\int_{-l}^{l}\varphi(v)\,dv\int_{v}^{l}(v-u)^{p+1}\varphi(u)\ln(\varepsilon u-\varepsilon v)\,du+O(\varepsilon)$$

Next, using integration by part for the integral $\int_v^l(v-u)^{p+1}\varphi(u)\ln(\varepsilon u-\varepsilon v)du$ we have:

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}(\varphi_\varepsilon, x), \psi(x)\right\rangle = -\frac{\varepsilon^{p+1}}{p+1}\psi(0)\int_{-l}^{l} v^{p+1}\varphi(v)\ln(\varepsilon u-\varepsilon v)\,dv$$

$$+\frac{\varepsilon^{p+1}}{p+1}\psi(0)\int_{-l}^{l}\varphi(v)dv\int_{v}^{l}\frac{v^{p+1}}{u-v}du+O(\varepsilon)$$

Applying integration by parts for the first integral above we estimate its value is 0 whereas

$$\left\langle \widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}(\varphi_\varepsilon, x), \psi(x)\right\rangle = \frac{\varepsilon^{p+1}}{p+1}\psi(0)\int_{-l}^{l} v^{p+1}\varphi(v)\,dv\int_{v}^{l}\frac{du}{u-v}+O(\varepsilon)$$

$$=\frac{\varepsilon^{p+1}}{p+1}\psi(0)\int_{-l}^{l} v^{p+1}\varphi(v)\ln|u-v|\,dv+O(\varepsilon)$$

Applying integration by parts once again,we obtain that

$$\widetilde{x_+^p}(\varphi_\varepsilon, x)\cdot \widetilde{\ln x_+}(\varphi_\varepsilon, x)\approx 0$$

## References

[1] Colombeau, J. F. *Elementary introduction new generalized functions* , North Holland Math. Studies 113, Amsterdam (1985).
[2] Colombeau, J. F. *Multiplication of Distributions* , Springer-Verlag (1992).
[3] Colombeau, J. F. *New generalized functions and multiplication of distribution*, North Holland Math. Studies 84, Amsterdam (1984).
[4] Damyanov, B. *Balanced Colombeau products of the distributions* $x_{\pm}^{-p}$ *and* $x^{-p}$, Czechoslovak Mathematical Journal,Vol. 55, No.1, 189-201 (2005).
[5] Damyanov, B. *Some distributional products of Mikusi´nski type in the Colombeau algebra* $G(\mathrm{R}^m)$, Journal of analysis and its applications,Volume20,No3, 777785 (2001).
[6] Damyanov, B. *Multiplication of Schwartz Distributions and Colombeau Generalized Functions*, Journal of Applied Analysis, vol. 5, No. 2, pp. 249-260 (1999).
[7] Damyanov, B. *Mikusi´nski type Products of Distributions in Colombeau Algebra*, Indian J. pure appl. Math, 32(3): 361-375, March2001.
[8] Damyanov, B. *Modelling and Products of Singularities in Colombeau Algebra G*(R), Journal of Applied Analysis, vol. 14, No. 1, pp. 89-102 (2008).
[9] Damyanov, B. *Results on Balanced products of the distributions* $x_{\pm}^{a}$ *in Colombeau algebra G*(R), Integral Transforms and Special functions, vol. 17, No. 9, 623-635, September 2006.
[10] Damyanov, B. *Results on Colombeau product of distributions*, Comment. Math. Univ. Carolinae 43, 627-634 (1997).
[11] Delcroix, A. *Remarks on the Embedding of Spaces of Distributions into Spaces of Colombeau Generalized Functions*. Novi Sad J. Math.Vol. 35, No. 2, 27-40 (2005).
[12] Farassat, F. *Introduction to GeneralizedFunctions With Applications in Aerodynamics and Aeroacoustics* , NASA Technical Paper 3428
[13] Grosser, M.,Farkas, E., Kunzinger, M., Steinbauer, R. *On the foundations of nonlinear generalized functions I, II*. Mem. Amer. Math. Soc., 153(729) (2001).
[14] Grosser, M., Kunzinger, M., Steinbauer, R., Vickers, J. *Aglobal theory of algebras of generalized functions*. Adv. Math., 166:179206
[15] Gsponer, A. *The sequence of ideas in a rediscovery of the Colombeau algebras*. Report ISRI-08-01, July, 2008.
[16] Gsponer, A. *A concise introduction to Colombeau generalized functions and their applications in classical electrodynamics*. Eur. J. Phys. /30/, 109–126, (2009).
[17] Hormann, G., Oberguggenberger, M. *Elliptic Regularity and Solvability for Partial Differential*

*Equations with Colombeau Coefficients* Electronic Journal of Differential Equations,Vol. 2004, No. 14, 130 (2004).

[18] Jolevska, T. B., Takaci, A., Ozcag, E. *On Differential Equations with Nonstandard Coefficients*. Applicable Analysis and Discrete Mathematics, 1, 276283 (2007).

[19] Jolevska, T. B., Atanasova, P. T. *Further results on Colombeau product of distributions*, IJMMS, Volume 2013, Article ID 918905, 5 pages, http://dx.doi.org/10.1155/2013/918905.

[20] Kunzinger, M., Steinbauer, R. *Foundations of a nonlinear distributional geometry*. Acta Appl. Math., 71:179206 (2002). (2002).

[21] Kunzinger, M., Oberguggenberger, M. *Group analysis of differential equations and generalizedfunctions*. SIAM J. Math. Anal., 31(6):11921213(2000).

[22] Li, C. K. *Several results on the commutative neutrix product of distributions*. Integral Transforms and Special Functions, 18(8), 559 -568, (2007).

[23] Miteva, M., Jolevska, T. B. *Some results on Colombeau product of distributions*, Adv.Math.Sci.Journal,Volume1, No.2, 121-126, (2012)

[24] Miteva, M., Jolevska, T. B., Atanasova, P. T. *On products of distributions in Colombeau algebra*, Mathematical Problems in Engineering, Volume 2014, Article ID 910510,4pages (2014)http://dx.doi.org/10.1155/2014/910510

[25] Oberguggenberger, M., Todorov, T. *An Embedding of Schwartz Distributions in the Algebra of Asymptotic Functions*. Internat. J. Hath. and Hath. Sci.Vol. 21 No.3417-428 (1998).

[26] Oberguggenberger, M. *Regularity Theory in Colombeau Algebras*. Bulletin, Classe des Sciences Mathematiques et Naturelles, Sciences mathematiques naturelles/sciences mathematiques Vol. CXXXIII, No. 31, pp. 147162 (2006).

[27] Oberguggenberger, M. *Multiplication of distributions and Applications to Partial Differential Equations*, Longman, Essex (1992). (1996).

[28] Schwartz, L. *Sur Limpossibilite de la Multiplication des Distributions* C.R. Acad.Sci.Paris 239, 847-848, (1954).

[29] Todorov, T. *Algebraic Approach to Colombeau Theory of Generalized Functions*

[30] Vickers, J. A. *Distributional geometry in general relativity*. Journal of Geometry and Physics 62, 692705 (2012).

# ПРИМЕНА НА CRANK-NICOLSON МЕТОДОТ ЗА РЕШАВАЊЕ НА ТОПЛИНСКИ РАВЕНКИ

Мирјана Коцалева[1], Владо Гичев[1]

[1] Факултет за информатика, Универзитет „Гоце Делчев“, Штип
(mirjana.kocaleva, vlado.gicev)@ugd.edu.mk

**Апстракт.** Во овој труд разгледуваме еднодимензионален (1-Д) проблем на трансфер на топлина низ прачка. Иницијално прачката е загреана по должина, а на краевите температурата се одржува на нула во тек на време. Проблемот се опишува со парцијална диференцијална равенка која ја решаваме нумерички со Crank-Nicolson методот.
Од решението може да се види како во тек на време прачката се лади при што температурата по цела должина на прачката асимптотски се приближува кон нула. Во овој труд, ние го истражувавме влијанието на дискретизацијата (sampling) на точноста на решението со Crank-Nicolson методот.

**Клучни зборови:** парцијални равенки, параболични равенки, Crank-Nicolson метод

# APPLICATION OF THE CRANK-NICOLSON METHOD FOR SOLVING HEAT EQUATIONS

Mirjana Kocaleva[1], Vlado Gicev[1]

[1]Faculty of computer science, Goce Delcev University, Stip, Macedonia
(mirjana.kocaleva, vlado.gicev)@ugd.edu.mk

**Abstract.** In this paper we consider one-dimensional (1 - D) problem of heat transfer through the rod. Initially the rod is heated longitudinally and the ends are maintained at zero temperature over time. The problem is governed by a partial differential equation which is solved numerically by Crank-Nicolson method.
From the solution it can be seen that as time elapsing the rod is cooling whereby the temperature of the rod asymptotically approaches zero. In this paper, we investigate what is the impact of sampling on the accuracy of the solution of Crank-Nicolson method.

**Kew words:** partial equations, parabolic equations, Crank-Nicolson method.

## 1. Вовед

Природните и инженерски феномени се опишуваат со диференцијални равенки. Еден мал дел од нив се опишуваат со обични, а многу поголем број со парцијални диференцијални равенки. Само за мал број парцијални диференцијални равенки со специјални иницијални и гранични услови постојат затворени, аналитички решенија. Поради непостоење на аналитички решенија, истражувањата на физичките феномени се врши со примена на математичко моделирање и нумеричка анализа. Така авторите предлагаат нумерички шеми и методи за решавање на елиптични 4,7,8,9, параболични1,4,5,6,8,9 и хиперболични2,3,8,9 парцијални диференцијални равенки.

Равенката која го опишува нашиот проблем е еднодимензионалната топлинска равенка

$u_t = c^2 u_{xx}$ (c е константа). (0)

Оваа равенка обично се користи за x во фиксни интервали $0 \le x \le L$ и време $t \ge 0$, пропишана почетна температура u(x,0) = f(x) (f е дадено) и гранични услови во x=0 и x=L за сите $t \ge 0$. Претпоставуваме дека c=1 и L=1; ова секогаш може да се оствари со линеарна трансформација на x и t. Тогаш топлинската равенка и условите се

$$u_t = u_{xx} \quad 0 < x < 1 \quad t \ge 0 \tag{1}$$

во внатрешноста на доменот

$$u(x,0) = f(x) \tag{2}$$
$$u(0,t) = u(1,t)=0 \tag{3}$$

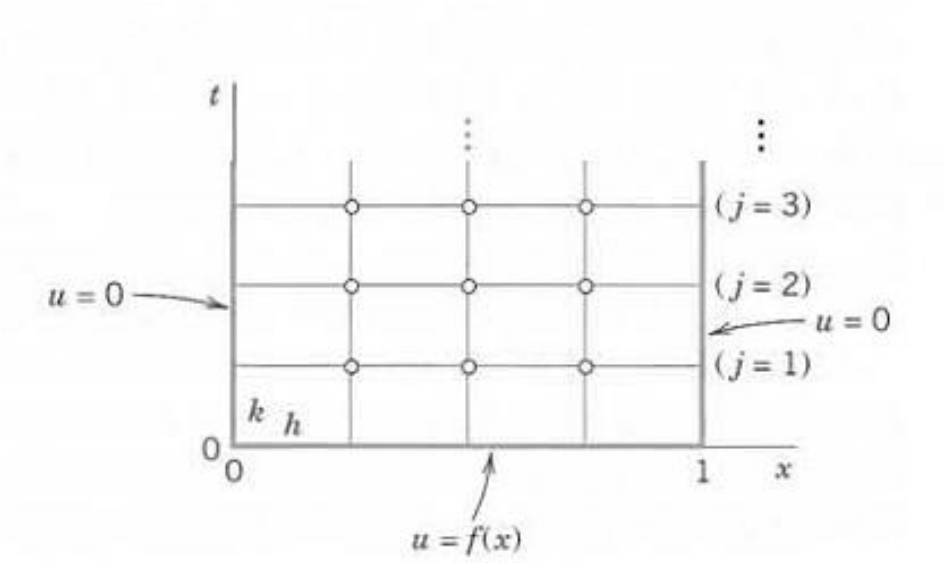
каде (2) се почетни услови, а (3) се гранични услови.
Апроксимацијата на (1) со конечни разлики е

$$\frac{1}{k}(u_{i,j+1} - u_{ij}) = \frac{1}{h^2}(u_{i+1,j} - 2u_{ij} + u_{i-1,j}) \quad (4)$$

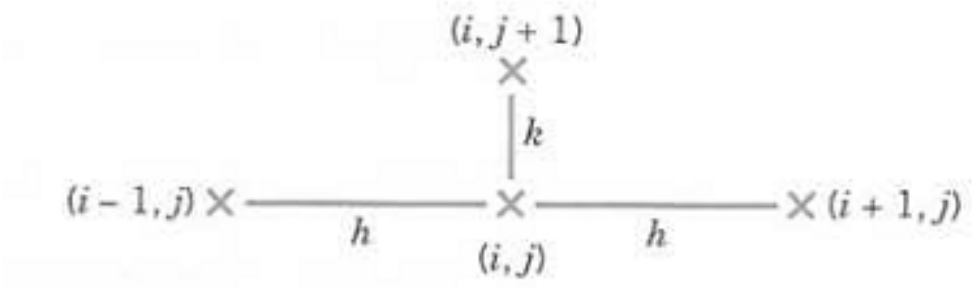
Слика 1 ја покажува соодветната мрежа и мрежните точки. Просторните инкременти се h во x-правец и k во t-правец. Формулата (4) ги вклучува четирите точки прикажани на слика 2. На лево користиме конечна разлика напред бидејќи немаме информација за негативно x на почетокот. Од (4) го пресметуваме $u_{i,j+1}$ кој одговара на временскиот ред j+1, во однос на другите три кои одговараат на временскиот ред j; решавајќи го (4) за $u_{i,j+1}$ добиваме

$$u_{i,j+1} = (1 - 2r)u_{ij} + r(u_{i+1,j} + u_{i-1,j}) \quad (5)$$

каде $r = \frac{k}{h^2}$.




**Слика 1 Мрежа и мрежни точки кои одговараат на равенките (4) и (5)**
Figure 1 Network and networked points corresponding to equations (4) and (5)




**Слика 2 Четирите точки во равенките (4) и (5)**
Figure 2 The four points in equations (4) and (5)

Пресметките со овој експлицитен метод базирани на (5) се едноставни. Сепак, може да се покаже дека клучно за конвергенција на овој метод е условот

$$r = \frac{k}{h^2} \leq \frac{1}{2}, r = \frac{1}{2}, \quad (6)$$

тоа е бидејќи $u_{ij}$ има позитивен коефициент во (5) или (за $r = \frac{1}{2}$) ќе биде отсутен од (5). Интуитивно (6) значи дека не треба да одиме брзо во t-насоката. Пример е даден подолу.

### 1.1. Crank-Nicolson метод

Условот (6) не е многу ефикасен во пракса. Всушност, за да се постигне доволна точност, треба да се избере h мало, што го прави и k многу мало од (6). Ако h=0.1 тогаш k≤0.005. Префрлањето на 1/2 h четирикратно го зголемува бројот на временски чекори потребни за да се постигне одредена t-вредност.

Метод кој не наметнува ограничувања на $r = \frac{k}{h^2}$ е Crank-Nicolson методот [1] кој користи вредности на u во шест точки на слика 3. Идејата на методот е замена на разликата количник на десната странана (4) со $\frac{1}{2}$ пати од збирот на двата различни количници во двата временски реда. Наместо (4) имаме

$$\frac{1}{k}\left(u_{i,j+1} - u_{ij}\right) = \frac{1}{2h^2}\left(u_{i+1,j} - 2u_{ij} + u_{i-1,j}\right) + \frac{1}{2h^2}\left(u_{i+1,j+1} - 2u_{i,j+1} + u_{i-1,j+1}\right) \quad (7)$$

Со множење со 2k и запишување на $r = \frac{k}{h^2}$, ги собираме условите кои одговараат на временскиот ред j+1 од лево и условите кои одговараат на временскиот ред j од десно:

$$(2 + 2r)u_{i,j+1} - r\left(u_{i+1,j+1} + u_{i-1,j+1}\right) = (2 - 2r)u_{ij} + r\left(u_{i+1,j} + u_{i-1,j}\right). \quad (8)$$

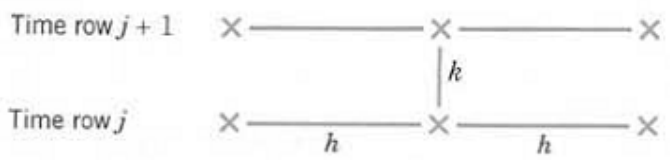
Генерално, трите вредности на лево се непознати, додека трите вредности на десно се познати.

Ако го поделиме x-интервалот 0<x<1 во (1) на n еднакви интервали, имаме n-1 внатрешни мрежни точки за временски ред. Тогаш за j=0 и i=1,.., n-1, формулата (8) дава линеарен систем од n-1 равенки за n-1 непознати вредности $u_{11}$, $u_{21}$,.., $u_{n-1,1}$ во првиот временски ред во однос на првичните вредности u00,u10,..,un0 и граничните вредности $u_{01}$,$u_{n1}$(=0).

Слично за j=1, j=2... односно за секој временски ред треба да решиме систем од n-1 линеарни равенки кои произлегуваат од (8).

Иако $r = \frac{k}{h^2}$ не наметнува ограничувања, помал r ќе дава подобар резултат. Во пракса, се избира k со која може да се зачува значителна сума на работа, без правење на r многу големо. Често добар избор за r е r=1. Тогаш (8) станува поедноставен.

$$4u_{i,j+1} - u_{i+1,j+1} - u_{i-1,j+1} = u_{i+1,j} + u_{i-1,j} \quad (9)$$



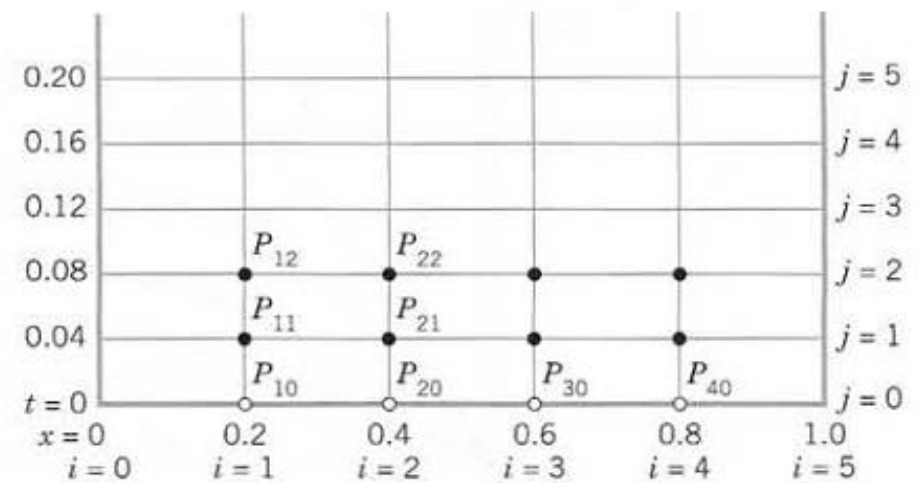

**Слика 3 Шесте точки во Crank-Nicolson формулите (7) и (8)**
Figure 3. Six points in the Crank-Nicolson formula (7) and (8)

## 2. Математички модел

Разгледуваме странично изолирана метална шипка со должина 1 и таква што $c^2$=1во топлинската равенка (0). Претпоставуваме дека краевите на шипката се чуваат на температура $u=0^0$C и дека температурата на шипката во одреден момент t=0 е f(x) = sinπx [1]. Се применува Crank-Nicolson методот со h=0.2 и r=1. Ја наоѓаме температурата u(x,t) во шипката за време t во интервал $0 \le t \le 0.2$.

Исто така треба да се примени методот т.е. равенката (5) со r кој го задоволува условот од равенката (6) т.е. r=0.25 и со незадоволителни вредности (6) r=1 и r=2.5.

Овој пример ќе биде решен и со експлицитниот метод за да се направи споредба на двете добиени решенија.




**Слика 4 Мрежата на нашиот проблем**
Figure 4 Network of our problem

Бидејќи r=1, формулата (8) ја добива формата (9). Бидејќи h=0.2 и $r = \frac{k}{h^2}$=1, тогаш,

к=$h^2$=0.04.

Оттука треба да решиме пет чекора. Потребни ни се почетни вредности. Нив ги добиваме со решавање на равенката f(x) = sin πx и имаме

$u_{10}=0.587785=u_{40}$ и
$u_{20}=0.951057=u_{30}$

($u_{10}$ значи u во $P_{10}$ на слика 4). Во секој временски ред има 4 внатрешни мрежни точки. Оттука во секој временски чекор ќе имаме да решиме четири равенки со четири непознати. Но бидејќи почетната температура има симетрична дистрибуција со однос x=0.5 и u=0 на двата краја за сите t, имаме $u_{31}=u_{21}$, $u_{41}=u_{11}$ во првиот временски ред и соодветно за другите редови. Ова го намалува секој систем до две равенки со две непознати. Од (9), бидејќи $u_{31}=u_{21}$ и $u_{01}=0$, за j=0 овие равенки се

(i=1)$4u_{11} - u_{21} = u_{00} + u_{20} = 0.951\,057$
(i=2)$-u_{11} + 4u_{21} - u_{21} = u_{10} + u_{20} = 1.538\,842$

Решението е $u_{11}$=0.399 274, $u_{21}$=0.646 039. Слично за j=1 го имаме системот

$4u_{12} - u_{22} = u_{01} + u_{21} = 0.646\,039$ за i = 1
$-u_{21} + 3u_{22} = u_{11} + u_{21} = 1.045\,313$ за i = 2

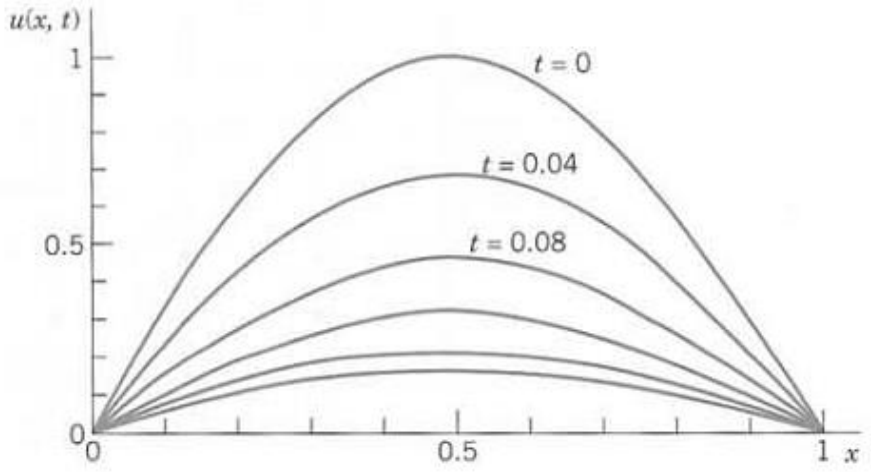
Решението е $u_{12}$=0.271 221, $u_{22}$=0.438 844 и.т.н.

На слика 5 се прикажани сите решенија на овој проблем,

| $t$ | $x = 0$ | $x = 0.2$ | $x = 0.4$ | $x = 0.6$ | $x = 0.8$ | $x = 1$ |
|---|---|---|---|---|---|---|
| 0.00 | 0 | 0.588 | 0.951 | 0.951 | 0.588 | 0 |
| 0.04 | 0 | 0.399 | 0.646 | 0.646 | 0.399 | 0 |
| 0.08 | 0 | 0.271 | 0.439 | 0.439 | 0.271 | 0 |
| 0.12 | 0 | 0.184 | 0.298 | 0.298 | 0.184 | 0 |
| 0.16 | 0 | 0.125 | 0.202 | 0.202 | 0.125 | 0 |
| 0.20 | 0 | 0.085 | 0.138 | 0.138 | 0.085 | 0 |

**Слика 5 Сите решенија на проблемот**
Figure 5 All the solutions of the problem

додека пак на слика 6 е прикажана температурната распределба $u(x,t)$ каде времето t е дадено во вид на параметар. Температурната распределба по должина на прачката е прикажана во временски инстанци t = 0; 0.04s; 0.08s; 0.12s; 0.16s; 0.20s




**Слика 6 Температурна распределба по должина на прачката**
Figure 6 Temperature distribution along the rod

**2.1. Решение на проблемот со експлицитниот метод (5) со r=0.25**

Од h=0.2 и $r = \frac{k}{h^2}$=0.25 за к имаме к=rh²=0.25*0.04=0.01. Оттука треба да извршиме 4 пати повеќе чекори отколку со Crank-Nicolson методот. Формула (5) со r=0.25 е

$$u_{i,j+1} = 0.25(u_{i-1,j} + 2u_{ij} + u_{i+1,j}) \qquad (10)$$

И овде можеме да користиме симетрија. За j=0 ни требаат $u_{00}$=0,$u_{10}$=0.587 785, $u_{20}$=$u_{30}$=0.951 057 и пресметуваме

$u_{11} = 0.25(u_{00} + 2u_{10} + u_{20}) = 0.531\ 657$
$u_{21} = 0.25(u_{10} + 2u_{20} + u_{30}) = 0.25(u_{10} + 3u_{20}) = 0.860\ 239$

Секако можеме да ги изоставиме граничните услови $u_{01}$=0,$u_{02}$=0,.. од формулата. За j=1 имаме

$u_{12} = 0.25(2u_{11} + u_{21}) = 0.480\ 888$
$u_{22} = 0.25(u_{11} + 3u_{21}) = 0.778\ 049$ и т.н.

Треба да извршиме 20 чекори, но нумеричките вредности покажуваат дека точноста е иста со Crank-Nicolson вредностите CN (точните вредности се дадени со три децимали):

| $t$ | $x = 0.2$ | | | $x = 0.4$ | | |
|---|---|---|---|---|---|---|
| | CN | By (11) | Exact | CN | By (11) | Exact |
| 0.04 | 0.399 | 0.393 | 0.396 | 0.646 | 0.637 | 0.641 |
| 0.08 | 0.271 | 0.263 | 0.267 | 0.439 | 0.426 | 0.432 |
| 0.12 | 0.184 | 0.176 | 0.180 | 0.298 | 0.285 | 0.291 |
| 0.16 | 0.125 | 0.118 | 0.121 | 0.202 | 0.191 | 0.196 |
| 0.20 | 0.085 | 0.079 | 0.082 | 0.138 | 0.128 | 0.132 |

**Слика 7 Табела со точни вредности**
Figure 7 Table with the correct values

### 2.2. Неуспех на равенката на Crank-Nicolson методот т.е. на равенката (5) поради нарушени вредности на r (равенка (6))

Формулата (5) $u_{i,j+1} = (1-2r)u_{ij} + r\left(u_{i+1,j} + u_{i-1,j}\right)$ со h=0.2 и r=1 што ја нарушува (6) е

$$u_{i,j+1} = u_{i-1,j} - u_{ij} + u_{i+1,j}$$

и дава многу мали вредности:

| $t$ | $x = 0.2$ | Exact | $x = 0.4$ | Exact |
|---|---|---|---|---|
| 0.04 | 0.363 | 0.396 | 0.588 | 0.641 |
| 0.12 | 0.139 | 0.180 | 0.225 | 0.291 |
| 0.20 | 0.053 | 0.082 | 0.086 | 0.132 |

**Слика 8 Формула (5) дава мали вредности**
Figure 8 Formula (5) gives small values

Додека пак формулата (5) со големи вредности за r, на пример за r=2.5, дава комплетно бесмислен резултат.

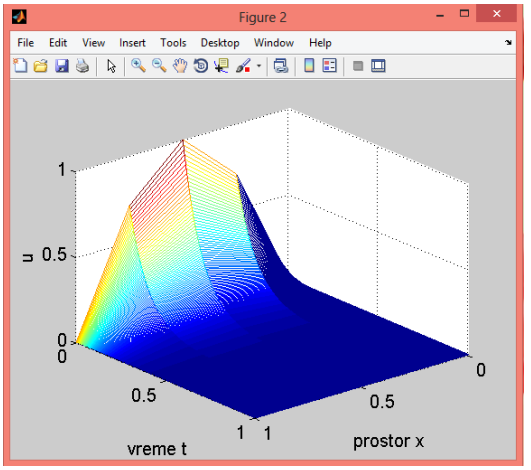
| $t$ | $x = 0.2$ | Exact | $x = 0.4$ | Exact |
|---|---|---|---|---|
| 0.1 | 0.0265 | 0.2191 | 0.0429 | 0.3545 |
| 0.3 | 0.0001 | 0.0304 | 0.0001 | 0.0492. |

**Слика 9 Формула (5) дава бесмислен резултат**
Figure 9 Formula (5) gives senseless result

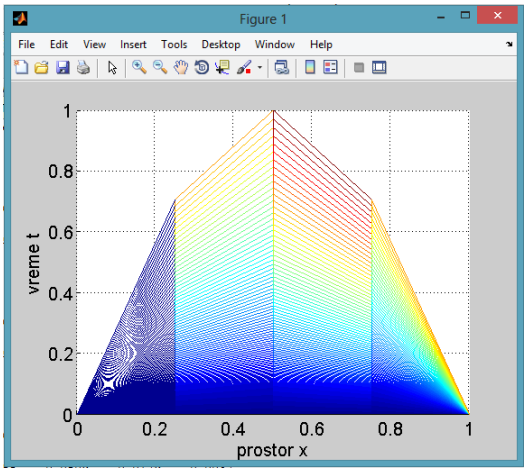
### 2.3. Приказ на проблемот со користење на Matlab

Со помош на Matlab со примена на Crank-Nicolson методот ги добиваме следниве решенија за различен број на интервали.

- Ова е претстава на Crank-Nicolson методот во случај кога имаме четири просторни интервали. На цртежите е прикажана зависноста на просторот x од времето t со помош на три-димензионален и дво-димензионален приказ. Забележуваме дека параболата нема правилен изглед.

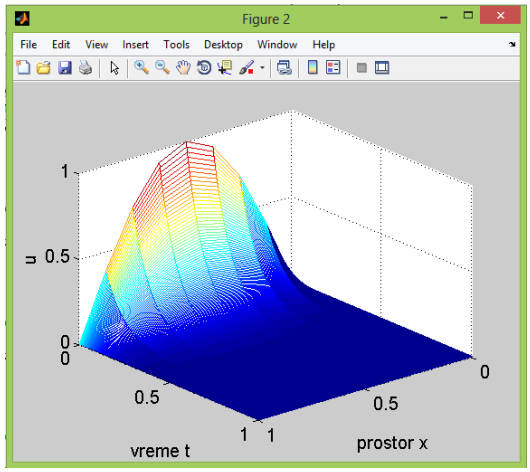



**Цртеж 1Три-димензионален приказ со 4 интервала**
Drawing 1 Three Dimensional display with 4 interval

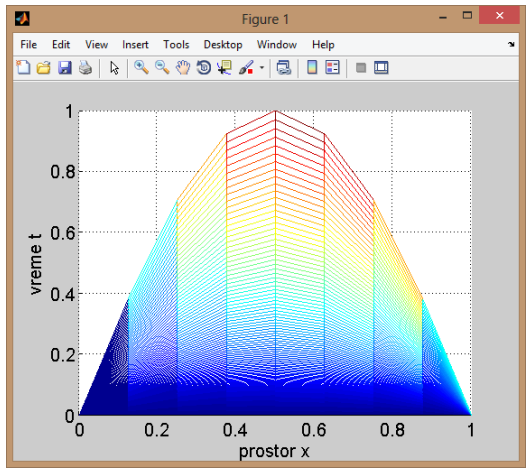



**Цртеж 2Дво-димензионален приказ со 4 интервала**
Drawing 2 Two-dimensional display with 4 interval

- Ова е претстава на Crank-Nicolson методот во случај кога имаме осум просторни интервали. На цртежите е прикажана зависноста на просторот x од времето t со помош на три-димензионален и дво-димензионален приказ. Забележуваме дека параболата има подобар изглед, отколку параболата претставена со четири интервали.

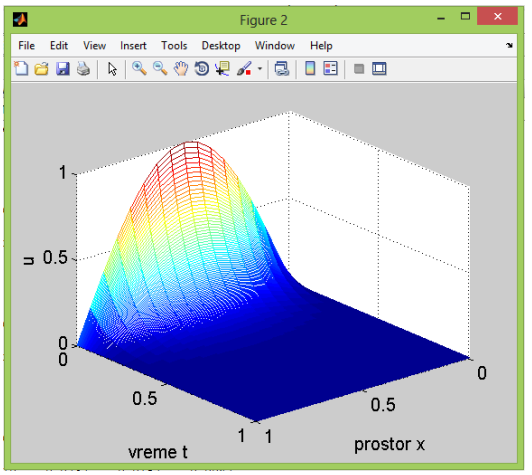



**Цртеж 3 Три-димензионален приказ со 8 интервала**
Drawing 3 Three Dimensional display with 8 interval

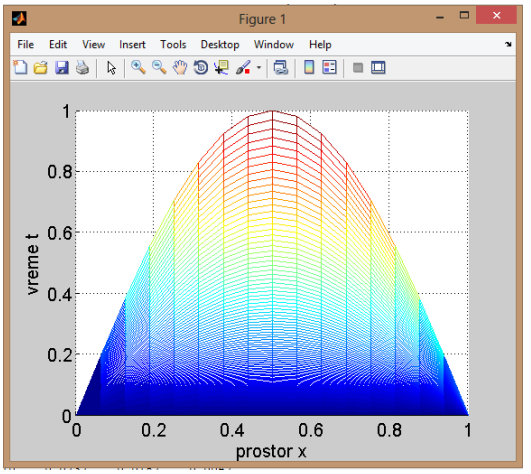



**Цртеж 4 Дво-димензионален приказ со 8 интервала**
Drawing 4 Two-dimensional display with 8 interval

- Како последна е претставата на Crank-Nicolson методот во случај кога имаме шеснаесет просторни интервали. На цртежите е прикажана зависноста на просторот x од времето t со помош на три-димензионален и дво-димензионален приказ. Забележуваме дека параболата има совршен изглед, за разлика од параболите претставени со четири и осум интервали.




**Цртеж 5 Три-димензионален приказ со 16 интервала**
Drawing 5 Three Dimensional display with 16 interval



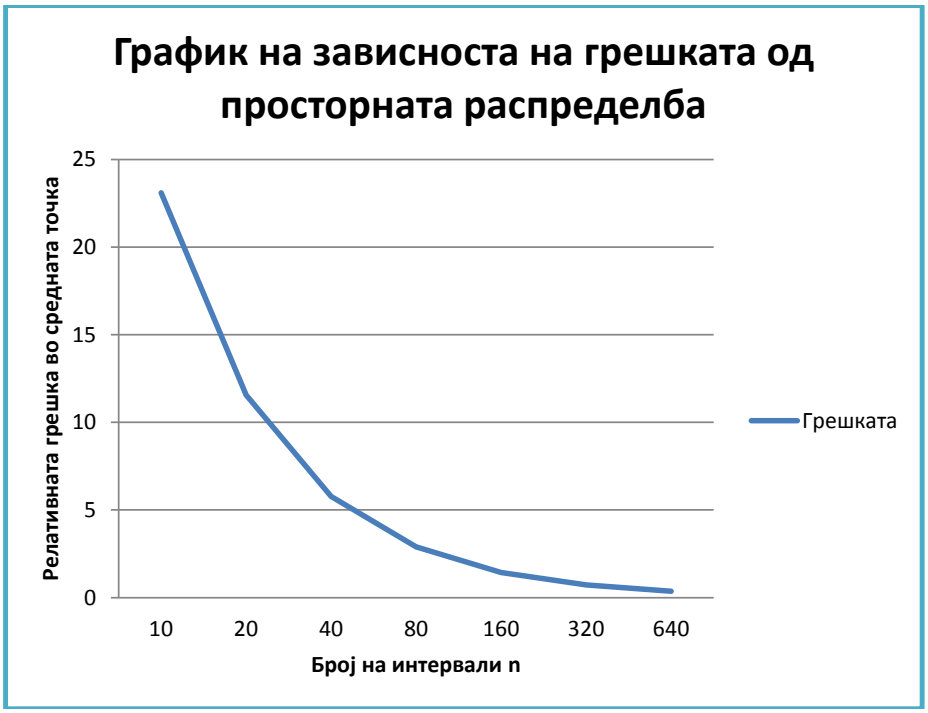

**Цртеж 6 Дво-димензионален приказ со 16 интервала**
Drawing 6 Two-dimensional display with 16 interval

## 3. Заклучок

Од приказот на Crank-Nicolson методот со помош на програмскиот јазик Matlab т.е. од претходните 6 цртежи доаѓаме до следниов заклучокот: за поголем број на интервали параболата се исцртува подобро и има подобар изглед, исто така со зголемување на бројот на интервали се намалуваат релативната и апсолутната грешка.

За да ја оцениме грешката во зависност од дискретизацијата, почнуваме со груба дискретизација (на пр. 10 интервали, 11 просторни точки). Во првата и крајната точка според граничните услови, температурата е постојано 0. Точките од 2 до 9 имаат x координати од 0.1 до 0.9. За овие вредности на x го добиваме точното (аналитичко) решение во временскиот момент t=0.2 или t=2 секунди. Точното решение го пресметуваме со формулата $u(x,t) = \frac{8}{\pi^2} * \sum_{n=1}^{\infty} \frac{1}{n^2} * sin\frac{n\pi}{2} * \sin(\pi x n) * e^{-\pi^2 n^2 t}$.

На крајот на анализата, за t = 2 sec, од точното решение по Crank Nicolson го вадиме нумеричкото решение, делиме со точното решение и множиме со 100 и на тој начин ја добиваме релативната грешка во средишната точка изразена во проценти.




**Цртеж 7 Зависноста на грешката од просторната распределба за различен број на интервали**
Drawing 7 The dependence of the error by the space distribution for different number of intervals

Ова го правиме за секоја дискретизација.

На цртежот 7 е претставена зависноста на грешката од бројот на интервали. Всушност од цртежот гледаме дека грешката зависи од бројот на интервали, т.е. со зголемување на бројот на интервали (постепено од 10, на 20, па на 160...) грешката постепено се намалува, а тоа е резултат на тоа што со текот на времето загреаната прачка се лади при што температурата по целата должина на прачката асимптотски се приближува кон нула. Преку овој цртеж го прикажавме влијанието на дискретизацијата на точноста на решението со Crank-Nicolson методот

## 4. Литература:

[1] Chupa, M.A. Numerical Techniques for Solving the One-Dimensional Heat Equation Numerical Analysis 2, 1998.

[2] Gicev, V. and Trifunac, M.D. Non-linear earthquake waves in seven-storey reinforced concrete hotel,
NISEE, Pacific Earthquake Engineering (PEER) Center, Univ. of California, Berkeley, 2006.

[3] Gicev, V. and Trifunac, M.D. Amplification of linear strain in a layer excited by a shear-wave earthquake pulse, *Soil Dynamics and Earthquake Engineering,* vol. 30, issue 10, 2010, 1073-1081.

[4] Giordano, N.J. and Nakanishi, H. Computational Physics, 2nd edition “Implicit Methods: the Crank Nicolson Algorithm”, 2005.

[5] Kreyszig, E. “Advanced Engineering Mathematics”, 8th edition, 1999

[6] Li, J-R., and Greengard, L. On the numerical solution of the heat equation I:
Fast solvers in free space, Journal of Computational Physics 226, 2007, 1891-1901

[7] McKenney, A., Greengard, L., and Mayo, A. A fast Poisson Solver for Complex Geometries, Journal
of Computational Physics 118, 1995, 348-355

[8] Proskurowski, W. Lectures on CE504 “Numerical Solution of PDE”, Univ. of Southern California, 2001

[9] Smith G.D., Numerical Solution of Partial Differential Equations, 3rd Edition, Oxford Univ. Press, 1986.

# S-BOXES – PARAMETERS, CHARACTERISTICS AND CLASSIFICATIONS

**Dusan Bikov[1], Stefka Bouyuklieva[2] and Aleksandra Stojanova[3]**

[1] "Goce Delcev" University – Stip
(dusan.bikov, aleksandra.stojanova)@ugd.edu.mk
[2] "St.Cyril and St.Methoduis University" of Veliko Tarnovo
(stefka_iliya)@yahoo.com

**Abstract.** S-Boxes are key building blocks in the design of the block ciphers. They are basically used to hide the relationship between the plain text and the cipher text.
In this paper we study the parameters of Boolean functions and S-boxes, which are important in the design of good cryptosystems. We give a brief overview of the selection criteria on S-boxes, which can be resistant to different type of cryptanalytic attacks. For this goal optimality of S-box is defined. We present different variants for classification of S-boxes and give some examples. Also we list the results of our computer calculations for the parameters of Boolean functions and S-boxes that are essential in the cryptographic research. Finally, we give general framework of the direction in which our study is focused.

**Keywords:** Boolean function, Differential cryptanalysis, Linear cryptanalysis, Affine equivalence.

## 1 Introduction

In his paper "Communication Theory of Secrecy Systems" from 1949, Claude Shannon introduced some design principles for ciphers [1]. He proposed *confusion* and *diffusion* in the encryption algorithms. Cryptosystems are still designed according to these principles. The key elements in almost all block ciphers are the substitution boxes (S-boxes), which are used to ensure the confusion [1] of the information.

S-boxes form the non-linear part of a block cipher and therefore they are very important for the security of these ciphers. S-boxes have to be chosen carefully, in order to make the cipher resistant against different attacks. Thus, the generation and classification of small S-boxes with good linear and differential properties is very helpful. The S-box is a function S with values that are bit strings, or

$$S: F_2^n \to F_2^m$$

In many cases it is represented by a table. For any vector $v \in F_2^m$ a component function $S_b: F_2^n \to F_2$ is defined by $S_b(x) = b \cdot S(x)$. As $S_b$ are Boolean functions, some their parameters and properties are very important in the design of S-boxes.

We take into account the following parameters of an S-box:

- Difference distribution table.
- Differential Uniformity (Diff(S) or Δ(S)).
- Linear approximation table.
- Linearity, linear probability and linear probability bias.
- Branch number.

We give some examples for 4×4, and greater S-boxes and present some classification results in the 4×4 case.

We can generate good S-boxes with two primary ways: (1) picking a random large S-box or (2) generating small S-boxes with good linear and differential properties. The main drawback of picking a random large S-box, is that these S-boxes are much more inefficient to implement, especially in hardware [2].

It is difficult to find an optimal S-box, because of a huge number of permutations for small values of n-bits S-box. For example, the number of 4-bit permutations is still huge: roughly $2^{44}$. Because of this, after exhaustively checking all, finding good S-box, is no option. Resistance of S-box against most attacks remains unchanged, when invertible affine transformation before and after the S-box is applied. This reduction allows us to check all optimal S-boxes thoroughly, with consideration to the other criteria, such as algebraic degree.

### 1.1 Overview of this paper

In section 2, we give s-box properties notation. In section 3, we find parameters for example 4-bit S-box, and we show results for testing S-boxes with different size. In section 4, we define optimal criteria. In section 5, we suggest further ideas to be investigated. We conclude in section 6.

**2. S-Box Properties - Notation**

Let $F_2 = \{0,1\}$ be a finite field with two elements and $F_2^n$ be the n-dimensional vector space over $F_2$. A Boolean function in *n* variables is a function $f: F_2^n \to F_2$ which maps any binary vector of length *n* (n-tuple or *n* bit input) to 0 or 1. A common way of representing a Boolean function is by supplying a list of output values for each n-bit input vector, called the truth table of the function. Actually this is a vector consisting of all the outputs which we obtain for the lexicographically ordered inputs:

$$f \mapsto v_f = (v_0, v_1, \dots, v_{2^n-1}) \in F_2^{2^n},$$

where $v_i = f(\bar{\imath}), \bar{\imath}$ is the binary representation of the integer *i*. The number of all Boolean functions in n variables is $2^{2^n}$.

Every Boolean function can be written as a polynomial:

$$f(x_1, x_2, \dots, x_n) = \sum_u c_u x^u, \qquad (1)$$

where $c_u \in F_2, x^u = x_1^{u_1} x_2^{u_2} \dots x_n^{u_n}, u = (u_1, u_2, \dots, u_n) \in F_2^n$. This presentation is called Algebraic Normal Form (ANF) of the function. The degree of the polynomial (1) is the algebraic degree of *f* (deg f). Obviously, the maximum degree of a Boolean function in *n* variables is *n*.

A Boolean function with algebraic degree at most 1 is called affine, so the function *f* is affine Boolean function if

$$f(x_1, \dots, x_n) = a_0 + a_1 x_1 + \dots + a_n x_n = a \cdot x + a_0,$$

where $a \in F_2^n, a_0 \in F_2$. If $a_0 = 0$, the affine function is called linear.

Nonlinearity nl (f) of the Boolean function f is the minimal Hamming distance from f to the affine functions:

$$nl(f) = \min\{d(f, g) \mid g - affine\ function\}$$

The nonlinearity is at most $2^{n-1} - 2^{n/2-1}$ [7]. For cryptographic Boolean functions, *nl (f)* must be close to this maximum to prevent the system from attacks by linear approximations, correlation attacks, fast correlation attacks etc. [8].

A Boolean function *f* on $F_2^n$ is also uniquely determined by its Walsh transform. The Walsh transform $f^W$ of $f$ is an integer valued function defined by

$$f^W(a) = \sum_{x \in F_2^n} (-1)^{f(x)+\langle a,x \rangle} = 2^n - 2d_H(f, f_a)$$

where $\langle a, x \rangle$ is scalar product.

Linearity *Lin (f)* of the Boolean function *f* is defined by using Walsh transform

$$Lin(f) = \max_{a \in F_2^n} |f^W(a)| \geq 2^{n/2}.$$

Linearity and nonlinearity of a Boolean function are connected by the equality

$$nl(f) = 2^{n-1} - \frac{1}{2} Lin(f).$$

From mathematical point of view S-box (or vectorial Boolean function) is a function S, with values that are bit string, or mapping of n bits to m bits

$$S: F_2^n \to F_2^m.$$

For any vector $b = (b_1, b_2, \dots b_m) \in F_2^m$ we consider the corresponding component function $S_b: F_2^n \to F_2$ defined by

$$S_b(x) = \langle b, S(x) \rangle = b_1 S_1(x) + \dots + b_m S_m(x).$$

**2.1 Linear cryptanalysis (LC)**

Linearity is a measure for resistance against linear cryptanalysis [3]. We define linearity of S as

$$Lin(S) = \max_{a \in F_2^n, b \in F_2^m, b \neq 0} |S_b^W(a)| = \max_{b \in F_2^m, b \neq 0} Lin(S_b)$$

In the theory of block ciphers related to linear cryptanalysis, the linear approximation table is studied. The linear approximation table is a $2^n \times 2^m$ table whose entries are defined as

$$L_{a,b} = \#\{x \in F_2^n : \langle b, S(x) \rangle = \langle a, x \rangle\} = 2^n - d_H(S_b, f_a)$$

The probability of a linear approximation of a linear combination of output bits $S_b$ by a linear combination of input bits we define as

$$p_{a,b} = \frac{1}{2^n} L_{a,b}.$$

Linear probability bias ε is a correlation measure for this deviation from the probability ½ for which it is entirely uncorrelated:

$$\varepsilon_{a,b} = \left| p_{a,b} - \frac{1}{2} \right| \leq \left| \frac{Lin(S)}{2^{n+1}} \right|$$

The smaller is the linearity more resistant is the S-box against linear cryptanalysis. An open problem for given integers and m is to find nxm S-boxes with the smallest linearity.

**2.2 Differential cryptanalysis (DC)**

Differential cryptanalysis is proposed by Biham and Shamir [4], and is basically applied to block ciphers. This attack keeps up with the differences in the propagation during the encryption of the messages *m* and *m+δ* through the different rounds in a block cipher. Here a difference distribution table DDT is defined as

$$D_{a,b} = \#\{x \in F_2^n : S(x) \oplus S(x \oplus a) = b\}.$$

Similarly to the linear case, a differential probability is defined as

$$DP_{a,b} = \frac{1}{2^n} D_{a,b}.$$

To measure the resistance against differential cryptanalysis we take the highest possible value in DDT called differential uniformity

$$Diff(S) = max\{D_{a,b}, a \in F_2^n, a \neq 0, b \in F_2^m\}.$$

Diff(S) is related to the maximal probability that any fixed nonzero input difference causes any fixed output difference after applying the S-box.

**2.3 Branch number**

An important parameter describing the diffusion capabilities is the branch number. Branch number [5] is defined as

$$BN(S) = \min_{a,b \in F_2^n, a \neq b} (w_H(a \oplus b) + w_H(S(a) \oplus S(b)))$$

where $w_H$ is the Hamming weight and S the S-box.

The branch number here depends on the position of the values in the difference distribution table. For bijective S-boxes BN ≥2. Branch number is related to the avalanche property [9] of the S-box and should be as greater as possible. In [6] differential branch number and linear branch number are defined.

**3. Finding S-boxes parameters**

Here we calculate some parameters of the 4-bit S-box $G_3$, which is one of the 16 different optimal S-boxes classified in [2]. We present $G_3$ by the following table:

**Table 1. S-box $G_3$**

| a | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S(a) | 0 | 1 | 2 | 13 | 4 | 7 | 15 | 6 | 8 | 12 | 5 | 3 | 10 | 14 | 11 | 9 |

It can be represented also as a permutation, in this case this is the 16-tuple with values from the second row of Table 1: (0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 5, 3, 10, 14, 11, 9), so

$G_3$: (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) → (0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 5, 3, 10, 14, 11, 9).

Replacing every number by its binary 4-bit string, we obtain

$$(0,1,2,13,4,7,15,6,8,12,5,3,10,14,11,9) \rightarrow \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

To calculate the linearity Lin(S) of S, we use the first order Reed-Muller code RM (1, 4). The set of all binary vectors (true tables) corresponding to the affine Boolean functions in n variables, coincides with the first order Reed-Muller code RM (1, n). It is a linear code of length $2^n$, dimension n+1 and minimum distance $2^{n-1}$.

RM (1, 4) has a generator matrix:

$$G(RM(1,4)) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

For the linearity of $G_3$ we have $nl(S_b) = d(S_b, RM(1,4))$

$$\Rightarrow Lin(S_b) = 2^4 - 2nl(S_b) = 16 - 2d(S_b, RM(1,4))$$

$$Lin(S) = \max Lin(S_b) = 8$$

For the 4-bit S-box $G_3$ we calculate Linear Approximation Table (see Table 2). To do that, we wrote the program S-box_LATv0.2 in C++ programming language. The results from the calculations are saved in a text file.

**Table 2. LAT for $G_3$**

| a\x | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0001 | 0 | 4 | 0 | 4 | 4 | 8 | -4 | 0 | 0 | 4 | 8 | -4 | -4 | 0 | -4 | 0 |
| 0010 | 0 | 8 | 4 | 4 | 0 | 0 | 4 | -4 | 0 | -8 | 4 | 4 | 0 | 0 | 4 | -4 |
| 0011 | 0 | 4 | 4 | 0 | 4 | 0 | 0 | 4 | 0 | 4 | -4 | 8 | -4 | -8 | 0 | 4 |
| 0100 | 0 | 0 | 8 | 0 | 4 | 4 | -4 | 4 | 4 | -4 | -4 | -4 | 8 | 0 | 0 | 0 |
| 0101 | 0 | 4 | 0 | -4 | 0 | 4 | 8 | 4 | 4 | 0 | -4 | 0 | -4 | 8 | -4 | 0 |
| 0110 | 0 | 0 | 4 | 4 | 4 | -4 | 8 | 0 | -4 | 4 | 0 | -8 | 0 | 0 | 4 | 4 |
| 0111 | 0 | -4 | -4 | 8 | 0 | 4 | 4 | 8 | -4 | 0 | 0 | 4 | 4 | 0 | 0 | -4 |
| 1000 | 0 | 0 | 0 | 0 | -4 | 4 | 4 | -4 | 8 | 8 | 0 | 0 | 4 | -4 | 4 | -4 |
| 1001 | 0 | 4 | 0 | 4 | 0 | -4 | 0 | -4 | 0 | 4 | 0 | 4 | 8 | 4 | -8 | 4 |
| 1010 | 0 | -8 | 4 | 4 | 4 | -4 | 0 | 0 | 8 | 0 | 4 | 4 | -4 | 4 | 0 | 0 |
| 1011 | 0 | 4 | 4 | 0 | -8 | -4 | -4 | 8 | 0 | 4 | 4 | 0 | 0 | 4 | 4 | 0 |
| 1100 | 0 | 0 | 0 | -8 | 8 | 0 | 0 | 0 | -4 | 4 | 4 | 4 | 4 | 4 | 4 | -4 |
| 1101 | 0 | 4 | -8 | 4 | 4 | 0 | -4 | 0 | 4 | 0 | -4 | 0 | 0 | 4 | 8 | 4 |
| 1110 | 0 | 0 | -4 | -4 | 0 | 0 | 4 | 4 | 4 | -4 | 8 | 0 | 4 | -4 | 0 | 8 |
| 1111 | 0 | -4 | 4 | 0 | -4 | 8 | 0 | -4 | -4 | 0 | 0 | 4 | 0 | 4 | 4 | 8 |

Moreover, we wrote the program S-box_DDTv0.3 in C++ to calculate DDT (Difference Distribution Table) for the same 4-bit S-box $G_3$ (see Table 3). The results from the calculations are saved in a text file.

**Table 3. DDT for $G_3$**

| a\x | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 | 16 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| 0001 | - | 2 | 2 | 2 | 4 | - | 2 | - | - | 2 | - | - | - | - | - | 2 |
| 0010 | - | 4 | 2 | - | - | - | - | 2 | - | - | - | 2 | 2 | 2 | - | 2 |
| 0011 | - | - | 2 | 4 | - | 2 | - | - | 2 | 2 | - | 2 | - | 2 | - | - |
| 0100 | - | - | 2 | - | 2 | 2 | 4 | 2 | 2 | - | - | - | 2 | - | - | - |
| 0101 | - | - | 2 | - | 2 | 2 | 4 | 2 | 2 | - | - | - | 2 | - | - | - |
| 0110 | - | - | - | 2 | - | 2 | 2 | 2 | - | - | 2 | - | - | 2 | - | 4 |
| 0111 | - | 2 | - | - | - | 2 | 2 | 2 | - | 4 | - | 2 | - | - | 2 | - |
| 1000 | - | - | - | - | 2 | - | - | 2 | 2 | 2 | - | - |  | 2 | 4 | 2 |
| 1001 | - | 2 | - | - | - | - | 2 | - | 2 | 2 | 2 | - | 2 | 4 | - | - |
| 1010 | - | 2 | 2 | - | - | 4 | - | - | 2 | - | 2 | - | - | - | 2 | 2 |
| 1011 | - | 2 | - | 2 | 2 | 2 | - | - | - | - | - | - | 4 | 2 | 2 | - |
| 1100 | - | - | - | - | 2 | 2 | - | - | - | 2 | 4 | 2 | 2 | - | - | 2 |
| 1101 | - | - | - | 2 | - | - | 2 | - | 2 | - | - | - | 4 | 2 | 2 | 2 |
| 1110 | - | 2 | - | 2 | 2 | - | - | 2 | 4 | - | 2 | 2 | - | - | - | - |
| 1111 | - | - | 2 | 2 | - | - | - | 4 | - | 2 | 2 | - | 2 | - | 2 | - |

Using the program S-box_DDTv0.3, we also calculated

$$Diff(S) = \max_{a \neq 0,\ b} D_{a,b} = 4;\ \ DP_{a,b} = \frac{D_{a,b}}{2^n} = 0, \frac{1}{4}\ or\ \frac{1}{8};\ \ BN = 2.$$

The mentioned program can be used to calculate the numbers in DDT, and the parameters, connected with this table, for bijective S-boxes with different lengths. We test the program for a resource computer consummation for S-boxes of different sizes (see Table 4). To generate the considered S-boxes, we use the program Generate S-box (written in C++).

**Table 4. Calculations for DDT in different S-boxes (S-box_DDTv0.3)**

| **Platform** | **Intel(R) Core(TM)2 Duo CPU E8300 @2.83 GHz, 2 GB RAM (VS2013, C/C++)** | | |
|---|---|---|---|
| **S-box** | Running Time: | RAM: | Size of the text file with the results: |
| 4x4-bit | 0.002 sec | … | 3 KB |
| 6x6-bit | 0.015 sec | … | 41 KB |
| 8x8-bit | 0.155 sec | 1-2MB | 771 KB |
| 10x10-bit | 3.619 sec | 16 MB | 14.5 MB |
| 12x12-bit | 108.185 sec | 80-160 MB | 260MB |
| 13x13-bit | 669.195 sec | 400-500 MB | *132 MB |
| 14x14-bit | 12108.8 sec | 550-1100 MB | *525 MB |
| **Platform** | **AMD Turion X2 Mobile TL-56 1.79 GHz, 2 GB RAM (VS2010, C/C++)** | | |
| **S-box** | Running Time: | RAM: | Size save result text file from Calculation: |
| 4x4-bit | 0.002 sec | … | 3 KB |
| 6x6-bit | 0.046 sec | … | 41 KB |
| 8x8-bit | 1 sec | 1-2 MB | 771 KB |
| 10x10-bit | 24 sec | 10-20 MB | 14.5 MB |
| 12x12-bit | 758 sec | 85-170 MB | 260MB |
| 13x13-bit | 3920.91 sec | 260 – 550MB | *132 MB |
| 14x14-bit | … | … | … |

* Without the values of S(x)⊕S (x⊕a), because the text file becomes very large with these values.

**4. Optimal 4 Bit S-Boxes**

A natural requirement for the S-boxes is their optimal resistance against linear and differential cryptanalyses. Unlike for higher dimensions the optimal values for Lin(S) and Diff(S) are known for the 4-bit S-boxes. More precisely, Lin(S) ≥ 8 and Diff(S) ≥ 4 (see [2]). More formally, as it is given in [2], the definition of an optimal 4-bit S-box is the following:

**Definition 1.** Let $S: F_2^4 \to F_2^4$ be an S-box. If S fulfills the following conditions we call S an optimal S-box.

1. S is a bijection.
2. Lin(S) = 8.
3. Diff(S) = 4.

When designing a block cipher it is important to know the set of S-boxes to choose from in order to get an optimal resistance against known attacks. Number of all permutations on $F_2^n$ is $2^n$ and even for small dimensions n, it is crucial to reduce the number of S-boxes which have to be considered.

It is well known (see for example [8]) that the values of Diff($S$) and Lin($S$) remain unchanged if we apply affine transformations in the domain or co-domain of $S$. In particular if we take an optimal S-box in the above sense and transform it in an affine way, we get another optimal S-box. That's why we could find only representatives of the different equivalence classes. The definition for the affine equivalence is the following:

**Definition 2.** The S-boxes $S_1, S_2: F_2^n \to F_2^m$ are affine equivalent if

$$S_2(x) = B \cdot S_1(A \cdot x \oplus a) \oplus b$$

where A and B are invertible $n \times n$ and $m \times m$ matrices, respectively, $a \in F_2^n, b \in F_2^m$.

In [2] Leander and Poschmann proved that there are only 16 different optimal 4-bit S-boxes up to affine equivalence. In [9] Saarinen extends on this work by giving further properties of the optimal S-Box equivalence classes. He defines two S-Boxes to be cryptanalytically equivalent if they are isomorphic up to the permutation of input and output bits and a XOR of a constant in the input and output. In [5] the authors consider all invertible 4-bit S-boxes and search for most efficient S-box in each equivalence class.

**5. Future Work**

This research is focused on the calculation of the most important parameters of given S-boxes, generation of optimal S-boxes and classification of all (or only the optimal) S-boxes of given size. We are going to improve our technique in two ways:

- Optimization of the algorithms and search for new effective methods for computations. Our examples in this work are mainly for 4 × 4-bit S-boxes. The application of the used methods to calculate the parameter for large S-boxes is not feasible with a conventional computer and basic architecture.
- Parallel programming.
  Modern processors offer more advanced techniques, such as parallelism, pipelining and instruction set extensions. Using these features for S-box implementations can result in other tradeoffs which could be investigated. Selection of a technology for parallel programming combined with different optimizing methods can ensure promising results.

**6. Conclusion**

S-boxes form the nonlinear part in the block ciphers therefore they are very important for security of the ciphers. We must select S-Boxes carefully in order to be optimally resistant against known attacks.

Here, we gave a brief classification of the S-boxes criteria. We considered some important parameters of the S-boxes and presented the programs for their calculation which we wrote in C++ programming language. We also added some test results on different S-boxes with the running time, the size of the used RAM, and the size of the text file with the results. There are different methods and algorithms to calculate these parameters. Here, we mentioned some of them and explained what we have used.

We gave a concept for optimality of an S-box. Searching for optimal S-Boxes is a difficult task. There are many algorithms, using different representations of the optimal S-boxes, but still the problem remains.

In Section 5 we mentioned different techniques which can be used to obtain promising results. Parallel programing together with different methods and optimizing techniques can offer promising results in calculations of the properties and finding optimal S-boxes.

**References:**

[1] C. E. Shannon: “Communication Theory of Secrecy Systems.” Bell System Technical Journal, Vol 28, pp. 656–717, October 1949.

[2] G. Leander and A. Poschmann: “On the Classification of 4 Bit S-Boxes.” In C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547, pp. 159–176. Springer (2007).

[3] M. Matsui. *Linear cryptanalysis method for DES cipher*. In Advances in Cryptology – EUROCRYPT’93, vol. 765 of LNCS, pp.386-397, Springer Verlag, 1994.

[4] Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1990).

[5] M. Ullrich, C. De Cannière, S. Indesteege, Ö. Küçük, N. Mouha, and B. Preneel: “Finding Optimal Bitsliced Implementations of 4x4-bit S-Boxes.” SKEW 2011 Symmetric Key Encryption Workshop, Copenhagen, Denmark, 16-17 February 2011.

[6] J. Daemen and V. Rijmen. The Design of Rijndael. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2002.

[7] An Braeken (March 2006): Cryptographic Properties of Boolean Functions and S-Boxes, PhD Thesis, Katholieke Universiteit Leuven.

[8] Claude Carlet, **“**Vectorial Boolean Functions for Cryptography”, Chapter of the monography “Boolean Models and Methods in Mathematics, Computer Science, and Engineering”, Cambridge University Press, 2010.

[9] M.J. O. Saarinen: "Cryptographic Analysis of All 4x4 Bit SBoxes." In A. Miri, S. Vaudenay (Eds.): Selected Areas in Cryptography 18th International Workshop, SAC 2011. Toronto, ON, Canada, August 1112, 2011, Revised Selected Papers. LNCS 7118, pp. 118133. Springer (2012)

# Пребарување информации во ЕРП системи: АртАИИС студија на случај

Ѓорѓи Гичев[1], Ана Паневска[1], Ивана Атанасова[1], Зоран Здравев[2], Цвета Мартиновска-Банде[2], Јован Пехчевски[3]

[1]Артисофт, Скопје, Македонија
(george.gicev, ana.panevska, ivana.atanasova)@artisoft.net
[2]Факултет за информатика, Универзитет „Гоце Делчев“ - Штип, Македонија
(zoran.zdravev, cveta.martinovska)@ugd.edu.mk
[3]Факултет за информатика, Европски универзитет - Скопје, Македонија
jovan.pehcevski@eurm.edu.mk

**Апстракт**

Во процесот на раководење и водење на една компанија, богатството информации со кои располага компанијата, а кои укажуваат на нејзиното функционирање и развој и кои се употребуваат за подобрување на целосниот тек на работа, е од голема важност да биде постојано на допир и пристап до оној кому му е потребно. ЕРП системите кои денес претставуваат јадрото на информации на бизнисот на една компанија сè повеќе наоѓаат место во истражувачките кругови поради потребите за нивно подобрување и редефинирање на функционалниот аспект на достапност на податоците во системот.

Во овој труд е прикажана практична имплементација на пребарувачка машина за постоечки ЕРП систем наречен АртАИИС. Решението се обидува да воведе една нова насока во пребарувањето податоци во ЕРП системот АртАИИС, имено текст базирано пребарување, кое овозможува искористување на богатството на информации во компанискиот информациски систем, како за редовни така и за нередовни и необучени корисници за увид, бизнис аналитика и сл. Резултатите од нашата евалуација на стандардното филтер пребарување и пребарувачката машина за дадена тест колекција на информациски потреби покажуваат дека димензијата на текст ориентирано пребарување придонесува за полесна употреба на пребарувачка функционалност во ЕРП системот АртАИИС за сите типови на корисници.

**Клучни зборови:** *пребарувачка машина, ЕРП системи, текст базирано пребарување, компаниско пребарување.*

## 1 Вовед

Во светот на континуиран и зголемен проток на информации, постои евидентно зголемување на квантитетот на податоци потребни за анализа, бизнис увид и управување со информацијата во модерните интегрирани информациски системи. Денешниот свет веќе генерира околу 2.5 ексабајти ($2.5x10^8$B) нови информации секој ден, што резултира со огромен импулс на решенија за Big Data (Halim, 2013).

Поради богатството на информации што ги има на веб, способноста да се пронајдат бараните информации со употреба на алатки за пребарување како Google заштедува многу време. Слични и поголеми предности, исто така, може да се добијат доколку пребарувањето на информации се ограничи во рамки на информациските системи на една компанија. Компаниска апликација, слично како и интернетот, поврзува компјутерски податоци низ целата компанија, обединувајќи различни типови информации во една единствена целина.

Како и во раните денови на интернетот, за да се пронајде информација во компаниската бизнис апликација потребно е да се знае каде истата се наоѓа. Овој метод

на пребарување претставува прифатлив начин за редовни корисници на системот за пребарување на информации за набавки, добавувачи или клиенти. Но, истиот не е применлив за повремен корисник на системот, па дури и за поредовен корисник кој пребарува информации низ апликацијата во област која не му е позната. Бидејќи компаниските апликации покриваат повеќе различни оддели и области на информации, тешко е корисниците на системот да имаат подетално познавање на функционалностите на целата апликација. Поради ова и апликациските вендори доаѓаат на пазарот со ралични решенија за пребарување во нивните продукти.

Постојат два различни приоди за овозможување на ваков вид на критично пребарувачка функција. Првиот приод се базира на компаниска апликациска алатка за пребарување која е цврсто интегрирана со компаниската апликација, и доставува пребарувачки резултати од апликацикиот систем на знаење. Овој тип на приод е применет од бројни технолошки вендори, вклучувајќи го и Google, кој ја претстави својата Google Search Appliance и Google Mini Products (Gaudin, 2012). Дополнително, SAP и Oracle продолжуваат со маркетинг на своите пребарувачки алатки како засебни продукти не само за своите апликации, туку и каде било на друго место во компанискиот интранет и бази на податоци.

Вториот приод на пребарување низ компанискиот информациски систем вклучува пребарувачка функција која е поцврсто интегрирана со специфична апликација, и истата претставува неопходна карактеристика која е потребно да се бара во една компаниска апликација. Само неколку апликациски вендори се фокусираат на доставување на функционалност на пребарување во рамки на нивната бизнис апликација која нуди пребарувачки способности слични на Google.

Денешните водечки светски софтверски вендори на ЕРП решенија сè повеќе започнаа со воведување на напредни пребарувачки машини во своите системи со цел подобрување на искуството на своите корисници. Дел од нив започнаа соработка со постоечки компании кои изработуваат вакви системи за интеграција на нивните апликации за поефикасно пребарување. Така Ziliak (2013), коосновач на xkzero, укажува дека според истражување спроведено од нив, корисниците на традиционалните ЕРП системи може да поминат и до 25% од своето време во пребарување на основни податоци низ своите системи. Нивниот систем GetX овозможува пребарување во стилот на Google за познатите Sage ЕРП системи преку пребарување на индексирана база на податоци (Ziliak, 2013).

Дополнително, сè повеќе компании ги препознаваат предностите од ваква надградба на својот ЕРП систем. Таков пример е компанијата EnPro (Frey, 2013). Компанијата решава да имплементира скалабилно и аналитичко решение кое ќе обезбеди преглед во корисничките интереси во реално време. Со помош на технологиите in-memory, овој приод овозможува податочно процесирање и аналитика во неколку секунди – искористувајќи ја машината на ЕРП системите од новите генерации.

Во овој труд детално е прикажана практичната имплементација на *артисофт пребарувачката машина*. Во продолжение на трудот е направен осврт на архитектурата, компонентите и нивната меѓсебна комуникација. Понатаму се опишани чекорите за имплементација на артисофт пребарувачка машина во ЕРП системот АртАИИС. На крај се прикажани резултатите од евалуацијата на двата типа на пребарување, филтер пребарување и артисофт пребарувачка машина и соодветно се диксутирани заклучоците и идните надградби и доработки на предложеното решение.

## 2. ЕРП пребарувачка машина во АртАИИС

Основната идеја на оваа практична имплементација беше да се развие сервисен и веб-ориентиран софтверски модул кој е интеграбилен, односно може да се користи како

пребарувачка машина во рамки на било која веб-базирана апликација и без разлика на документите т.е. содржините низ кои истата ќе пребарува.

Идејата се темели на два основни концепта:

- *Plug-n-play концепт на интеграбилност на корисничкиот интерфејс* – овој концепт подразбира дека пребарувачката машина како кориснички интерфејс за пребарување може да се имплементира врз која било веб-базирана апликација, независно од технологијата што се користи за развој на апликацијата во која се имплементира, како и од онаа за развој на пребарувачката машина.
- *Концепт на независност од колекција на документи* - овој концепт подразбира независност од видот на документи низ кои сакаме да пребаруваме, како и содржината на истите. Пребарувачката машина се полни, т.е. храни со податоци за овие документи преку јавно достапни веб-сервиси кои може да се повикаат од кој било софтвер независно од технологијата што се користи за развој на истиот. Од овој аспект, артисофт пребарувачката машина претставува сервисно-ориентиран продукт.

Артисофт пребарувачката машина претставува интегриран софтверски модул кој е комбинација од веб-апликација и множество на веб-сервиси за интерна комуникација во рамки на апликацијата, како и екстерни сервиси за комуникација со надворешни апликации. Токму екстерните сервиси се оние сегменти од решението кои овозможуваат имплементација на артисофт пребарувачката машина на која било веб-базирана апликација, т.е. систем. Апликацијата за потребите на индексирање и пребарување на документи го користи Lucene[1] - open-source множество од библиотеки кое овозможува поддршка за развој и имплементација на апликации за пребарување низ документи. Lucene, главно, се користи за пребарување низ текстуални содржини, иако има можност и за еден вид „имитација” на релациона база на податоци. Целиот пакет е збир од Јава базирани библиотеки кои содржат моќни класи и функции за индексирање и пребарување на текстуални содржини.

### 2.1. *Архитектура на артисофт пребарувачката машина*

Артисофт пребарувачката машина е продукт кој претставува комбинација од веб-апликација и множество од веб-сервиси за комуникација во рамки на истата, како и со надворешни системи врз кои истата би се интегрирала. Развојот на веб-апликацијата и веб-сервисите е доволно параметарски така што поддржува функционалност на различни платформи и технологии. Во продолжение ќе ги резимираме основните поими за пребарување информации и елементи на артисофт пребарувачката машина.

**Документ**

Документ е ентитет кој претставува логичка целина од содржина, автор, наслов, опис и сл. кој е од одредена вредност за дадена компанија, но истиот физички не мора да постои. Може да биде збир од записи во база на податоци, извештај добиен од некоја апликација, документ кој физички се чува во некој системи за менаџирање на документи или кој било електронски документ.

Секоја компанија може да чува повеќе документи од различни категории. Секој еден документ кој се индексира мора да се креира како Lucene Document објект или поточно објект од класата org.apache.lucene.document.Document. Полињата содржина, наслов, автор и краток опис се индексираат при градење на индексот. Сите полиња, освен полето

[1] http://lucene.apache.org/

содржина се чуваат во рамки на документ објектот, т.е. во индексот. Полето содржина не се чува поради фактот што индексот може да бара голема меморија за манипулација и да го забави процесот на пребарување. Сите останати информации се доволни за идентификација на документот и приказ на резултатите при пребарување. URL на документот може да биде мрежно достапна физичка локација на постоечки документ, URL до одреден документ во веб-апликација итн.

**Стоп-зборови**

Стоп-зборови е множество од зборови за дадена компанија кои треба да се игнорираат при индексирање и пребарување. Секоја компанија го параметризира ова множество на зборови. Стоп-зборовите се најчесто сврзници, предлози и слични зборови кои не се многу значајни при пребарување. Од аспект на индексирање, ваквите зборови значително придонесуваат во намалување на големината на индексот.

**Стоп-карактери**

Стоп-карактери е множество од специјални карактери кои се користат за поделба на даден текст на зборови. Иницијален стоп-карактер е празното место. Дополнително стоп-карактери може да бидат карактери како “,./\';][!@#$%^&*()_+=” итн.

Мора да напоменеме дека колку и да изгледа едноставно мора да се посвети внимание при дефинирање на ваквите карактери, бидејќи истите може значајно да влијаат на пребарувањето. Пример за вакво сценарио е користење на “.” како стоп-карактер. На крајот од реченица таа е стоп-карактер, меѓутоа при индексирање на датумот 22.03.2013, термовите (терм, во понатамошниот текст збор) кои ќе се индексираат се “22”, “03” и “2013”.

**Парсер**

Парсерот е ентитет кој во интерниот дизајн на решението се нарекува *тип на парсер*. Всушност, операцијата на парсирање се извршува преку Lucene објектот Analyzer, поточно објект од класата org.apache.lucene.analysis.standard.StandardAnalyzer. Тип на парсер како ентитет се користи заради дефинирање на различни комбинации на стоп-зборови и стоп-карактери при индексирање на различни видови документи.

**Инвертиран индекс**

Инвертиран индекс претставува структура која чува статистики за множеството од зборови во документната колекција, како и листа од документи во кои даден збор се појавува. Целата комплексност на форматот на зачувување, заедно со сите информации и врски меѓу објектите кои се креираат при градење на индексот, е задача која ја извршува Lucene. Она што треба да се дефинира при генерирање на индексот е неговата физичка локација, односно директориумот во кој истиот ќе се чува. За Lucene индексот е збир од датотеки кои се запишуваат во еден директориум и се меѓусебно зависни. Оваа комплексност ја елиминираме така што индексот го нарекуваме директориум и ја знаеме локацијата на која треба да запишуваме и од која треба да читаме при пребарување.

### *2.2. Компоненти на артисофт пребарувачката машина*

Архитектурата на артисофт пребарувачката машина се состои од неколку компоненти: Document Crawler, Document Creator, Index Builder, Index и Searcher. Тие се објаснети како што следува.

*Document Crawler* – е компонента која комуницира со надворешни системи заради пронаоѓање на документи кои на одреден начин се означени дека треба да се

индексираат. Алгоритмот е креиран да ги помине рекурзивно сите директориуми на дадената локација и да ги собере сите пронајдени документи. Секој од овие документи се процесира и според форматот на истиот се повикува компонента која ја презема содржината на истиот во текст формат, како и други податоци од типот на наслов, автор и сл.

*Document Creator* - е компонента која директно може да се повика од кој било надворешен систем во вид на веб сервис. Се користи за обработка на документот во моментот на негово креирање, при што сервисот ја експортира содржината на истиот или пак ја добива во форма на текст како влезен аргумент. По процесирање на документот се повикува *Index Builder* компонентата која го индексира истиот.

Паралела на горниве две компоненти е веб crawler, робот компонента која го изминува вебот и ги индексира новите документи. Во случајот кога треба да се изминат веќе постоечки документи има потреба од дополнителни сетирања. Ова парче код го нарекуваме docProxy и е прашање на имплементација на секој систем кој ќе ја користи пребарувачката машина.

*Index Builder* - оваа компонента игра една од клучните улоги во системот и се користи за индексирање на еден или група на документи. Се повикува од една од класите documentCrawler или documentCreator во Lucene кои како резултат даваат множество на документи. Всушност, задачата на оваа компонента е да запише еден или множество на документи во т.н. индекс на компанијата на која и припаѓаат документите.

*Searcher* - Searcher (Пребарувач) е компонента која се користи за пребарување. Оваа компонента како влезни аргументи прима идентификатор на компанијата и корисникот кој пребарува, како и клучните зборови. Нејзината задача е да пребарува низ директориумот кој се чува во RAM меморија, или пак низ главниот индекс, доколку не постои индекс во RAM меморија. Притоа се дефинира и по која од колоните кои се индексирани ќе се пребарува.

### 2.3. Практична имплементација на артисофт пребарувачката машина

ЕРП системите на компаниите се централно место каде што се чуваат сите документи потребни за функционирањето на истите. Пребарувањето во ЕРП системите најчесто се врши со полиња филтри каде што корисникот е потребно да знае точна информација за идентификување на документот или пребарувањето резултира во голема листа на документи, подредени по нерелевантни фактори за оној кој пребарува.

АртАИИС е ЕРП системот на артисофт кој генерира 50-тина различни типови на документи. Пребарувањето се врши низ посебни функции за секој различен тип на документ со предефинирани филтри селектирани според проектантските анализи и одлуки при иницијалното проектирање на системот или пак при редизајн, секако со ограничувачки фактори. На овој начин не би можеле да се земат предвид сите можни сценарија, промени и потреби на корисниците, па во даден момент истиот е нефлексибилен и крут за корисниците.

Во продолжение се резимирани сите чекори потребни за имплементација на функционалност за индексирање и пребарување на документи од АртАИИС од тип *тикети* преку *артисофт пребарувачката машина*. Овие чекори се генерализирани и важат при имплементација на пребарувачката машина над која било колекција на документи од каква било категорија.

1) *Чекор 1: Поставување на компанија* – Првиот чекор е евиденција на компанијата која ќе ја користи *пребарувачката машина*.
2) *Чекор 2: Внес и мапирање на корисници* – За секоја компанија е потребно да се внесат

и мапираат корисниците на ЕРП системот кои би го користеле пребарувањето како функционалност. Секое пребарување се евидентира во историјат на пребарувања за корисникот кој пребарувал.

3) *Чекор 3: Конфигурација на системот* – Задолжителен чекор пред да се индексираат документите е конфигурација на начинот на процесирање на содржината на документите. Овој чекор опфаќа пополнување на стоп-карактери и стоп-зборови, како и креирање на потребните типови на парсери. Типот на парсер кој го креиравме за целите на имплементација на Пребарувачката машина во АртАИИС е означен за default и ги вклучува стоп карактерите ^|,;:!?'"$*&/\., како и стоп зборовите *во, да, до, е, и, иако, итн, каде, како, на, но, од, по, покрај, пред, се, сл, т.е., што*, итн.
4) *Чекор 4: Полнење на индекс* – Веќе ги објаснивме компонентите *documentCrawler* и *documentCreator* кои се користат за обработка на документите кои треба да се индексираат и повикување на компонентата Index Builder која ќе ги индексира. Компонентата *documentCreator* е погодна доколку документите физички постојат на дадена мрежно достапна локација. Во нашиот случај документите (тикетите) се виртуелни, т.е. се комбинација од податоци кои се чуваат во релациона база на податоци. Во овој случај мора да креираме *docProxy* компонента, т.е. парче код кое ќе ги креира документите кои сакаме да ги индексираме. Секој систем во кој се чуваат виртуелни документи треба да има можност за нивно печатење, при што документот се генерира во некаков отворен формат (најчесто pdf). Готовиот модул за печатење на документи се користи за нивно физичко креирање, по што пред да бидат избришани, се повикува компонентата која ќе ги индексира. Компонентата *documentCreator* може да се користи и за индексирање на сите новонастанати документи.
5) *Чекор 5: Интеграција на кориснички интерфејс* – Овој чекор подразбира воведување на можност за пребарување низ индексираните документи преку апликацијата на самиот корисник, во овој случај АртАИИС ЕРП системот.

## 3. Евалуација на ефективноста на артисофт пребарувачка машина

Во оваа секција се резимирани резултатите од евалуација и тестирање на практичната имплементација на артисофт пребарувачката машина во ЕРП системот АртАИИС. Методологијата за евалуација вклучува статистичка анализа и презентација на перформансите на двата системи преку добро познат сет од мерки за евалуација: Presicion, Recall и MAP (Manning et al., 2009). За пресметка на овие мерки користен е TREC_EVAL 8.1 софтверскиот пакет.

Најважните метрики за евалуација на ефективноста на еден пребарувачки систем се:

- RECALL – враќање на сите релевантни документи;
- PRECISION – враќање на најрелевантните документи на почеток од листата;
- КОМБИНАЦИЈА
    - враќање на што помалку нерелевантни документи;
    - враќање на релевантните документи пред нерелевантните.

Precision (P) е делот на вратени документи кои се релевантни

$$Precision = \frac{\#(\text{вратени релевантни документи})}{\#(\text{вратени документи})}$$

Recall (R) е делот на релевантни документи кои се вратени

$$Recall = \frac{\#(\text{вратени релевантни документи})}{\#(\text{релевантни документи})}$$

Mean Average Recall (MAP) единствена мерка за квалитетот на сите нивоа на recall:

$$MAP(Q) = \frac{1}{|Q|}\sum_{j=1}^{|Q|}\frac{1}{m_j}\sum_{k=1}^{m_j} Precision(R_{jk})$$

Дополнително, пребарувањето на информации низ компаниските информациски системи има различни потреби и специфики. Компаниските ЕРП системи се користат од различни типови на корисници, корисници кои се во секојдневна интеракција со системот и функционалности кои се блиски со обврските кои ги имаат на работното место и корисници кои не се доволно обучени да го користат системот или одреден дел од системот кој не е поврзан со нивните секојдневни обврски. Во евалуацијата што следува ќе ги земеме предвид двата типа на корисници.

### *3.1. Опис на тест колекција*

Секоја тест колекција што се користи за евалуација на ефективност на информациски ситеми се состои од три главни компоненти:

- Колекција на документи, која е множество од документи што ќе се индексираат и врз кои ќе се извршува пребарување и мерење;
- Колекција на упити или пребарувања, т.е. тест множество од информациски потреби (пребарувања, query-ja);
- Множество на рачно идентификувани релевантни документи за секој упит или пребарување.

#### *3.1.1. Колекција на документи*

Колекцијата на документи е множество од сите документи од АртАИИС од тип *тикети*. Тикет претставува документ кој се генерира за секоја активност во рамки на компанијата која подразбира интеракција со клиент на истата. Секоја пријава на проблем, барање за модификација, оперативна поддршка и сл. резултира со документ од овој тип во ЦРМ (CRM – Customer Relationship Management) модулот од АртАИИС. Тикетите содржат повеќе описни податоци внесени од страна на клиентите, како опис и манифестирање на проблем, како и информации кои се внесуваат од страна на вработените кои го разрешуваат проблемот, како што се причина за појава на проблем, мислење, опис на решение на проблемот и сл.

Во продолжение, во табела 1 се прикажани основни статистики за колекцијата на документи (тикети):

**Табела 1.Статистики за колекцијата на документи**

| | | | |
|---|---|---|---|
| **Бр. на документи** | 2908 | **Бр. на зборови** | 363166 |
| **Просечен бр. на зборови во документ** | 124.8 | **Големи на индекс на хард диск** | 1.12MB |
| **Време на генерирање на док.** | 60ms | **Време на индексирање на документ** | 422ms |

#### *3.1.2. Тест множество на упити*

Тест множеството од информациски потреби претставува збир од различни видови на упити или пребарувања (queries) кои се генерирани од експерти, односно лица кои секојдневно ги креираат или пак употребуваат на било каков начин документите од тип *тикет.*

Колекцијата содржи вкупно 25 пребарувања кои се поделени во две категории:

1. *Филтер, DB (Database)-ориентирани пребарувања* - Пребарувањата кои припаѓаат на оваа категорија може релативно лесно и точно да генерираат резултати од пребарувањето користејќи ги постоечките филтри за пребарување во ЕРП системот АртАИИС. Тикетот е збир од полиња кои се пополнуваат според шифрарници, односно еден вид на формулар, како и од полиња кои се текстуални. Доколку за пребарувањето е доволно пополнување на одредени филтер полиња или пак датумски полиња, тогаш пребарувањето припаѓа во оваа категорија. Оваа категорија содржи 14 од вкупно 25 пребарувања и се користи за моделирање на потребите на корисниците кои се во секојдневна интеракција со системот и функционалности кои се блиски со обврските кои ги имаат на работното место.
2. *Текст-ориентирани пребарувања* - Пребарувањата кои припаѓаат на оваа категорија, односно резултатите кои се очекуваат од истите не може да се добијат користејќи ги постоечките филтри за пребарување во ЕРП системот АртАИИС, односно системот или не поседува можност за пребарување според одредени услови или пак генерира огромна листа од резултати која не е подредена според никаква релевантност во однос на она што се пребарува. Овие пребарувања најчесто се комбинација од зборови кои може да се појават како дел од кое било од текстуалните, т.е. описните полиња на тикетот. Пример за такво пребарување е комбинација од неколку збора и датум или пак дел од датум. Оваа категорија содржи 11 од вкупно 25 пребарувања и се користи за моделирање на потребите на корисниците кои не се доволно обучени да го користат системот или одреден дел од системот кој не е поврзан со нивните секојдневни обврски.

### 3.1.3. Множество на релевантни документи

Последниот сегмент од тест колекцијата е множеството на релевантни документи за секој упит или пребарување. Резултатите од пребарувањата во двата система, како и листата на релевантни документи потоа се користи како влез во TREC_EVAL.8.1 кој пресметува множество на метрики кои се користат за евалуација (оценување) и споредба на двата система.

Итеративно се поминуваат сите пребарувања и за секое се извршуваат следните чекори кои резултираат со добивање на множество од максимум 80 документи за евалуација за секое пребарување, како и вектор на релевантност за секој од овие 80 документи:

1. *Пребарување во пребарувачка машина* - Се извршува пребарување во артисофт пребарувачката машина со одреден сет на клучни зборови и се евидентира времето на пребарување, како и листа од идентификациски броеви на документите кои се добиваат како резултат сортирани според алгоритам за Scoring на документи на Lucene (OkapiBM25) за релевантност. Пребарувањето го извршува корисник кој не е многу искусен во работа со документи од тип *тикети*.
2. *Пребарување во АртАИИС* - Се извршува пребарување во АртАИИС со сет на филтри кои ги дефинира корисникот од информацискатa потреба на пребарувањето.

Се евидентира времето на пребарување, како и листа од идентификациски броеви на документите кои се добиваат како резултат сортирани според редослед на внес на документите во системот. Редоследот на приказ на даден документ е всушност неговиот ранг. Пребарувањето го извршува корисник кој не е многу искусен во работа со документи од тип *тикети*.

3. *Сет на резултати кои се повторуваат* – Од евидентираната листа на идентификациски броеви на тикети, како и нивните рангови, програмски се селектираат оние кои се повторуваат како резултат во пребарувањата извршени во првите два чекора. Доколку има 80 или пак помалку од 80 вакви документи сите стануваат дел од множеството на документи за евалуација на релевантност. Доколку има повеќе од 80 документи, се селектираат првите 80 сортирани според средната вредност на рангот на документот во двата система. Во овој случај се прескокнува чекорот 4.
4. *Сет на резултати кои не се повторуваат* – Доколку во претходниот чекор не се формира колекција од 80 документи, истите се дополнуваат со документи кои се појавуваат како резултати само во еден од системите. Распределбата е подеднаква.
5. *Оценување на релевантност на* пребарувања – Во овој чекор се избираат експерти, односно лица кои ја познаваат проблематиката и кои ќе ја оценуваат релевантноста на секој од документите во колекцијата на документи за евалуација на даденото пребарување. Секој од документите бинарно се означува дали е релевантен за моменталното пребарување (со 1 или 0). Оваа листа на вредности го формира векторот на релевантност.
6. *Генерирање на влез во TREC_EVAL* – Од генерираните листи на резултати, придружени со нивните рангови, како и колекцијата на документи за евалуација и векторот на релевантност, програмски се генерираат текстуални документи кои потоа претставуваат влезни аргументи во програмата за евалуација. При ваквата обработка на резултатите се добиваат и одредени статиситки за тест колекцијата.

Во продолжение се прикажани општи статистички податоци за тест колекцијата за секоја категорија на пребарувања (табела 2 и табела 3).

**Табела 2. Статистички податоци за тест колекцијата за категорија *текст***

| Резултати | Максимален бр. | Минимален бр. | Просечен бр. |
|---|---|---|---|
| **Артисофт пребарувачка машина** | 2899 | 22 | 1474 |
| **АртАИИС** | 2445 | 0 | 458 |
| **Релевантни док. во колекција на док. за евалуација** | 80 | 0 | 40 |

**Табела 3. Статистички податоци за тест колекцијата за категорија DB**

| Резултати | Максимален бр. | Минимален бр. | Просечен бр. |
|---|---|---|---|
| **Артисофт пребарувачка машина** | 2894 | 25 | 1394 |
| **АртАИИС** | 2445 | 0 | 660 |
| **Релевантни док. во колекција на док. за евалуација** | 80 | 7 | 29 |

### *3.2. Експериментални резултати*

Во продолжение се прикажани резултатите, табеларно (табела 4 и табела 5) и графички (слика 1 и слика 2) од евалуација на двата система за пребарување со двете категории, DB базирани и текст базирани пребарувања.

**Табела 4. Резултати од пребарување со DB базирани пребарувања**

| DB БАЗИРАНО | |
|---|---|
| **Артисофт пребарувачка машина** | |
| **Метрика** | Вредност |
| **P5** | 0.27 |
| **P10** | 0.26 |
| **P15** | 0.25 |
| **P20** | 0.26 |
| **P30** | 0.27 |
| **P100** | 0.28 |
| **MAP** | 0.25 |
| **AP** | 0.05 |

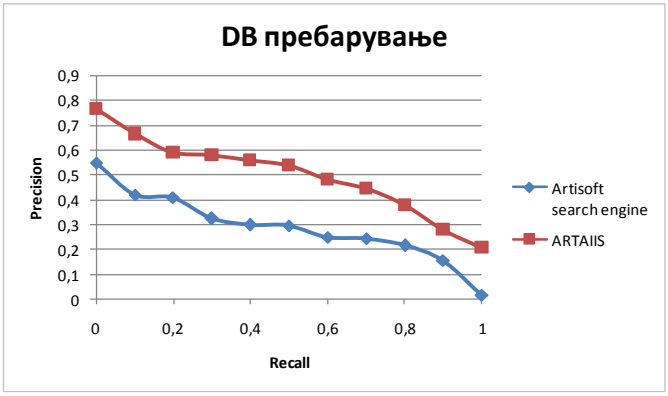
| DB БАЗИРАНО | |
|---|---|
| **АртАИИС** | |
| **Метрика** | Вредност |
| **P5** | 0.43 |
| **P10** | 0.44 |
| **P15** | 0.42 |
| **P20** | 0.42 |
| **P30** | 0.42 |
| **P100** | 0.41 |
| **MAP** | 0.45 |
| **AP** | 0.19 |

**Табела 5. Резултати од пребарување со текст базирани пребарувања**

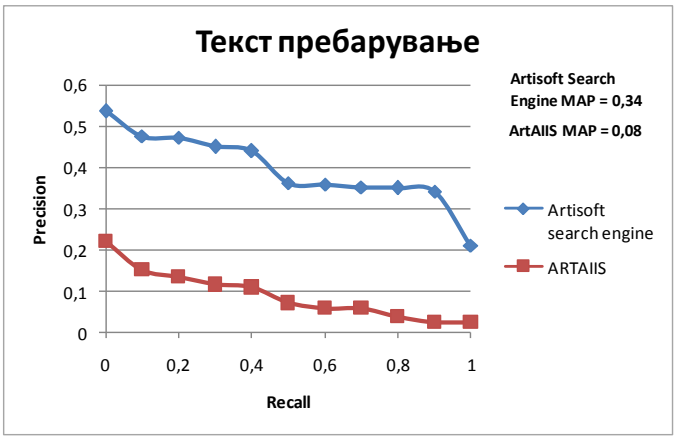
| ТЕКСТ БАЗИРАНО | |
|---|---|
| **Артисофт пребарувачка машина** | |
| **Метрика** | Вредност |
| **P5** | 0.36 |
| **P10** | 0.32 |
| **P15** | 0.31 |
| **P20** | 0.30 |
| **P30** | 0.25 |
| **P100** | 0.27 |
| **MAP** | 0.34 |
| **AP** | 0.22 |

| ТЕКСТ БАЗИРАНО | |
|---|---|
| **АртАИИС** | |
| **Метрика** | Вредност |
| **P5** | 0.11 |
| **P10** | 0.07 |
| **P15** | 0.08 |
| **P20** | 0.08 |
| **P30** | 0.08 |
| **P100** | 0.08 |
| **MAP** | 0.08 |
| **AP** | 0.01 |

Резултатите покажуваат дека артисофт пребарувачката машина е значително поефективна при текст-базирани пребарувања (табела 5 и слика 2), додека очекувано стандардното филтер пребарување во АртАИИС ЕРП системот се покажа како поефективно во пребарувањето на информации поврзани со дадени точно познати вредности за атрибутите на документот кој се бара (табела 4 и слика 1). Секако, вториот случај подразбира детално познавање на начинот на кој функционира целиот систем, додека првиот е прикладен за корисници кои воопшто не се запознаени со спецификите на системот и се научени да пребаруваат информации користејќи стандардни методи на веб (или Google-like) пребарување.




**Слика 1. Резултати Precision и Recall од пребарување со DB базирани пребарувања**




**Слика 2. Резултати Precision и Recall од пребарување со текст базирани пребарувања**

## 4. Заклучок и идна работа

Во овој труд прикажавме практична имплементација на пребарувачка машина за постоечки ЕРП систем наречен АртАИИС. Преку експериментални резултати покажавме дека без разлика колку и да му е добро познат системот на корисникот кој пребарува, времето потребно да се навигира до одреден кориснички екран за пребарување низ даден тип на документи, како и времето потребно да се пополнат сите филтри, не смее да се запостави. Придонесот од имплементација на пребарувачка машина врз кое било парче софтвер е во можноста за брзо и ефективно пребарување низ множество на документи и текстуални содржини од различни типови, користејќи единствен и едноставен кориснички интерфејс.

Во иднина би можело да се направат неколку дополнителни оптимизации на пребарувачката машина во поглед на претпроцесирањето на документите, како и во алгоритамот за рангирање на истите. Поддршка на латинично и кирилично пребарување е исто така потребна идна надградба на пребарувачката машина, со цел да се овозможи намалено време за доаѓање до потребната информација преку олеснување на корисничката интеракција со системот.

## Литература

[1] Frey, L, (2013). Reinventing the ERP Engine. Tech Trends 2013 – Enablers http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Services/Consulting/uk-con-reinventing-erp-engine.pdf

[2] Gaudin, S, (2012). Google upgrades Search Appliance for enterprises. ComputerWorld, http://www.computerworld.com/s/article/9232198/Google_upgrades_Search_Appliance_for_enterprises

[3] Halim, N. 2013, Stream processing. Director and Chief Architect of Big Data, IBM. прегледано на 20.11.2013 http://www.ibm.com/smarter-computing/us/en/technical-breakthroughs/stream-processing.html

[4] Manning, C, D, Raghavan, P, Schütze, H, (2009). *An Introduction to Information Retrieval,* Cambridge University Press

[6] Ziliak, P, (2013). Powerful ERP search tool now available for Sage 100 ERP v2013. http://www.prweb.com/releases/2013/2/prweb10478394.htm, прегледано на 10.12.2013

# ЕДУКАТИВНО ПОДАТОЧНО РУДАРЕЊЕ СО MOODLE 2.4

Зоран Милевски[1], Зоран Здравев[1]

[1] Факултет за информатика, Универзитет „Гоце Делчев“ - Штип
milevskiz@gmail.com, zoran.zdravev@ugd.edu.mk

**Апстракт**

Околините за е-учење имаат за цел да обезбедат ефикасни методи за учење, да овозможат корисниците во кое било време да пристапат кон одредени ресурси, да постават решенија за одредени проблеми, да бидат оценети за нивниот труд и сл. Една од попознатите такви околини е системот за е-учење Moodle. Овие околини како Moodle користат и складираат големи количини на податоци, но во повеќето случаи не задоволуваат поголем дел од барањата за нивна примена и недоволно ја прикажуваат активноста на учесниците при учењето. Целта на овој труд е со помош на техники за податочно рударење како што се класификација, кластерирање, статистики и регресија, да се опише процесот на селекција и добивање на податоци од базата на податоци на Moodle и да се креира контролна табла – веб базирана апликација што ќе комуницира со системот за е-учење Moodle и ќе обезбедува неколку нивоа на пристап и тоа: менаџерско, администраторско, наставничко и корисничко ниво, и практично ќе прикажува обработени податоци и извештаи кои ќе го подобрат пристапот на евалуација на поголеми групи на учесници во процесот на учење. Со тоа директно се решава и проблемот на наставниците во поглед на нивната поддршка при работа со ваков тип на платформи и големи количини на податоци.

**Клучни зборови:** *далечинско учење, е-учење, едукативно податочно рударење, Moodle, едукативни контролни табли, извештаи во повеќе нивоа.*

# EDUCATION DATA MINING WITH MOODLE 2.4

Zoran Milevski[1], Zoran Zdavev[1]

**Faculty of computer science, Goce Delcev University, Stip, Macedonia**
milevskiz@gmail.com, zoran.zdravev@ugd.edu.mk

**Abstract**

The goal of e-learning environments is to supply effective learning methods, to enable the users to approach certain resources at any time, to set solutions for certain problems, assessment for the work etc. One of the best known environments of this kind is e-

learning system Moodle. These environments like Moodle use and save large amount of data in their databases, but in most cases they don't offer enough information of the course participants and their activities in the system. The aim of this work is, by the use of data mining techniques such as classification, clustering, statistics and regression, to describe the process of selection and acquiring data from the Moodle database, and to create dashboard - web based application, that would communicate with the e-learning system Moodle and supply multilevel approach as: manager, administrator, teacher and user level; and practically will improve the approach to evaluation of larger groups of participants in the learning process. This will help teachers to evaluate web activity of the students, to get more objective feedback and find out more about how the students learn. Also this dashboard will directly solve the teachers problems in the terms of dealing with this kind of platforms and big amounts of data.

**Keywords:** *Distance Education, E-learning, Educational data mining, Moodle, Educational Dashboard, Multilevel reports.*

## 1. Introduction

Web-based educational systems and their usage has increased rapidly in the last few years. The impact on this trend comes from the fact that neither teachers nor students are limited any longer to be at the same time on the same location, and additionally these online education-based systems are independent from any hardware platforms [6]. The approach to these platforms is only through internet browser and thus the dependence on different operative systems and their demands is neutralized. These educational systems have been installed in many universities, and even individual teachers use them with a goal of setting certain resources that will be easily approachable for certain groups of people.

Moodle (Modular Object Oriented Developmental Learning Environment) as an educational system is well known and widely used because it is open code and also satisfies greater part of the needs for its use, and it is also simple to use both for the teachers and the students as course participants [1], [2], [3]. Moodle accumulates great amount of different information that is very important when analyzing the students conduct and represents a gold mine of educational data. Moodle stores all the data of the activities in which the students are involved. Moodle also keeps data of the participants profiles, their activity in different courses, their sent assignments etc.

The e-learning system Moodle is used in 232 countries in the world and at the moment there are 79429 active Moodle web sites, whereas in Macedonia there are 39 Moodle web sites most of which belong to the universities in the country [14].

Although Moodle, as well as the other systems of this type, offers tools for reports and view of the more important activities of the course participants, when it comes to a bigger number of students it becomes hard to follow their activity. On the other hand, although the goal of the e-learning systems is to motivate the

student by the use of multimedia materials to make studying more interesting and of higher quality, they don't always succeed in keeping the student's focus on the learning itself. Instead of learning they use the opportunities that the system offers in the direction of social communication between them (chat) [5]. Whatsoever, to make studying more effective, it is important to supply personalization of the contestants, based on their activity, an opportunity to analyze the participants in different courses, prediction of the results of the participants and better survey of the activities of the students. A promising area, when it comes to fulfilling this goal is data mining, and in this case it is educational data mining with the Moodle 2.4 database [3], [6].

Educational data mining means selective extraction of the kept data of large databases, their processing with the use of several educational techniques of data mining such as classification, clustering, statistics, regression etc. and acquiring the processed data that would improve the approach to larger groups of participants in the learning process [7]. The acquired information can be used not only by the teachers, but the students themselves too. They can get recommendations and directions for certain activities and resources that would improve their learning, where the teacher can get the feedback necessary for the evaluation of the students activity, separating the students in groups based on the need for their monitoring, finding the frequent mistakes made both by the students and the teachers; view into the activities assigned for the students; and have greater effect than the others [6].

Web based application connected to the active Moodle database can provide several levels of approach:

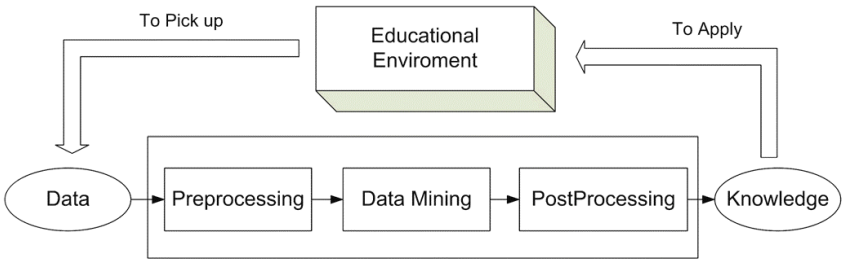
- Manager level approach,
- Administrator level approach,
- Teacher level approach and
- User level approach.

All of these roles are included in the, so called, dashboard and they will be explained in this study.

This dashboard is external application made to be very easy to use, because all needed reports for the various users are simplified in one place and enable a survey of some information kept in the new dashboard database, while the standard reports don't give such view with the use of standard reports.

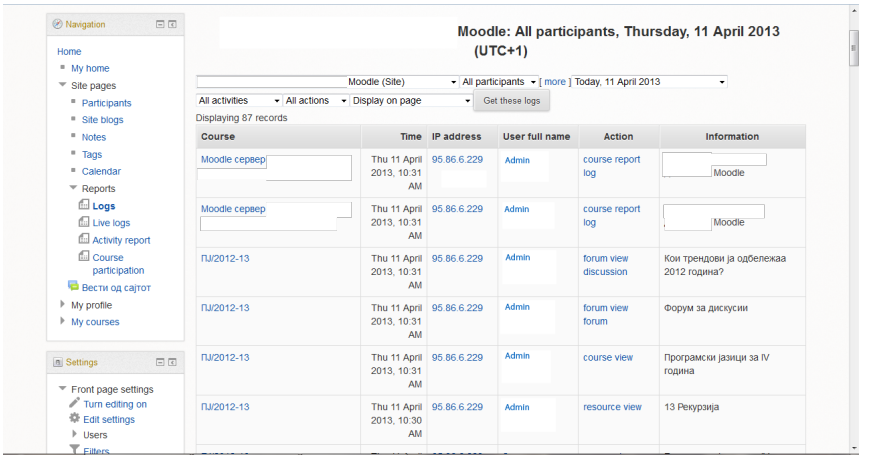
## 2. Data analyses in the Moodle database

It is very important what kind of data is kept in the database and the more data is processed the more information can be acquired. Figure 1 illustrates the process of educational data mining and the way this process works [2].




Слика 1. Процес на едукативно податочно рударење
Figure 1. Process of educatonal data mining

Educational data mining is an interactive process in which not only the processed data can be acquired, but it can also be filtered so that a certain decision can be made. The process consists of gathering information about the students' interaction within the process, than data processing so that they can be transformed into a relevant format to be mined. Data mining is applied, i.e. algorithms are used that provide and summarize the acquired interests about a certain user (teacher, student, manager etc.). Finally, the results are interpreted, evaluated and represented [2], [6].




Слика 2. Приказ на Moodle извештај
Figure 2 Moodle log report screen

Moodle stores every click of the user and its system navigation. Figure 2 shows a scheme of modest report record of Moodle about the site activities. Records can be filtered by course, participant, data and type of activity [15]. Teachers can use this report to follow the course participants activity, what they do and when. For activities such as quizzes the report contains data about the results, the time length of the quiz activity, as well as detailed analyses of every answer of the student. These reports are useful, but at the same time they are not clear enough. For a more effective view for the teacher, besides course activity it is important to be able to see which of the activities attracted greatest attention, which is the least visited material, in the quiz section, besides detailed analyses of every

answer, which is the question that was answered by the smallest number of students, analyses of the results of one student or all the students in several quizzes etc. [4], [13].

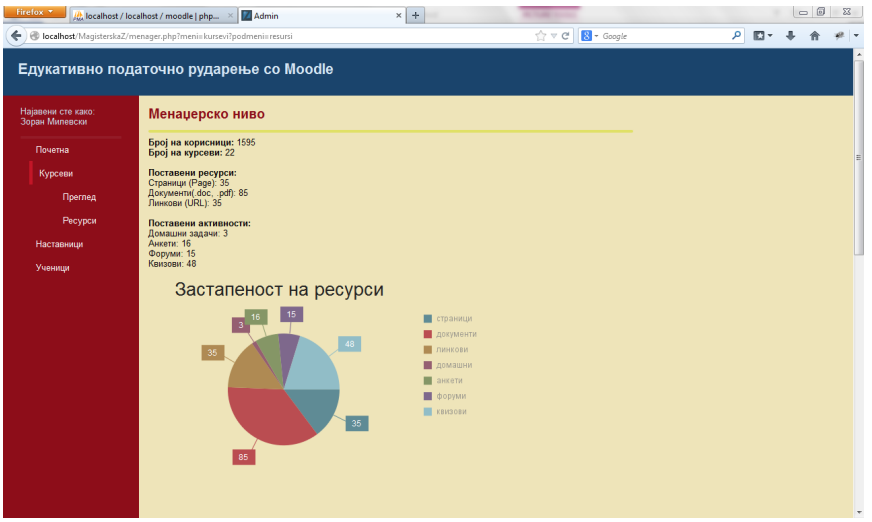
Moodle doesn't keep these records as text but keeps them in relational MySql database. Moodle database has around 145 related tables, but all of them are not necessary to implement educational data mining. Table 1 schemes the more important tables with their description that would be used for getting raw data so later be processed with several different techniques [6].

Табела 1. Поважни табели во базата на податоци на Moodle и нивни опис
Table 1. More important tables in Moodle database and their description

| Table name | Table description |
|---|---|
| mdl_assign | Homework data |
| mdl_assign_submission | Sent homework status for a student |
| mdl_assign_grades | Homework score |
| mdl_choise, mdl_answers и mdl_option | View of questionnaire answers |
| mdl_course | Created courses data |
| mdl_enrol | Type of log on, course logging password |
| mdl_forum и mdl_forum_discussions | Created course forums and survey discussions started by a certain user |
| mdl_posts | Forum answers with date, |
| mdl_read | user, message, |
| mdl_grades и | Forum participants activity |
| mdl_grade_letters | Summarizing participant grades and score criteria and |
| mdl_lesson | final grade |
| mdl_log | Set lessons data |
| mdl_message и | Log for every student action |
| mdl_message_read | Survey of sent messages |
| mdl_question | Question base for the quizzes |
| mdl_quiz | with answers |
| mdl_user | Quiz questions, answers |
| mdl_enrolments | All users information |
| mdl_user_lastaccess | Enrolled users in a certain course |
| | participant's last course access |

Data preprocessing provides data to be transformed in relevant format for data mining to be applied. Before using data mining it is important to identify the necessary user, the course he is enrolled etc [9], [10].

For example, to show the number of resources (figure 3) there is created new i.e. warehouse that is linked with the original Moodle database and it is filled with data in sertain time period.




Слика 3. Страница за ресурси во контролната табла
Figure 3. Resources page in the dashboard

To get certain reports it is important to analyze several tables from the database so that a summary of the system activities can be provided, to get user-friendly results scheme. That is the aim of this research, with which we consider that system users (all within their own role) will get view in their activities.

## 3. Data mining of analyzed data

Besides analyzing the data in the Moodle database, it is very important how the data will be grouped in order to achieve the required effect.
For that purpose we hold up on data mining and we use some of the known techniques that can provide us all necessary information and data in the effort to give the teacher simplified view on the processed knowledge.

In e-learning systems clustering can be useful for finding similar characteristics students clusters, revealing the user conduct and grouping the students into several groups: students who are active in the system, discuss in forums, send homework, spend some time in the system in checking different contents etc. [6].

In this research we will divide students into three clusters as follows: cluster 0 (inactive), cluster 1 (very active), and cluster 2 (active course participants). Cluster 0 is characterized by students who haven't sent homework, have read only few messages, took only few quizzes and spent very little time in checking the resources, activities and forum participation. Cluster 1 is characterized by students who have sent at least one message in the forum, have read at least three messages, have passed successfully at least half of the quizzes and have finished less than half of them unsuccessfully and have high score and grades. Cluster 2 is characterized by students who have lower score than students in

cluster 1 and more than the students in cluster 0. In this way the teacher can use these information so that he can divide the students into groups of different type of students for example at least one student from cluster 1 and students from the other clusters or a group of students from cluster 1 who would work on problem assignments of higher degree than the others [6], [12].

Classification of participants is used to discover potential students with similar characteristics for a definite specific pedagogical strategy, to predict the final results for a group of students, even to identify the students who need motivation to get better results.

We divide the students into bad, good and excellent by generating decision trees that involve certain classification rules. Our goal is to classify students in different groups depending on their activity in Moodle. Table 2 represents the knowledge by decision tree with if-else rules. This process goes on until all data are classified perfectly or we run out of attributes. Students with lower number of passed quizzes are classified as weak students, students with bigger number of quizzes are classified as excellent and the students with an average number of quizzes as good and of course taking into account the total time spent on resources and activities, the number of sent homework assignments etc. [6], [9], [11].

Табела 2. Множество правила генерирани од одлучувачко дрво
Table 2. Rule set generated by Decision Tree

```
if(n_quiz=low) then mark=bad
else if(n_quiz=medium) then {
      if(total_time=low) then {
           if(view_resource=low) then mark=bad
                else if view_resource =medium) then {
                     if(forum_post=low) then mark=bad
                          else if(view_resource=medium) then {
                               if(total_assigments=high) then
mark=good
                                    else if(overall_core=high) then
mark=excellent
}
       else if(total_time =medium) then {
            if(view_resource=low) then mark=bad
                 else if(view_resource=medium) then mark=good
                      else if(view_resource=high) then
mark=excellent
                           if(overall_score=good) then
                                if(forum_post==good) then
                                     mark=excellent
            }
```

Teachers can use this information from these rules to get an overview of the course activity and the classification of the course participants. For example, it is obvious that the main discriminator in this case are the successfully realized

quizzes, but there are also other decisive factors that would help the teacher to decide about the type of activities he would use in the future, to decide which activities not to use in the future due to the bad results or their insufficient attractiveness among the other activities and resources. The teacher can and decide which of the students have difficulties in learning, which topics are more difficult to overcome, so that he can react on time.

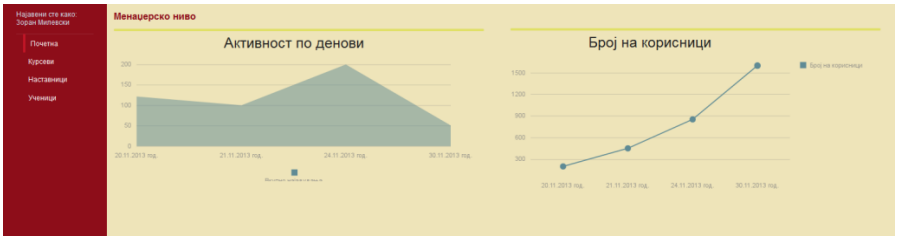
The last mining technigue that will be described in this paper is regresion. It is the easiest technique to use, but is also probably the least powerful. Regresion is a data mining function that predicts a number. A regression task begins with a data set in which the target values are known. In the model build (training) process, a regression algorithm estimates the value of the target as a function of the predictors for each case in the build data. These relationships between predictors and target are summarized in a model, which can then be applied to a different data set in which the target values are unknown [19]. For example, in our case study, using regresion we can predict the students grades, based on observed data for many students activities over a period of time.

For our dashboard, different roles of users (manager, administrator, teacher, user), display different reports gained with the mining techniques.

### a. Manager level acquired data

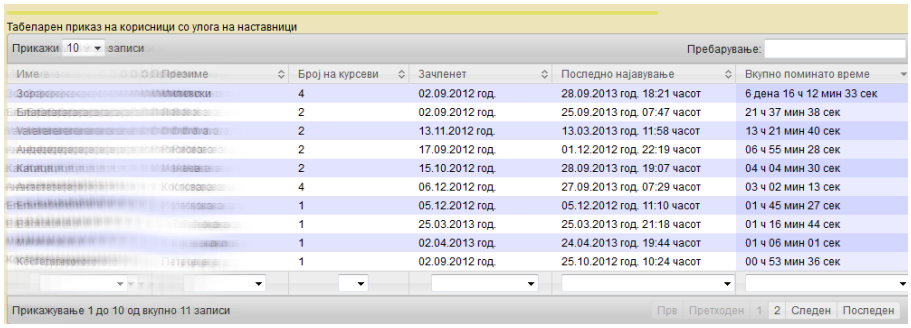
Manager level enables manager role data survey and getting reports that enable to follow the activity of all the participants in the system, number of courses, set materials and resources, realized quizzes etc.

After logging as role manager, the home page (figure 4) gives the manager quick view of the activity of the users and review of the number of the participants in the courses.




Слика 4. Почетен поглед по најавување во улога на менаџер
Figure 4. First view after login in the role manager

The menager can look over all system registered users, users that have confirmed their registration and those that haven’t confirmed the registration, whereas in the submenu user activities he can see the last system access of the users, shown for a certain date. An example for how much time the participants (teachers/students) spent in the system is given at figure 5.




Слика 5. Поминато време во системот од извештајот за корисничка активност

Figure 5. Time spent in the system from the user activity report

The course menu schemes a list of courses in categories and a total number of, list of all courses and an opportunity to choose a certain course. After a course is chosen a view of the number of discussions without content display is acquired, but a view of the activities of the discussion participants, number of started topics, number of theme answers. A list of all resources and access to all of them with additional details for most visited and least visited resource. A survey of all the activities such as homework and its assessment with a list of students with highest and lowest score is also available. This part also offers a survey of all questionnaires and their results as well as a possibility to print the questionnaire results.

User portfolio enables individual course users' data preview, as well as table preview for all the course participants by viewing the activity (inactive, active, very active), division in categories according to the assessment into bad, good and excellent, prediction of whether they will complete the course successfully or not and complete summary.

The user portfolio view gives contrastive analysis of a student's results in several courses and all the activities that characterize the student.

### b. Administrator level acquired data

The administrator is the user of the application who has all the privileges. The application administrator has the overall view of the user from the manager level. There is an additional opportunity to give tasks in precisely defined period of time (when it is expected not to have any activities in the system) to keep the data in the new database, as well as to archive the previous preview, because previously all overviews through cancel procedures are read from the Moodle database that is linked to the new database, the warehouse. Besides that the administrator has the right to register new users of the system from external bases for example excel documents.

### c. Teacher level acquired data

The teacher has a similar role in the application to the manager, with the little difference that the manager has an overview of all courses and all users of the application, whereas the user with the teacher's role can view only the data that refers to the courses that he has created and the system users that are participants only in his courses.

Additionally the teacher has better view of the section that refers to the results of the student's homework, quizzes and their activity in the system.

The teacher can see which of the questions the participants have been answered correctly and which not so that he can direct the participants to find out the correct answers in the following lessons. For example, in the quiz section, to be able to see the results according to the standard Moodle report several steps are required in order to get a table view, so the application enables getting view with only one click, automatic sorting of the results and a percentage representation of the score as well as another column with a grade in form of letter.

In the section that refers to the comparison of the results and the activity of the students in the other quizzes, the teacher can see only the analyses of the activities and the processed data only for the courses that he has created, but not for all the other quizzes in the e-learning system.

### d. User level acquired data

User with the user level role in the application is in fact the student who participates in one or several courses of the e-learning system Moodle. The user has a username and a password as in the profile he has created on the e-learning system Moodle itself. The data that the user can see is from the user portfolio of the manager and the teacher and refer only to the logged user. In this way the user can view in which subject he participates, to see his activity, results, comparison of the activities in different courses etc.

Besides these views the user gets certain suggestions by the teacher for the necessity to pay more attention and to be more active in the working obligations within the course in order to motivate him to accomplish better final results.

## 4. Conclusion

This work gives analyses of the data from the database in the e-learning system Moodle and gives survey of the results from the data mining with the use of several techniques applied on the application that offers several levels of approach. It is necessary to integrate the data mining tools in the e-learning environments which is the goal of this research, because in this way all these data mining techniques will be applied in a single application and the feedback and the acquired results will be directly applied on the e-learning environments [16].

Here are several data mining techniques that can be used for acquiring processed results and reports in the process of learning, and they are not complicated to be used by the teachers. That is why this approach of creating

dashboard – web based application, which is user-friendly and give better control when it comes to larger groups of students when the standard reports reduce the control clarity and the ability to evaluate their results at the end of the course [3], [5], [16].

Nowadays, data mining tools are too complex to be used by the educators and their futures go beyond the scope of what educator might to do. By creating a dashboard that would communicate with the e-learning system Moodle, the teachers can easily evaluate web activity in order to get more objective feedback, and find out more about students capability in successfully passing the exam. Also this dasboard will directly solve the teachers problems in supplying support in dealing with various kind of algorithms. It could also be oriented towards the academics and administrators responsible in order to obtain parameters about how to improve site efficiency and adapt it to the behavior of their users, have measures about how to better organize institutional resources (human and material) and their educational offer, enhance educational program offers, etc.

**Литература (References)**

[1] Ramaswami M., and Bhaskaran R.: A Study on Feature Selection Techniques in Educational Data Mining”, vol.1, Journal Of Computing, ISSN:2151-9617, https://sites.google.com/site/journalofcomputing (December 2009)

[2] Elatia S., Ipperciel D., Hammad A.:Implications and Challenges to Using Data Mining in Educational Research in the Canadian Context, Canadian journal Of Education, pp. 101--119 (2012)

[3] Baradwaj B. K., Pal S.:Mining Educational Data to Analyze Students’ Performance, (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 2, no. 6 (2011)

[4] Yadav S. K., Bharadwaj B., Pal S.:Mining Education Data to Predict Student’s Retention - A comparative Study, (IJCSIS) International Journal of Computer Science and Information Security, vol. 10, no. 2 (2012)

[5] Cocea M., Weibelzahl S.: Disengagement Detection in Online Learning - Validation Studies and Perspectives, IEEE transactions on learnin technologies, vol. 4, no. 2 (April-June 2011)

[6] Romero C., Ventura S., García E.:Data mining in course management systems - Moodle case study and tutorial

[7] BAKER R.S.J.D., YACEF K.:The State of Educational Data Mining in 2009 - Review and Future Visions

[8] Retalis S., Papasalouros A., Psaromiligkos Y., Siscos S., Kargidis T.: Towards Networked Learning Analytics – A concept and a tool

[9] Romero C., Ventura S., Espejo P. G. and Hervás C.: Data Mining Algorithms to Classify Students, The 1st International Conference on

Educational Data Mining, Montréal, Québec, Canada, pp. 8-18 (June 20-21, 2008)

[10] Yadav S. K., Pal S.: Data Mining - A Prediction for Performance Improvement of Engineering Students using Classification, World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 vol. 2, no. 2, pp. 51-56 (2012)

[11] Dash M., Liu H.:Feature Selection for Classification, An International Journal of Intelligent Data Analysis, vol. 1, no. 3,2006, pp. 131-156 (1997)

[12] Chen G., Liu C., Ou K., Liu B.: Discovering decision knowledge from web log portfolio for managing classroom processes by applying decision tree and data cube technology, Journal of Educational Computing Research, pp. 305–332 (2000)

[13] Anozie N., Junker B.W.: Predicting end-of-year accountability assessment scores from monthly student records in an online tutoring system, Educational Data Mining AAAI Workshop, pp. 1-6, California, USA (2006)

[14] Moodle org. LMS Moodle official site. web. 11 Apr. 2013, http://moodle.org

[15] High school Dobri Daskalov, E-learning Moodle, Kavadarci, R. of Macedonia: n.p., 2009. web. 11 Apr. 2013, http://moodle.dobridaskalov.edu.mk

[16] Darrell M. W.:Big Data for Education - Data Mining, Data Analytics, and Web Dashboards, U.S. Department of Education Office of Educational Technology, Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics”, pp. 36 (2012)

[17] Oracle. Oracle Data Mining Concepts. Release 1 (11.1), Oracle Data Mining Concepts , web.7 Sept. 2013

# ПРЕГЛЕД НА ТЕХНИКИ ЗА ПРЕПОЗНАВАЊЕ НА ЛИК ОД ВИДЕО

Ана Љуботенска[1], Игор Стојановиќ[2]

[1] Факултет за информатика, Универзитет „Гоце Делчев“ - Штип
(ana.ljubotenska, igor.stojanovik)@ugd.edu.mk

**Апстракт**

Во областа на анализирање на слики, значаен проблем претставува препознавањето на лик чија основна цел е да се открие или потврди идентитетот на личност од внесена слика, ако се дадени слика од лик како влезен податок и база со слики од познати ликови. Оваа проблематика стана особено актуелна во последните години, пред сè поради големата примена што ја има во различни домени, како на пример во биометриската верификација. Техниките кои се користат за оваа цел се класифицирани во три групи, во зависност од методологијата за добивање на податоците за ликот: методи кои обработуваат видео и аудио секвенци (аудиовизуелно препознавање на лик), интензитет на слика или други клучни податоци, како што се инфрацрвена слика, 3Д или 2Д податоци. Методологиите можат да се комбинираат, така што ќе се работи за бимодално препознавање на лик или мултимодално препознавање. Фокусот во овој труд е кон тоа како да се комбинираат различни биометриски карактеристики за биометриската верификација за да се направи посигурно препознавањето на лик. Главната идеја е да се направи преглед и споредба на перформансите на клучните техники кои се користат за препознавање на лик од видео, укажувајќи на нивните основни карактеристики и предности, со што овој труд ќе им послужи на авторите како основа за понатамошни истражувања и продлабочувања во оваа област.

**Клучни зборови:** *биометриска идентификација, препознавање на лик, препознавање на говор, видео.*

# PREVIEW OF METHODS FOR IMAGE RESTORATION FROM VIDEO

Ana Ljubotenska[1], Igor Stojanovik[2]

[1]Faculty of computer science, Goce Delcev University, Stip, Macedonia
(ana.ljubotenska, igor.stojanovik)@ugd.edu.mk

**Abstract**

In the field of image processing, significant problem is face recognition. Main goal is to determine or validate person identity from the entered image, if we have image with person as input and database with recognized faces. This issue has become particularly topic current years, primarily due to large scale applications that has in various domains, such as in biometric verification. The techniques which are used for this purpose are classified in three groups, depending on the methodology for obtaining data for person: methods that process video and audio sequences (audio - visual character recognition), intensity image, or other means data such as infrared image, 3D or 2D data. Methodologies can be combined, so face recognition can be bimodal or multimodal. The focus in this paper is how to combine different biometric features for biometric verification to make face recognition safer. The main idea is to review and compare the performance of the means techniques used for face recognition from video, showing their basic features and advantages. This paper will be base of our future research in this topic.

**Kew words:** *biometric identifications, face recognition, voice recognition, video.*

## 1. Вовед

Биометриски базираните технологии се покажаа како најсоодветно решение за препознавање на личности, со што се овозможува автентикација на личности и дозволен пристап до виртуелни и физички уреди. Ова е овозможено со користење на паметни картички, токени, лозинки, пинови и слично. Лозинките и пиновите, иако се често користени, лесно можат да се забораваат, а исто така можат да бидат откриени од друго лице кое нема овластен пристап. Токените и картичките, пак, можат лесно да се изгубат или да се направат нивни дупликати. Овие недостатоци ја навестуваат потребата од пронаоѓање на друг начин за идентификација на личности. Најсоодветен начин е оној кој се базира на индивидуалните биолошки карактеристики, бидејќи тие не можат да бидат заборавени, изгубени или украдени. Биометриски базираните технологии вклучуваат идентификација што се базира на физичките и логички карактеристики на

личноста, како што се лик, глас, отпечаток од прст, дланка, уво, геометрија на рака и геометрија на прст. Исто така, вклучуваат идентификација базирана на карактеристичните однесувања на личноста, како потписот, динамиката на удар и одењето [1].

Двете основни цели на препознавањето на лик се: *идентификација*, утврдување на идентитетот на личноста преку споредба на сликата со базата на податоци и *верификација*, односно потврда дека лицето е оној кој тврди дека е, што уште се познати како совпаѓање еден на повеќе и совпаѓање еден на еден, соодветно. Препознавањето на лик може да се разгледува и како специфичен облик на препознавање на објекти. Големата разлика меѓу нив е тоа што во најчестата форма на лицата, а тоа е фронталниот поглед, поради емоционалните движења, разликата меѓу ликовите е многу суптилна [2]. Како резултат на тоа, сликите со предната страна на лице формираат многу густ кластер во просторот на слики, каде што употребата на традиционалните техники за препознавање на модел е речиси невозможна за прецизно дефинирање на разликите меѓу нив со висок степен на успех.

Препознавањето на лик како техника нуди неколку предности во однос на другите биометриски методи. На пример, личноста треба да застане на фиксно место пред камерата или да ја постави раката на соодветно место за препознавање на геометријата на дланка. Препознавањето на лик може да се врши и пасивно, во отсуство на експлицитна корисничка акција, така што сликата на ликот може да се добие од камера од страна. Оваа карактеристика е клучната предност од аспект на безбедноста. Сепак, и оваа техника се соочува со проблеми како и останатите. Кога се потпира на примероци од прст или дланка, техниката може да биде бескорисна доколку епидермното ткиво е оштетено, на пример постои модринка или пукнатина. Кај примероците со лик ситуацијата е уште посложена, поради големата чувствителност на какво било движење на телото. Потписите можат да бидат модифицирани или заборавени, а препознавањето на говор е чувствително на шум. Сепак, добрите алгоритми за препознавање на лик, како и соодветната обработка на сликите, можат да го намалат влијанието на шумот на малите варијации во осветлувањето или на ориентацијата [3]. Друга предност е што оваа техника не подлежи на напади и нема никакви ризици за здравјето на личноста.

Широкиот опсег на примена е она што оваа биометрија ја прави посебно актуелна. Примената може да биде од безбедносен аспект, на пример на аеродромите, граничните премини [4], АТМ машините, компјутерската и мрежна безбедност [5]. Освен ова, може да се примени за испитувања на базата со слики, мултимедијални настани, кај секој облик на паметните картички [6], кај електронски регистрирања, видео индексирање, судски или кривични системи или надзор, на пример на бензинска пумпа, во банка или трговски центар. Во насока на ова е проектот „Безбеден град“ за покривање со видео-надзор на територијата на градовите Скопје, Куманово и Тетово, што е од суштинско значење за полицијата. Овој проект во Македонија започна во 2012 година, за чија цел се инсталирани над 300 километри оптичка мрежа, а кога проектот ќе биде целосно завршен треба во функција да бидат над 600 камери кои ќе вршат мониторинг. Ова е доказ дека препознавањето на лик како техника се актуализира и во нашата земја, пред сè за безбедносни цели. Основните техники за препознавање на лик кај различни апликации претрпуваат модификации, а најдобри резултати се добиваат со комбинирање на препознавањето на лик со друга биометрика, на пример отпечаток на прст или говор, со што се добива бимодално т.е. мултимодално препознавање. Всушност, мултимодалното препознавање е многу поефикасно и посигурно, додека единечното препознавање е прилично ограничено.

## 2. Алгоритми за препознавање на лик со аудиовизуелен пристап

Поради тоа што техниката за препознавање на лик најмногу се користи за безбедносни цели, што вклучува препознавање на лик во реално време од секвенци на слики добиени од видеокамера, аудиовизуелниот пристап се извојува како најприменуван. Мултимодалните аудиовизуелни пристапи за препознавање на лик се користат за широк спектар на примена на технологија на говор, вклучувајќи: препознавање на личност што говори, препознавање на говор, сегментација на говор и подобрување на говор. Гаусовиот мешан модел (GMM[1]) е еден од често користените модели за аудио препознавање, кој статички ги претставува особините на секој од целните говорници. Постои еден облик на GMM наменет за целните говорници и еден универзален, модел во позадина, скратено UBM (Universal Background Model), кој се користи како почетен за секој модел кој е обучен со адаптирање на Гаусовите карактеристики. UBM се користи во текот на тестирањето како алтернативна хипотеза чиј резултат се споредува со резултатот од моделот на целниот говорник за да се создаде веројатноста на анализираниот сооднос.

Кај визуелното препознавање на лик се разгледуваат два пристапа: пристап базиран на модел и пристап што се базира на поглед. Во модел базираниот пристап се проценуваат различните аспекти на лицето, како висината и ширината на усните и служи како извор за карактеристиките на колекцијата. Алгоритмите за оваа намена се ограничени од квалитетот на проценетите карактеристики. Кај другиот пристап препознавањето се имплементира врз основа на

[1] GMM=Gaussian Mixture Modal

оригинална слика. Клучен проблем овде бил проблемот со димензионалноста, со што се јавила потреба за методи за намалување на слики со лик во типичен ниско димензионален простор. Овој предизвик го решиле Turk и Pentland [7], користејќи ја анализата на главни компоненти-PCA (акронимот на англиски), популарно позната како Eigenfaces метода, со што се постигнати значајни резултати во визуелното препознавање на лик. Добри резултати се постигнуваат и со Fisherfaces [8], што претставува линеарна дискриминантна анализа-LDA (акронимот на англиски), надополнување на Eigenfaces, каде што класите се конвексни и линеарно деливи, со што со линеарна проекција може да се намали димензионалноста. И двата метода бараат претпроцесирачка фаза, во која лицата ќе се детектираат и нормализираат.

Eigenfaces пристапот го одредува оптималниот, линеарен простор за препознавање на лица. Сите нормализирани слики се претставуваат векторски $x_n$ и се одредува значаен т.е. среден лик $x_0$, кој се одзема од сите нормализирани ликови $\mathrm{A}_n = x_n - x_0$, со што се формира матрица А. Потребно е да се пресмета ковариjансата како $S = AA^T$, чиј што вектори Φ ќе ја формираат основата на просторот на лик. Turk и Pentland алтернативно предложиле формирање на коваријанса на помалку димензионален простор $S = A^T A$, чиј што вектори Φ се множат со матрицата: $\Phi_T = A\Phi$. Ова резултира со поделнакво ефикасна основа за претставување на лица. Колоните на матрицата $\Phi_T$ формираат основа за Eigenfaces просторот на лица чиј оригинал е значајниот лик, кој се означува со Ψ. За време на тестирањето секоја нормализирана слика може да се проектира во просторот на лица со $y_n = \Phi_T(x_n - x_0)$.

Кај пристапот Fisherfaces односот меѓу класата на матрицата на растурање $S_W$ и помеѓу класата на матрица на растурање $S_b$ се пресметува според претходно опишаниот пристап. Целта е да се максимизира функцијата за поделба на просторот помеѓу класите, во однос на поделбата во класите, што се добива со решавање на $S_b x = S_W x\, \lambda$. Добиените решенија потоа можат да бидат генерирани со проектирање на векторите добиени со Eigenfaces, во просторот дефиниран од векторите од решението на Eigenfaces проблемот [9]. За разлика од аудио препознавањето, кај визуелното не постои статистички модел за претставување на целта во парадигмата на тестирање. Наместо тоа, постои Eigenfaces т.е. Fisherfaces вектор што одговара на секоја слика во испитуваната група. Последица од ова се повеќе резултати за секоја испитувана слика. За добивање на резултатите можат да се користат повеќе пристапи, на пример Евклидова метрика, Махаланобисово растојание и нормализирана корелација.

Според Chibelushi [10] и Brunelli [11], кои се меѓу првите што се занимавале со комбинирање на аудио и визуелните информации за препознавање на лица, комбинираната информација од говор и лик се пресметува според фузијата на пондерираниот збир со облик: $f = w_1 o_1 + w_2 o_2$, каде $o_1$ и $o_2$ се проценки генерирани од говорот и профилот на ликот, со соодветни тежини $w_1$ и $w_2$. Проценката одговара на веројатноста за побарување, базирана на собраните информации. Ниската проценка сугерира дека тврдењето не е точно, додека високата проценка сугерира дека тврдењето доста е веројатно дека е точно. Збирот на тежините изнесува 1, од каде што се добива обликот: $f = w_1 o_1 + (1 - w_1) o_2$.

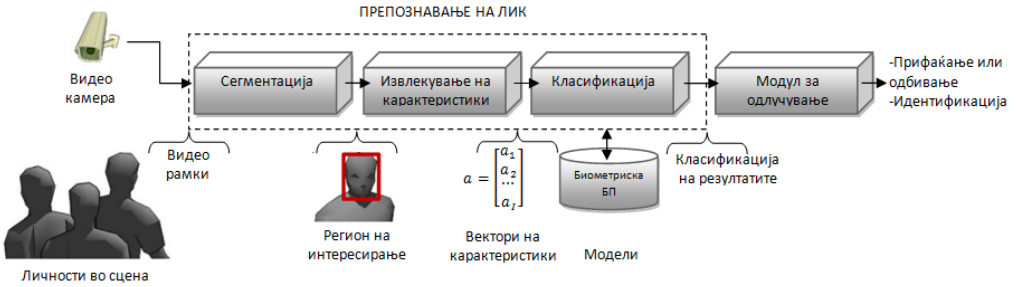
Анализите направени според ова [12] покажуваат дека кога се користи само говорот, т.е. кога $w_1$=1, се постигнува вкупна стапка на грешка EER[2] од 3,4%, а кога се користи само профилот на лик т.е. $w_1$=0 се добива вкупна стапка на грешка од 3%. Со користење на оптимална тежина и праг, вкупната стапка на грешка се намалува на 1,5%. Brunelli ги има комбинирано проценката на лик, добиена од геометриските карактеристики од статички слики со фронални ликови и говор, со пристап на пондериран производ, добивајќи $f = (o_1)^{w_1} \mathrm{x}\, o_2{}^{(1-w_1)}$ . Според овој начин, кога се користи само говор, стапката на идентификација е 51%, а со испитување само на профилот на лик, се постигнува стапка на идентификација од 92%. Со користење на оптимална тежина и праг, стапка на идентификација расте.

### 3. Препознавање на лик од видеосеквенци

Видео-базираното препознавање на лик се состои од три модули: еден за детектирање на лик, втор за негово следење и трет за препознавање [13]. Најчесто се одбираат неколку добри слики, извадени од видеото, врз кои се применува некоја од техниките за интензитет на слика, со што се определуваат регионите на интерес, па се формираат соодветни вектори на лик, според претходно опишаните приоди. Кај системите за препознавање на лица од видеосеквенци се користат дводимензионални слики т.е. видеорамки добиени од реална околина, односно тридимензионална сцена. Во поновите достигнувања од оваа област [14] авторите ги комбинираат временската и просторна информација содржани во видеосеквенците за да обезбедат високо ниво на прецизност во неограничените сцени. Речиси сите методи ги следат чекорите прикажани на слика 1. На пример, дистрибуирана сензор мрежа е предложена од Foresti и Snidaro [15] како решение на проблемот со парцијално затворање, што е застапено во динамички средини. Li и

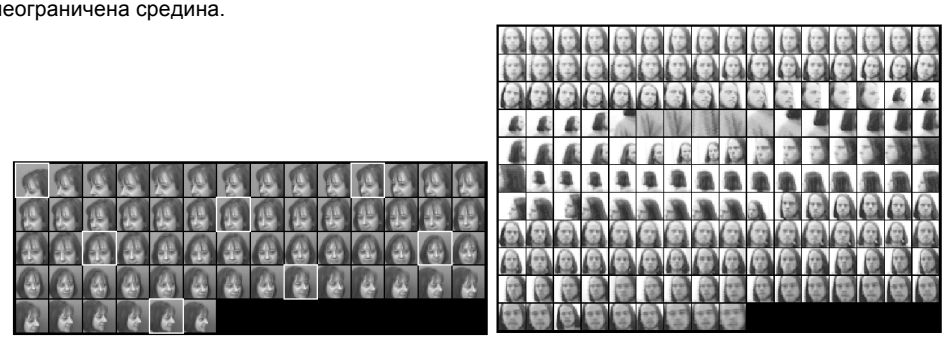
[2] EER=Equal error rate

Chellappa [16] го воведоа системот за верификација на лик што користи траектории со Габорови црти на лицето за идентификација на личности, со употреба на позадинска густина карактеризирана со движење. Majumdar и Nasiopoulos [17] предложија препознавање врз основа на слика, базирано на информацијата за боја. Mian [18] користи ненабљудуван пристап на учење за откривање на идентитетот на личноста врз база на привремено цврсто совпаѓање на деловите на видео секвенците.




**Слика 1. Генерален биометриски систем за препознавање на лик од видео**
**Извор: „An adaptive classification system for video-based face recognition“, J. F. Connolly, E. Granger, R. Sabourin, 2012**

Еден од најзначајните пристапи за препознавање на лик од видеосеквенци е оној на Howell и Buxton [19], кои развиле двослојна, хибридна RBF мрежа[3][20] за учење со употреба на карактеристиките на Гаусово филтрирање и Габорова брановидна анализа[4] за претставување на цртите на лик. Мрежата се состои од надгледуван слој, кој е од скриените до излезните единици и слој кој е без надзор, од влезот до скриените единици, каде што за секоја скриена единица, индивидуални радијални Гаусови функции го поттикнуваат ефектот на препокривање и локално синхронизирање на отворени полиња. Препознавањето на лик кај овој пристап е од видео со слаба резолуција. Тестирањата се вршат со употреба на два вида на секвенци од слики: 8 примарни секвенци, земени во релативно ограничена средина и втора секвенца, направена во понеограничена средина.

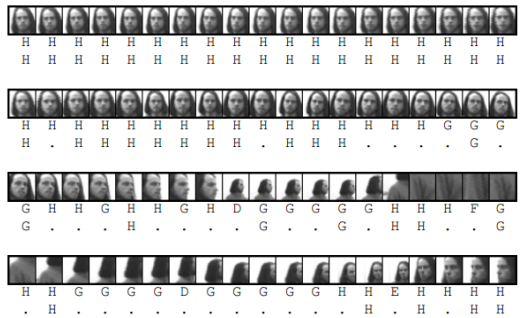


**Слика 2. Изглед на комплетна примарна и секундарна секвенца за класите Карла и Стив, пред процесирањето, а по сегментацијата, според методот на Howell и Buxton**
**Извор: „Towards Unconstrained Face Recognition from Image Sequences“, A. Jonathan Howell H. Buxton, © 1996IEEE**

Примарната секвенца со слики треба да обезбеди соодветни податоци за обука на систем со вклучен извор на тест слики, кои се состојат од едно лице кое се движи од една профилна позиција до друга, додека лицето седи на стол, со цел да се ограничи движењето на телото, во средина со сива позадина за да се ограничат и позадинските ефекти. Оваа секвенца содржи од 62 до 94 рамки. Секундарната секвенца на слики, пак, е наменета за симулирање на онлајн извор на тест слики, кои се многу повеќе променливи од примарната секвенца, за да се симулира следење во неконтролирана околина. Се состои од прилично долги секвенци на едно лице, кое се движи низ соба, со менување на позадина. Бројот на рамки е многу поголем. Понатаму се продолжува со

[3] RBF=Radial basis function, што претставува вештачка невронска мрежа, каде што основната радијална функција се користи како функција на активирање, а излезот е линеарна комбинација од основната радијална функција на влезовите и невронските параметри
[4] Специјален вид на краткотрајна Фуриева трансформација

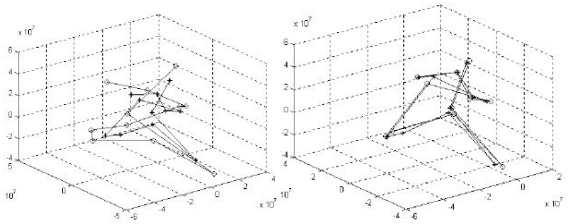
процесирање на сегментираните податоци. Се применува RBF мрежата за учење со употреба на Гаусовото филтрирање и Габоровата брановидна анализа за примарната и секундарна секвенца и се споредуваат добиените резултати. На слика 3 е прикажан излезот за дел од Габоровото процесирање на секундарната секвенца за класа Стив.



**Слика 3. Излез од процесирањето со Габорова анализа на секундарната секвенца на класата Стив**
**Извор: „Towards Unconstrained Face Recognition from Image Sequences“,A. Jonathan Howell H. Buxton, © 1996IEEE**

Горниот ред на букви го покажува првичниот излез, а понискиот ред го покажува излезот по отфрлањето на вредностите со ниска доверба, т.е. тие кои се далеку од оригиналните слики во базата. Карактерот '.' укажува на отфрлени вредност.

Во оваа област истражуваат и Biuk и Loncaric [21] од Универзитетот во Загреб. Нивните истражувања се однесуваат на секвенци од слики каде што позицијата на ликот се менува од -90 до 90 степени. Секвенците се проектираат во простор, генериран според Eigenfaces методот, со цел да се добие прототип на траекторија за секоја позната личност. Секоја точка од траекторијата одговара на еден агол на поглед на една иста личност. За време на фазата на препознавање, траекторијата на непознатиот лик се споредува со траекториите-прототипови, за да се идентификува личноста. Целата математичка позадина е според Eigenfaces методот. Овој тест-систем има база која се состои од 28 личности, со 11 рамки за секој, иако Biuk и Loncaric добри резултати добиле и со користење на најмалку 4 рамки.



**Слика 4. а) Приказ на траекториите за 2 личности претставени со 3 компоненти во 11 различни агли; б) Приказ на траекториите за 2 секвенци за иста личност со 3 компоненти, според методот на Biuk и Loncaric**
**Извор: „Face recognition from multi-pose image sequence“, Z. Biuk, S. Loncaric, ©2001 IEEE**

Постојат уште неколку понови пристапи во кои е употребена парадигмата *видео во видео* во која информација од секвенца на рамки од видеосегмент е поврзана со една личност. Овој поим подразбира следење и временска анализа на видеосеквенца и препознавање на одредени проблеми, но оваа проблематика сè уште е предмет на тековните истражувања кои ги испитуваат разните варијации во ориентацијата и изразот на лице [22].

## 4. Предности и недостатоци

Техниките за аудиовизуелно препознавање на лик, како пример за системи за динамичко препознавање, имаат повеќе предности, но и недостатоци во однос на статичките. Во целина поголем е бројот на недостатоци, бидејќи тие обично се попречени со слаб квалитет на слики, иако квалитетот на сликата може да се зголеми преку искористување на техники со суперрезолуција. Други недостатоци се преполните средини, кои го отежнуваат откривањето на лик [23], присуството на повеќе од едно лице во слика, голема количина на податоци за обработка [24], но и тоа што

сликата со лик може да биде со помала големина од онаа што е потребна за системот за препознавање на лик.

Сепак, динамичките шеми имаат и предности во однос на статичките техники. Огромното изобилство на податоци овозможува системот за препознавање да одбере рамка со најдобра можна слика и да ги отфрли неповолните. Видеото обезбедува временски континуитет, па информациите од неколку рамки може да се комбинираат за подобрување на перформансите за препознавање. Покрај тоа, видео овозможува следење на слики од лица кои имаат варијации во изразот на лицето и позите, што резултира со подобрено препознавање на лик [25].

## 5. Заклучок

Препознавањето на лик е предизвик, но и тежок проблем во областа на анализирање на слики и компјутерска визија, на што е посветено големо внимание, поради големата апликација во различни домени. Истражувањата енергично се спроведуваат изминатите четири децении, но и покрај тоа што е направен голем напредок, добиени се охрабрувачки резултати и актуелните системи за препознавање на лик достигнаа одреден степен на зрелост кога работат под ограничени услови, сепак, тие се далеку од постигнување на идеалот да можат соодветно да се извршуваат во различни ситуации кои се среќаваат со употребата на овие техники во реалниот живот. Крајната цел на истражувачите е да се овозможи компјутерите да го поддржуваат човечкиот визуелен систем. Во контекст на ова е и ставот на Torres [25], кој смета дека за постигнување на крајната цел:

*„Потребен е силен и координиран напор помеѓу компјутерската визија, процесирањето на сигнали, психофизиката и невронауките“.*

Целта на трудот беше на едно место да ги собере позначајните презентирани методи за препознавање на лик од видео, за да се разбере суштината и потребата од визуелно препознавање и да се овозможи база за понатамошни истражувања во оваа област. Бидејќи истражувањето беше насочено кон препознавање на лик од видео, првично беа објаснети PCA и LDA, односно Fisherfaces и Eigenfaces методите, како елементарни. Истражувањето е заокружено со посочување на предностите и недостатоците на овој пристап и идните тенденции на оваа наука.

**6. Референци**

[1] K. Kim, "Intelligent Immigration Control System by Using Passport Recognition and Face Verification," in International Symposium on Neural Networks. Chongqing, China, 2005, pp.147-156.

[2] P. Melin and O. Castillo, "Human Recognition using Face, Fingerprint and Voice," in Hybrid Intelligent Systems for Pattern Recognition Using Soft Computing, Vol.172, Studies in Fuzziness and Soft Computing: Springer Berlin / Heidelberg, 2005, pp.140-156.

[3] Tim Cootes, Chris Taylor, Hzizhuang Kang, Vladimir Petrovic, “Modeling Facial Shape and Appearance”, Handbook of Race Recognition, Springer, 2005.

[4] J. N. K. Liu, M. Wang, and B. Feng, "iBotGuard: an Internet-based intelligent robot security system using invariant face recognition against intruder," IEEE Transactions on Systems Man And Cybernetics Part C-Applications And Reviews, Vol.35, pp.97-105, 2005.

[5] H. Moon, "Biometrics Person Authentication Using Projection-Based Face Recognition System in Verification Scenario," in International Conference on Bioinformatics and its Applications. Hong Kong, China, 2004, pp.200-210.

[6] P. J. Phillips, H. Moon, P. J. Rauss, and S. A. Rizvi, "The FERET Evaluation Methodology for Face Recognition Algorithms," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.22, pp.1090-1104, 2000.

[7] M. Turk and A. Pentland, “Eigenfaces for Recognition”, Journal of Cognitive Neurosciences, 3(1): 71-86, 1991.

[8] M. H. Yang, “Kernel Eigenfaces vs. Kernel Fisherfaces: Face Recognition using Kernel Methods, Proc. Of IEEE Int. Conf. on Face and Gesture Recognition, pp 2150220, Washington DC USA, May 2002.

[9] K. Brady, M. Brandstein, T. Quatieri, B.Dunn, “AN EVALUATION OF AUDIO-VISUAL PERSON RECOGNITION ON THE XM2VTS CORPUS USING THE LAUSANNE PROTOCOLS”, MIT Lincoln Laboratory, 244 Wood St., Lexington MA 02420-9185,2006

[10] C. C Chibelushi, F, Deravi and J. S. Mason, "Voice and Facial Image Integration for Speaker Recognition", IEEE Intemational Symposium Multimedia Technologies and Future Applications, Southampton, UK, 1993.

[11] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Trans. Pattern Anal. Machine Intell. 10 (1995) 955–965.

[12] R. Brunelli, D. Falavigna, T. Poggio and L. Stringa, "Automatic Person Recognition Using Acoustic and Geometric Features", Machine Vision & Applications, Vol. 8, 1995, pp. 317-325.

[13] L. Torres, L. Lorente, and J. Vilà, "Face recognition using self-eigenfaces," in International Symposium on Image/Video Communications Over Fixed and Mobile Networks. Rabat, Morocco, 2000, pp.44-47.

[14] J. F. Connolly, E. Granger , R. Sabourin, „An adaptive classification system for video-based face recognition“, Information Sciences 192 (2012) 50–70

[15] G.L. Foresti, L. Snidaro, A distributed sensor network for video surveillance of outdoor environments, in: IEEE Proc. on the Int’l Conf. on Image Processing, Rochester, USA, 2002.

[16] B. Li, R. Chellappa, Gabor attributes tracking for face verification, in: IEEE Proc. on the Int’l Conf. on Image Processing, 2001

[17] A. Majumdar, P. Nasiopoulos, Frontal face recognition from video, in: Advances in Visual Computing, Las Vegas, USA, 2008

[18] A. Mian, Unsupervised learning from local features for video-based face recognition, in: IEEE International Conference on Automatic Face and Gesture Recognition, 2008.

[19] A. Howell and H. Buxton, "Towards unconstrained face recognition from image sequences," in Proceedings of the Second IEEE International Conference on Automatic Face and Gesture Recognition, 1996, pp.2-7.

[20] B. Li and H. Yin, "Face Recognition Using RBF Neural Networks and Wavelet Transform," in Advances in Neural Networks – ISNN 2005, vol.3497, Lecture Notes in Computer Science: Springer Berlin / Heidelberg, 2005, pp.105-111.

[21] Z. Biuk and S. Loncaric, "Face recognition from multi-pose image sequence" in Proceedings of 2nd IEEE R8-EURASIP Int'l Symposium on Image and Signal Processing and Analysis. Pula, Croatia, 2001, pp.319-324.

[22] L. Rowden, B. Klare, J. Klontz, A. K. Jain, „Video-to-Video Face Matching: Establishing a Baseline for Unconstrained Face Recognition“,Michigan State University, East Lansing, MI, U.S.A., 2013

[23] M. H. Yang, D. Kriegman, and N. Ahuja, "Detecting faces in images: a survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.24, pp.34-58, 2002.

[24] Z. Liposcak and S. Loncaric, "A scale-space approach to face recognition from profiles," in Proceedings of the 8th International Conference on ComputerAnalysis of Images and Patterns, Vol. 1689, Lecture Notes In Computer Science. London, UK: Springer-Verlag, 1999, pp.243-250.

[25] L. Torres, "Is there any hope for face recognition?" in Proc. of the 5th International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS 2004). Lisboa, Portugal, 2004.

# ИНТЕРНЕТ АПЛИКАЦИЈА ЗА ОБРАБОТКА НА СЛИКИ СО МАТРИЧНИ ТРАНСФОРМАЦИИ

Иван Стојанов[1], Ана Љуботенска[1], Игор Стојановиќ[1], Зоран Здравев[1]

[1]Факултет за информатика, Универзитет „Гоце Делчев“ - Штип
(ivan.stojanov, ana.ljubotenska, igor.stojanovik, zoran,zdravev)@ugd.edu.mk

**Апстракт**

Дигиталните слики се создаваат за да прикажуваат или зачувуваат корисни информации, но поради големиот број недостатоци што постојат при процесот на нивна обработка, снимената слика секогаш претставува деградирана верзија на оригиналот. Затоа, потребата од сигурен метод за нивна обработка е и повеќе од неопходна. Од друга страна, софтверот со отворен код нуди низа предности. Тој е достапен за секого и секој може да го анализа, надградува и ажурира, со цел да се сподели поквалитетно решение со заедницата и понатамошно искористување на истото за лични или општествени потреби. Дозволата за пристап која ја има пошироката јавност, претставува појдовна точка на развојот на кодот, која е проследена со континуирано подобрување на структурата и функционалностите на истиот. Токму споменатите предности на софтверот со отворен код, како и потребата од интернет апликација за обработка на слики, се основната мотивација за овој труд. Нашата работа ќе биде насочена кон развивање на веб-апликација која ќе врши матрични манипулации и истата ќе ја имплементираме како проект со отворен код. Применливоста на апликацијата ќе биде насочена кон обработката на слики. Реставрацијата и одмаглувањето, како значајни процеси при обработката на слики, ќе се вршат со матрични трансформации во позадина. Поради актуелноста на оваа проблематика, се очекува готовата апликација да биде применлива, а добиените резултати користени за понатамошни истражувања од областа обработка на слики, како на нас, така и на други истражувачи, чии истражувања се во оваа област.

**Клучни зборови:** *веб-апликација, обработка на слики, операции со матрици, замаглување, реставрација на слики, PHP програмирање, MySQL системи.*

## 1. Вовед

Во денешното современо општество дигиталните медиуми ги заменија традиционалните аналогни медиуми, што е разбирливо живеејќи во ера на информации, каде што билиони битови податоци се создаваат во секој дел од секундата. Дигиталните слики се еден од најчестите видови на дигитални облици денес. Затоа и обработката на дигиталните слики е проблем од клучно значење. Под дигитална обработка на слики се подразбираат повеќе методи за нивна обработка со помош на компјутер.

Значаен дел од областа на обработка на слики претставува реставрацијата на слики, што уште се нарекува и одмаглување на слики или деконволуција. Таа се занимава со реконструкција, односно проценка на слики кои имаат замаглување или шум. Реставрацијата на слика се обидува да изврши операција врз сликата која е инверзна на несовршеностите појавени при системот на нејзино форматирање, како на пример шумот. При користењето на методи за реставрација на слика се претпоставува дека карактеристиките на системот на деградирање и шум се познати приори, иако во практични ситуации не секогаш може да се добие оваа информација директно од процесот на формирање на сликата [4]. Изворот на слика може да биде од различен вид, па поради тоа најдобро е при обработката на слики истите да се прикажат во матричен облик.

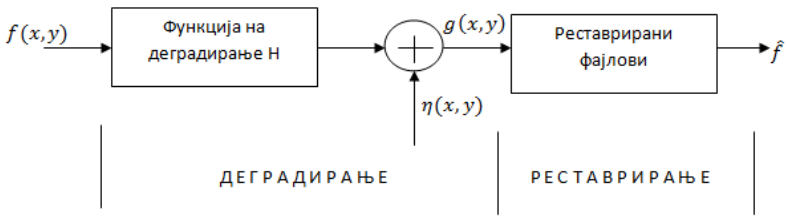
Како појдовна точка за развој на проектот беше анализата на литература со слична тематика [1,2,3] од која е преземена основата на овој проект. Идејата за изведба на начините на кои се внесуваат вредностите на сликите како елементи на матрици, заедно со другите функционалности за обработка на слики, се добиени преку анализа на споменатата литература. Имплементирањето на апликацијата за обработка на слики преку матрици ќе биде со користење на софтвер со отворен код, поради неговите предности и можноста за постојано надградување, што придонесуваат ваквите проекти да се усовршуваат во форма каква би била најприфатлива. Со давањето на дозвола за пристап до изворниот код на проектот се отвора можност за добивање на повратни информации од поширокота маса, со што ќе се добие фокус кон тоа што треба да се поправи и усоврши, за преку имплементација на најдобрите решенија, да се одговори на потребите.

За постигнување на целта на овој труд се користат техники со отворен код [5,6], како што се скрипт-јазикот PHP и системот за управување на релациони бази со податоци MySQL. Крајниот продукт во форма на веб-апликација ќе ги соедини сите концепти од линеарната алгебра кои се поврзани со манипулациите кои може да се извршуваат врз матрици во обработката на слики, конкретно објаснети подолу. Имплементирани во проектот, овие концепти ќе му овозможат на корисникот на едно место да може да ги зададе матриците како влезни параметри и истовремено да има пристап до еден широк спектар на операции од каде што со неколку кликови би се дефинирала манипулацијата што треба да се изврши врз внесените матрици, односно слики и со тоа да се добие соодветен краен резултат кој веднаш ќе се презентира на корисникот. Начинот на кој е постигната дефинираната цел би бил презентиран на поширокиот аудиториум преку поставување на крајната апликација на веб, заедно со изворниот код.

## 2. Обработка на дигитални слики со матрични трансформации

Применливоста на направената апликација ќе биде разгледувана за случај каде што влезни матрици, односно операнди внесени од страна на корисникот се дигитални слики. Ова доаѓа како последица од идејата оваа апликација да ја примениме за обработка на дигитални слики, поточно за нивна реставрација. Дигиталните слики наједноставно можеме да ги дефинираме како слики претворени во бинарен формат, читлив за компјутерот кој се состои од логички 0 и 1. Сликата како податок може да

биде дефинирана како дводимензионална функција $f(x,y)$, каде што $x$ и $y$ се просторни координати. Областа на обработка на дигиталните слики се однесува на обработувањето на сликите дигитално, со помош на компјутер. Дигиталните слики се состојат од конечен број на елементи, каде што секој од нив има посебна локација и вредност и овие елементи се среќаваат под името пиксели или елементи на сликата. Трите најголеми теми во областа на обработка на слики се: реставрација на слики, подобрување на квалитетот на слики и компресија на слики [7,8]. Реставрацијата на слики за првпат станува актуелна во педесеттите години на минатиот век, а големата актуелност и денес се должи на нејзината голема примена, на пример кај сателитските слики, медицинските снимки или компјутерската графика. Основната шема на процесот на обработка на слики, односно реставрирање на слики, е дадена во продолжение:




**Слика 1. Основна шема на обработка на слика**

каде што $f(x,y)$ е оригиналната, недеградирана слика, $\eta(x,y)$ е додаден шум односно замаглување, $g(x,y)$ е деградираната слика, а $\hat{f}(x,y)$ е реставрираната слика. На процесот на реставрација му претходи процесот на деградација, кој настанува со примена на одредена функција на деградирање врз оригиналната слика, на што уште се придружува замаглување или шум. Со ова се добива деградирана слика, врз која можат да се применат одредени филтри за реставрација и како резултат да се добие реставрирана слика. Успешноста на реставрацијата зависи од тоа колку реставрираната слика е поблизу до оригиналот. Колку реставрираната слика е послична со оригиналот, толку процентот на реставрација бил поуспешен.

Всушност, сликите прикажуваат или снимаат корисни информации. Поради голем број на недостатоци кои постојат при процесот на обработување на сликите, снимената слика секогаш претставува деградирана верзија на оригиналната слика. Постојат различни начини на кои сликата може да биде деградирана, како на пример: шумот, геометриските деградации (дисторзија на врвовите), осветлувањето или несовршености на боја (на пример сатурација) и замаглувањето [9]. Замаглувањето, како најчест причинител на деградација, е форма на намалување на пропусниот опсег на идеалната слика, што се должи на несовршености при формирањето на сликата. Најчесто се предизвикува од релативно моторно движење меѓу камерата и оригиналната сцена, оптички систем кој е надвор од фокусот или атмосферски турбуленции.

### *2.1. Математички модел за обработка на дигитални слики со матрични трансформации*

Во позадина на интерфејсот на апликацијата стојат алгоритми за реставрирање на слики, кои се повикуваат на основните концепти од линеарната алгебра, кои се однесуваат на манипулациите кои може да се извршуваат врз матрици при реставрирањето на слики [10]. Замаглувањето на слика делува како точка на ширење на функцијата, што се означува со $h(x,y)$. Методите кои се користат за реставрирање на слика спаѓаат во групата на линеарни, просторно независни филтри за реставрирање. Притоа се претпоставува дека статистичките својства на сликата не се менуваат просторно. Овие претпоставки на моделирање математички можат да се формулираат така што ќе претпоставиме дека ако $f(x,y)$ е оригиналната, просторно дискретна слика, која не подлежи на замаглување и шум, тогаш снимената слика $g(x,y)$ се моделира со:

$$g(x,y) = h(x,y) * f(x,y) = \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{M-1} h(k_1,k_2) * f(x-k_1, y-k_2)$$

На овој начин се прави проценка на идеалната слика, во случај кога се дадени само деградираната слика и функцијата на замаглување [11].

Ова може да се прошири за реална $H$ матрица од тип $mxn$. За неа обликот ќе биде:

$$g = Hf, g \in \mathbb{R}^m; f \in \mathbb{R}^n; H \in \mathbb{R}^{mxn}$$

Со ова се опишува недетерминистички систем од $m$ истовремени равенства, кои се вршат според горната формула, по едно за секој елемент од векторот $g$ и $n$ непознати, по едно за секој елемент од векторот $f$. Притоа бројот на непознати $n$ се пресметува според $n = m + l - 1$, каде што параметарот $l$ означува хоризонтално, линеарно замаглување, предизвикано од движење, изразено во пиксели. При реставрацијата на слика, која е замаглена од релативно моторно движење, резултатот се состои од решавање на недетерминистички систем, според последното равенство. Во такви услови, замаглената слика се опишува матрично со:

$$\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_m \end{bmatrix} = \begin{bmatrix} h_1 & \cdots & h_l & 0 & 0 & 0 & 0 \\ 0 & h_1 & \cdots & h_l & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & h_1 & \cdots & h_l \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix}$$

Елементите на матрицата $H$ се дефинирани како: $h_i = 1/l$, за секое $i = 1,2,3 \ldots l$. Целта е да се направи проценка на оригиналниот ред со помош на редовите од f (содржан во векторот $\mathrm{f}^{\mathrm{T}}$), според секој ред од матрицата на замаглената слика g (содржана во векторот $\mathrm{g}^{\mathrm{T}}$), под претпоставка дека карактеристиките на системот на деградирање $H$ е познат приор [9][11].

Аналогно може да се дефинира и матрица $F$ која ќе одговара на оригиналната детерминистичка слика, така што елементите на сликата ќе бидат $F_{ij}$ за $i = 1,2 \ldots r$ и за $j = 1,2 \ldots n$. Тогаш матрицата на замаглување овде ќе ја означиме со $G$ и ќе се пресметува со:

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

Матричниот облик на ова, што одговара на замаглување предизвикано од хоризонтално движење, е:

$$G = (HF^T)^T = FH^T$$

Кога се работи за процес на замаглување со вертикално движење, матричните трансформации се според следнава форма:

$$g = Hf, g \in \mathbb{R}^m; f \in \mathbb{R}^r; H \in \mathbb{R}^{mxr}$$

Овде за $r$ важи дека $r = m + l - 1$, а $l$ означува замаглување под дејство на вертикално, линеарно движење, изразено во пиксели. Соодветно, формата на матрицата $G$, што одговара на вертикално, линеарно замаглување на слика предизвикано од движење е:

$$\mathrm{G} = \mathrm{HF}, \mathrm{G} \in \mathbb{R}^{\mathrm{mxn}}; \mathrm{H} \in \mathbb{R}^{\mathrm{mxr}}; \mathrm{F} \in \mathbb{R}^{\mathrm{rxn}}$$

Овие матрични трансформации за реставрирање на замаглена слика ќе бидат имплементирани во крајното веб-решение. Благодарение на нив, се покажува како реставрацијата може да се примени врз замаглени слики, со што замаглувањето од сликите ќе се елиминира преку користење на манипулациите со матрици, според математичкиот облик, објаснет претходно. Освен овие матрични трансформации, ќе бидат овозможени и основните трансформации со матрици, како собирање, одземање, транспонирање и слично, бидејќи дел од нив ќе се користат и при реставрирањето.

3. **Функционирање на интернет апликацијата**

За развој на крајното веб решение е користен скрипт- јазикот PHP кој претставува слободен софтвер и воедно е најкористена технологија за развој на проекти со отворен код од типот на веб-апликации [12]. При извршување на одредена операција врз матрици, добиениот краен резултат заедно со покажувач кој ќе ја идентификува извршената операцијата и матриците со кои се оперира, се складираат во база со податоци на сервер, со цел при следното повикување на истите параметри резултатот да се земе директно од базата и со тоа да се редуцира времето за извршувањето на пресметките. Систем користен за управување на релациони бази со податоци е MySQL системот. [13]

Првиот чекор во процесот на пресметка е внесувањето на вредностите на елементите од матриците преку интеракција со корисникот. Вредностите на елементите може да бидат од типот на цели или децимални броеви и истите може да бидат зададени на кој било од трите начини опишани во продолжение. Првиот начин е преку задавање на димензиите на матриците и соодветно според внесените вредности на истите се пристапува кон формирање на матрична табела од текст полиња, така што вредноста во секое текст поле одговара на вредноста на еден елемент од матрицата. Вториот начин е преку директно внесување на елементите на матриците во текст полиња кои се достапни во интернет апликацијата, така што корисничкиот внес мора да исполнува одреден формат т.е. елементите во матрицата да се одделени еден од друг со карактер за празно место (blank space), додека пак преоѓањето во нов ред да се карактеризира со

знакот за премин во нов ред (Enter). Последниот начин на внесување на матриците е преку форма за прикачување на датотеки со .txt формат каде што содржината во датотеката треба да го исполнува претходно опишаниот формат како при вториот начин на задавање на вредностите на елементите во матриците.

Откако матриците се внесени во апликацијата, се пристапува кон избор на соодветна операција која ќе се изврши врз нив. На корисничкиот интерфејс ќе бидат достапни разни видови на манипулации, како што се операциите за собирање и одземање, наоѓање на производ на две матрици, транспонирање на матрица, наоѓање на инверзна матрица, пресметување на детерминанта на матрица, скалирање, степенување и разни комбинации од сите претходно споменати операции во насока за реставрирање на слика. За извршување на некои од манипулациите неопходно е да бидат внесени вредностите на елементите на две матрици, додека пак за дел од операциите доволни се вредностите на елементите и на само една матрица. За некои од операциите (комбинации од операции) како операнди ќе се јавуваат и три матрици. Изборот на посакуваната операција е чекор кој е проследен со извршување на истата.

По изборот на операцијата, а непосредно пред нејзиното извршување, се пристапува кон базата со податоци на серверот и се врши проверка дали во неа веќе постои резултатот од внесените матрици и избраната операција и како таков доколку е пронајден се зема од базата и се прикажува на корисникот без притоа да се губи време во пресметка. Ако не е пронајден резултат од пребарувањето во базата, се пристапува кон извршување на пресметка на избраната операција и добиениот резултат пред да биде презентиран на корисникот се складира во базата, за следниот пат кога ќе бидат повикани истите параметри за пресметка, да се редуцира времето за пресметка на операциите. Притоа, една матрица во базата се складира како низа од елементи така што елементите меѓусебно се разделени со запирки.

### 3.1. **Структура на базата**

Генерално, во базите со податоци ќе имаме два вида на табели во кои ќе се складираат матриците, влезни матрици – операнди внесени од страна на корисникот и врз кои ќе се извршуваат манипулациите и излезни матрици – крајни резултати добиени од пресметките на манипулациите. За влезните матрици покрај низа во која се чуваат вредностите на елементите, потребно е да бидат складирани и информација за димензијата на матрицата и единствен идентификатор по кој ќе се пристапува до матрицата кога ќе биде потребна.

**Табела 1. Структура на табелата за влезните матрици**

| ***matrices_in*** | | |
|---|---|---|
| ***id_in*** | ***elements_in*** | ***dimensions*** |
| 1 | 8,4,2,6 | 2x2 |
| 2 | 1,1,…,4,3 | 5x6 |
| 3 | 2,5,…,4,7 | 6x14 |

Кај табелите за излезните матрици, покрај низата во која се складираат вредностите на елементите и единствениот идентификатор, потребно е да се складира и поле кое ќе претставува некој вид на покажувач кон операцијата која се извршува (*operation*), колони кои содржат идентификатори кон матриците – операнди врз кои се извршуваат операциите, како и дополнителни параметри кои ќе бидат искористени за комбинации од манипулации.

**Табела 2. Структура на табелата за излезните матрици**

| ***matrices_out*** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***id_out*** | ***elements_out*** | ***operation*** | ***matrix_I*** | ***matrix_II*** | ***matrix_III*** | ***r*** | ***s*** | ***p*** | ***q*** |
| 1 | 8,2,4,6 | (A)T | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 16,8,4,12 | rA + sB | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 3 | 12,9,…,14,17 | A * B | 2 | 3 | 0 | 0 | 0 | 0 | 0 |

Воведувањето на дополнителните параметри (конкретно во случајот во табела 2) овозможува скалирање на матриците пред да се изврши некоја манипулација врз нив. Доколку корисникот сака да изврши манипулација врз матриците без тие да бидат скалирани, вредностите на параметрите ги поставува на вредност 1. Истите се искористени во повеќе формулации на изрази за манипулација. По внесување на матриците преку интерфејсот, со избор на одредена операција се генерира соодветен покажувач и истиот се бара во базата со податоци, поточно во табелата во која се складирани информациите за излезните матрици. Ако во базата се пронајдени полиња со истата операција, се пристапува кон споредба на внесените матрици преку идентификаторските броеви и во случај на пронајден резултат се враќа вредноста од *elements_out* колоната. Во спротивно, ако не е пронајден таков резултат во базата, се пристапува кон извршување на соодветните пресметки и складирање на излезниот резултат како нова колона во matrices_out табелата.

**Заклучок**

Користејќи ја претходно обработена идеја за развој на интернет апликација, со која би се извршувале матрични манипулации за обработка на слики, направивме анализа на истата и ја искористивме како основа за развој на целокупен проект. Целта на крајниот проект е имплементирање на бројни техники од линеарната алгебра во еден веб-кориснички интерфејс,

за имплементација на сработеното во процесот на обработка на слики. На почеток дадовме вовед во кој укажавме на потребата од интернет апликација за обработка на слики, поточно реставрирање на слики. Ги наведовме и предностите на проектите со отворен код, поради кои проектот што ќе го реализираме ќе го поставиме како таков. На тој начин секој ќе може да пристапува, да има увид во кодот на проектот и да го менува истиот, со цел да се добијат поефикасни крајни резултати, во смисла на развивање и имплементирање на подобри техники за редуцирање на времето потребно за пресметки или слично. Креираниот кориснички интерфејс за реставрација на слики може да се користи за понатамошни истражувања, анализи и споредби, конкретно во проблеми за одмаглување на замаглени слики. Исто така, може да се користи за проценување на ефикасноста на ваквиот начин, со матрични манипулации за реставрирање на слики, преку споредба на добиените резултати со овој пристап со резултатите добиени со некој друг пристап или, пак, да се утврди отстапувањето од математичките очекувања. Преку креираниот веб кориснички интерфејс за реставрација на слики се покажува уште и како PHP и MySQL може да се искористат за креирање на кориснички интерфејси кои можат да се користат за различни намени и притоа истите да бидат едноставни за употреба од страна на корисниците.

**Литература**

[1] M. Tasić (2011): Computation of generalized inverses using Php/MySql environment. International Journal of Computer Mathematics, Volume 88, Issue 11, 2011.

[2] S. Pepić (2012): Matricna izracunavanja u PHP/MySQL okruzenju. PhD thesis, Prirodno Matematicki Fakultet, Univerzitet u Nisu.

[3] James Theiler (2011): Sparse Matrix Transform for Hyperspectral Image Processing, IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, VOL. 5, NO. 3

[4] Bovik, A. (2009):The essential guide to image processing. London: Academic Press is an imprint of Elsevier.

[5] J. Greenspan, B. Bulger (2001):MySQL/PHP Database Applications, M&T Books: An imprint of IDG Books Worldwide, Inc., Foster City, NY, USA.

[6] H. Williams, D. Lane (2004): Web Database Applications with PHP & MySQL, 2nd Edition, O'Reilly Media, Inc., Beijing, Cambridge, Famham, KÄoln, Paris, Sebastopol, Taipei, Tokyo.

[7] Gerard Blanchet, M. C. (2006). Digital Signal and Image Processing Using MATLAB. London, UK: Hermes Science Europe Ltd.

[8] R.E., G. R. (2002). Digital image processing (2nd ed.). (N. Upper Saddle River.) Prentice Hall

[9] A. M. Tekalp, H. Kaufman, and J. W. Woods (2008): Identification of image and blur parameters for the restoration of non-causal blurs. IEEE Trans. Acoust., 34:963–972.

[10] A. K. Katsaggelos (2008): Digital Image Restoration. Springer Verlag, New York.

[11] J. Biemond, R. L. Lagendijk, and R. M. Mersereau (2009): Iterative methods for image deblurring. Proc. IEEE, 78(5):856–883.

[12] J. Meloni (2004): PHP 5, MA: Thomson Course Techology, Boston.

[13] R. Elmasri and S.B. Navathe (2003): Fundamentals of Database Systems, Addison-Wesley, 4th edition.

# УТАУТ И НЕЈЗИНАТА ПРИМЕНА ВО ОБРАЗОВНА СРЕДИНА: ПРЕГЛЕД НА СОСТОЈБАТА

Мирјана Коцалева[1], Игор Стојановиќ[2], Зоран Здравев[2]

[1] Центар за електронско учење, Универзитет „Гоце Делчев“, Штип
[2] Факултет за информатика, Универзитет „Гоце Делчев“, Штип
(mirjana.kocaleva, igor.stojanovik, zoran,zdravev)@ugd.edu.mk

**Апстракт.** Информатичките и комуникациските технологии (ИКТ) имаат потенцијал да ги подобрат сите аспекти на нашиот општествен, економски и културен живот. Воведувањето на ИКТ во универзитетите како високообразовни установи, јасно го менува начинот на кој образованието се спроведува. Но, колку што е важно воведувањето, толку е важно и прифаќањето на новите ИКТ. За таа цел ќе ја употребиме унифицираната теорија за прифаќање и употреба на технологијата (УТАУТ) со која ќе се објасни намерата на корисникот да користи информациони системи и последователно да го следи однесувањето од нивното користење.
Во трудов е опишан моделот УТАУТ и факторите кои влијаат на него, како и неговата модификација со текот на времето. Понатаму се дадени примери за примената на УТАУТ во различни средини. И на крај, во заклучокот наведуваме зошто прифаќањето на ИКТ е задолжително и што треба да се преземе за да се прифати една нова технологија.

**Клучни зборови**: *УТАУТ, клучни фактори, технологија.*

# UTAUT AND ITS APPLICATION IN AN EDUCATIONAL ENVIRONMENT: STATE-OF-THE-ART

Mirjana Kocaleva[1], Igor Stojanovik[2], Zoran Zdravev[2]

[1] E-learning Center, “Goce Delcev” University, Stip, Macedonia
[2]Faculty of computer science, “Goce Delcev University”, Stip, Macedonia
(mirjana.kocaleva, igor.stojanovik, zoran,zdravev)@ugd.edu.mk

**Abstract.** Information and communication technologies (ICT) have the potential to improve all aspects of our social, economic and cultural life. The introduction of ICT in universities as institutions of higher education is clearly changing the way in which education is conducted. But, as much as important its introduction is, the more important is the acceptance of new technologies. For that purpose, we shall use a unified theory of acceptance and use of technology (UTAUT) which will explain the user’s intention to apply information systems and subsequently to monitor the behavior of their usage.
This paper describes the UTAUT model and the factors that affect it, and its modification over time. Furthermore, examples are given for the application of UTAUT in different environments. Lastly, in the conclusion we note why the uptake of ICT is mandatory and what should be undertaken in order to accept a new technology.

**Keywords:** *UTAUT, key factors, technology.*

## 1. Introduction

The presence of communication and information technologies in organizations today has dramatically increased. Some studies suggest that, by 1980, about 50 percent of all new capital investments in organizations had been in information technology (Westland and Clark 2000). However, the technologies for improved productivity must be accepted and used by employees in organizations.

The explanation of customer acceptance of new technology is often described as one of the most researched areas in modern literature information systems (IS) (Hu et al. 1999). Studies in this area have resulted in several theoretical models, with roots in information systems, psychology and sociology (Davis et al. 1989; Taylor and Todd 1995b; Venkatesh and Davis 2000).

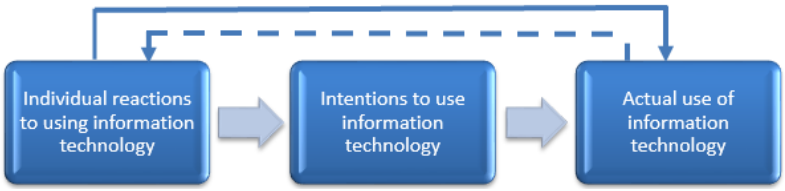



**Figure 1. Basic Concept Underlying User Acceptance Models (Venkatesh et al. 2003)**

Figure 1 presents the basic conceptual framework underlying class of models, explaining the individual acceptance of information technology that is the basis of this research (Venkatesh et al. 2003).

In this paper we describe the UTAUT theory created by Venkatesh in 2003, as well as its modified versions from 2008 and 2012 respectively, along with the factors that affect them. In the version of UTAUT of 2008 there are some changes in the schedule of the factors affecting the acceptance of new technologies and new three key factors, while the model of 2012 was extended and was intended for the consumer sector. Further, examples are given of the application of UTAUT in university environment where the surveys were conducted on university academics and their results are shown respectively in Table 2, Table 3 and Table 4, given below in part 5. Finally, in conclusion we note why the acceptance of ICT should be mandatory and which obligations should be undertaken to accept one new technology and to be used in a university environment.

## 2. Synthesis of various models and creating a unified view of user acceptance

Information technology (IT) accepts researches that gave many competing models for acceptance and use of information and communication technologies, each model with different acceptance of determinants. Each theory or model has been widely tested to predict user acceptance (Venkatesh and Davis, 2000; Thompson et al., 1991). However, no comprehensive instrument to measure the variety of perceptions of information technology innovations had existed until Venkatesh et al. (2003) attempted to review and compare the existing user acceptance models with an ultimate goal to develop a unified theory of technology acceptance by integrating every major parallel aspect of user acceptance determinants from those models.

The eight original models and theories of individual acceptance that are synthesized by Venkatesh et al. (2003) are: the Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Motivational Model (MM), Theory of Planned Behavior (TPB), Combined TAM and TPB (C-TAM-TPB), Model of PC Utilization (MPCU), Innovation Diffusion Theory (IDT) and Social Cognitive Theory (SCT). Constructs of each models and theories, including the UTAUT model, are represented in Table 1.

**Table 1: Models and Theories of Individual Acceptance (Oye et al. 2011)**

| Models and Theories | Constructs |
|---|---|
| Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975) derives from psychology to measure behavioral intention and performance. | Attitude<br>Subjective norm |
| Technology Acceptance Model (TAM) by Davis (1989) develops new scale with two specific variables to determine user acceptance of technology.<br><br>Technology Acceptance Model 2 (TAM2) by Venkatesh and Davis (2000) is adapted from TAM and includes more variables. | Perceived Usefulness<br>Perceived Ease of Use<br>Subjective Norm*<br>Experience*<br>Voluntariness*<br>Image*<br>Job Relevance*<br>Output Quality*<br>Result Demonstrability*<br>* indicates TAM2 only |

| | |
|---|---|
| Motivational Model (MM) also stems from psychology to explain behavior. Davis et al. (1992) applies this model to the technology adoption and use. | Extrinsic Motivation<br>Intrinsic Motivation |
| Theory of Planned Behavior (TPB) by Ajzen (1991) extends TRA by including one more variable to determine intention and behavior. | Attitude<br>Subjective norm<br>Perceived Behavioral Control |
| Combined TAM and TPB (C-TAM-TPB) by Taylor and Todd (1995). | Perceived Usefulness<br>Perceived Ease of Use<br>Attitude<br>Subjective norm<br>Perceived Behavioral Control |
| Model of PC Utilization (MPCU) by Thompson et al. (1991) is adjusted from the theory of attitudes and behavior by Triandis (1980) to predict PC usage behavior. | Social Factors<br>Affect<br>Perceived Consequences (Complexity, Job-Fit, Long-Term Consequences of Use)<br>Facilitating Conditions<br>Habits |
| Innovation Diffusion Theory (IDT) by Rogers (1962) is adapted to information systems innovations by Moore and Benbasat (1991). Five attributes from Rogers' model and two additional constructs are identified. | Relative Advantage*<br>Compatibility*<br>Complexity*<br>Observability*<br>Trialability*<br>Image<br>Voluntariness of Use<br>* indicates Roger's constructs. |
| Social Cognitive Theory (SCT) by Bandura (1986) is applied to information systems by Compeau and Higgins (1995) to determine the usage. | Encouragement by Others<br>Others' Use<br>Support<br>Self-Efficacy<br>Performance Outcome Expectations<br>Personal Outcome Expectations<br>Affect<br>Anxiety |
| Unified Theory of Acceptance and Use of Technology Model (UTAUT) by Venkatesh et al. (2003) integrates above theories and models to measure user intention and usage on technology | Performance Expectancy<br>Effort Expectancy<br>Attitude toward Using Technology<br>Social Influence<br>Facilitating Conditions<br>Self-Efficacy<br>Anxiety |

Researchers are faced with a choice among variety of models and know that they have to "choose" factors across models, or to choose "favorite model" and to ignore the contributions of alternative models. Thus, there is a need to review and synthesize in order to progress towards a unified view of user acceptance.

Based on the conceptual and empirical similarities across models, a single model is formulated and now a unified theory of acceptance and use of technology (UTAUT) is often used.

UTAUT was tested by using the original data and overcoming the eight individual models, and in that way it was founded. UTAUT has become a useful tool that managers need to apply in order to evaluate the probability of success while introducing a new technology and helps to understand the factors for its acceptance, in order to undertake more active interventions (such as training or marketing) targeted at users who may be less prone to adopt and use new systems (Venkatesh et al. 2003).

## 3. What is the UTAUT

UTAUT aims to explain user intention to use information systems and subsequently to monitor the behavior of their use. The theory considers that four key factors (performance expectancy, effort expectancy, social influence and facilitating conditions) are direct determinants of intention and usage behavior. Gender, age, experience and voluntary use are set to mediate between the impacts of the four key factors of the intention to use and the behavior (Venkatesh et al., 2003, Figure 2).

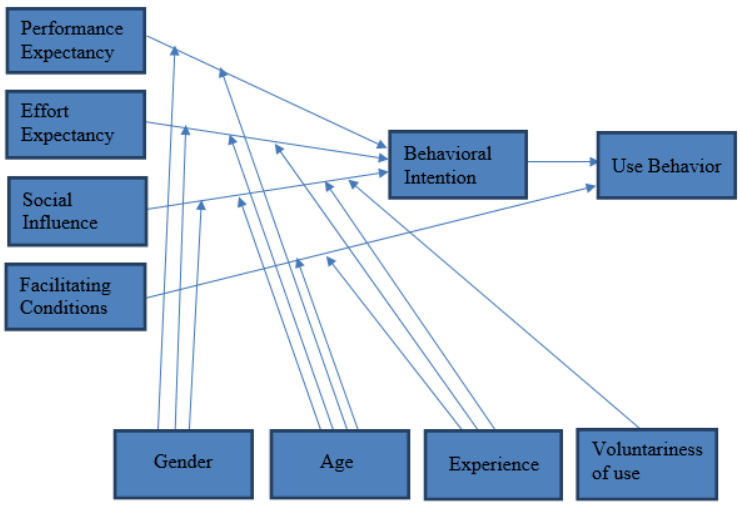
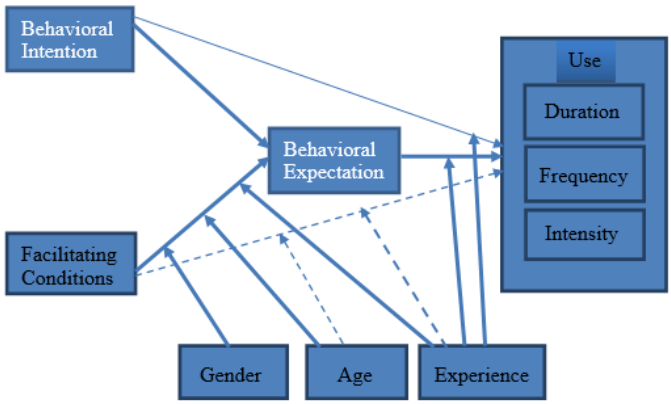



**Figure 2. Diagram of UTAUT theory (Venkatesh et al. 2003)**

## 4. Modifications of UTAUT

In 2008, Venkatesh made modification on UTAUT (Figure 3) and the new model used the behavioral intention, facilitating conditions, and behavioral expectations as predictors of the three key factors of a system that we use. The three key factors of the system here are duration, frequency and intensity. Each of these three predictors play different roles in predicting each of the three factors of the system we are using.



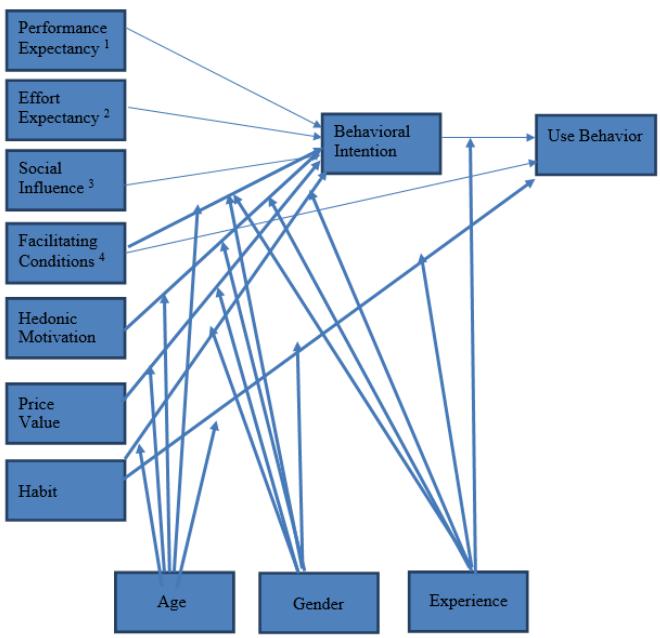

Relationship hypothesized as significant in UTAUT (Venkatesh et al. 2003), but nonsignificant here

UTAUT (Venkatesh et al. 2003) or TAM2 (Venkatesh and Davis 2000) relationships

New relationships

**Figure 3. Diagram of UTAUT theory (Venkatesh et al. 2008)**

In 2012 there was an expanding of the scope of unified theory of acceptance and use of technology (UTAUT) for acceptance and use of technology in the consumer context (Venkatesh et al.). This theory was called UTAUT 2.




1. Moderated by age and gender.
2. Moderated by age, gender and experience.
3. Moderated by age, gender and experience.
4. Effect on use behavior is moderated by age and experience.
5. New relationships are shown as darker lines.

**Figure 4. Diagram of UTAUT 2 theory (Venkatesh et al. 2012)**

UTAUT 2 included three new constructions in the previous model of UTAUT: hedonistic motivation, price value and habit. Individual differences – age, gender, and experience - were hypotheses for moderating effects of these constructs on the behavioral intention and the use of technology. Compared with the UTAUT, the proposed extensions in UTAUT 2 produced significant progress in explaining the variance in the behavioral intention (from 56 percent to 74 percent) and the use of technology (from 40 percent to 52 percent).

## 5. Application of the UTAUT

At the University of Jos Plateau, Nigeria, a pilot – study was conducted which contained 23 UTAUT survey questions and 9 demographic statements in the total amount of 32 questions (Oye et al. 2011). Respondents were university academics. The survey showed that, 57% of respondents were male and 43% were female. By using the pilot study questionnaire part of the demographic statements, they were able to give answer to the following questions (a) Was ICT mandatory or voluntary in their institution? (b) What were the greatest barriers for using ICT for academics? The following results were obtained: the majority of the full-time lecturers (89%) responded that ICT was mandatory. Question which talked about barriers of using ICT, had the majority of the respondents (42%) which said that their problem was the time; on the other hand (31%) said that the problem was the training. Others respondents (4%) said that the cost was their problem, another group (20%) said that they needed the compensation and the final group (3%) said that, it did not fit their programs. This implies that the university ICT made task more easily accomplished, thereby making them more productive. Hence result from the survey showed that 86.5% agreed with that. Therefore this determined the level of expected adoption of ICT by the respondents. Among the four UTAUT constructs, performance expectancy exerted the strongest effect. Therefore Performance expectancy was the most influential factor for the acceptance and use of ICT by the respondents.

Recommendations that were made were that, all employed teachers in Federal, State and Private universities should undertake mandatory training and retraining on ICT programs. This study used the models TAM and UTAUT to understand the teacher's behavioral intention on the acceptance and use of the technology.

**Table 2. Results from the study in Nigeria (with UTAUT constructs of reliability of above 0.70.)**

| **Results from the study in Nigeria (Number of respondents N = 100)** | | |
|---|---|---|
| **Gender** | Male | 57% |
| | Female | 43% |
| **Use** | Mandatory | 89% |
| | Voluntary | 11% |
| **Barriers for using ICT** | Time | 42% |
| | Training | 31% |
| | Cost | 4% |
| | Compensation | 20% |
| | Do not fit with the job | 3% |

Another survey was conducted in a large public university in the Midwest area. The revised questionnaires were distributed to 394 undergraduate students in a business administration course. There were 294 returned responses, for an overall response rate of 74.62 percent. The demographic data of respondents were also collected. Table 2 demonstrates sample characteristics.

The subject of the questionnaire was the assessment of the students' intention to use Blackboard (named MyGateway at the survey institution) which is a Web-based software system used to support flexible teaching and learning in face-to-face and distance courses. Blackboard is an educational innovation that provides tools and facilities for the online course management, content management and sharing, assessment management, and online collaboration and communication between faculty and students or among students themselves.

**Table 3. Sample Characteristics from the study in Midwest area (p-value <= .01)**

| Sample Characteristics | Results |
|---|---|
| **Academic Year** | Freshman 30.38 %<br>Sophomore 15.00 %<br>Junior 40.77 %<br>Senior 13.08 %<br>Other 0.77 % |
| **Gender** | Male 50.38 %<br>Female 49.62 % |
| **Age** | Mean 22.12<br>S.D. 5.19 |
| **Application Experience** | None 50.77 %<br>1-2 Semester 30.77 %<br>More than 2 Semester 18.46 % |
| **Application Training** | None 82.31 %<br>1-5 Hours 16.92 %<br>More than 5 Hours 0.77 % |
| **Voluntariness** | Yes 50.00 %<br>No 50.00 % |

The last study attempted to understand factors that affected university students' usage intention of library apps in university libraries. The survey was administered in Taiwan in the context of adopting library apps in university libraries; the subjects selected were distributed across various departments, and undergraduate and graduate students in eastern Taiwan from each department and school were fairly evenly distributed to ensure valid comparison.

All subjects participated in the study voluntarily. There were a total of 363 Participants, 168 males and 195 females. Within the sample population: 277 (76.3 percent) were undergraduate students and 86 (23.7 percent) were graduate students. The age of the participants ranged from 18 to 28 years. Most of the participants (69 percent) stated they were familiar with the term library APP before the survey.

**Table 4. Results from the study in Taiwan (p-value <= 0.05; 0.01; 0.001)**

| Results from the study in Taiwan (Number of respondents N = 363) | | |
|---|---|---|
| **Gender** | Male | 168 |
| | Female | 195 |
| **Population** | undergraduate students | 277 |
| | graduate students | 86 |

## 6. Conclusion

Today the majority of researches in IS are focused on adoption and use of various technologies. Hence the application of UTAUT is of great importance for them, because this theory helps us to get real result in real time, based on opinion of the respondents.

According to various studies that have been implemented in many universities that use the UTAUT, we conclude that the use of ICT is almost everywhere mandatory, but we are still working on an adoption and use of new technologies by academic staff.

However, we know that by using new technologies we improve the quality of work, if they are accepted and used by employees. The faster a technology is accepted by all employees, the faster the effectiveness and efficiency of operations will improve. For a technology to be accepted by the employees, mandatory training, time, and above all perseverance and desire to learn something new are required.

## References:

[1] Carmen C. Lewis, Cherie E. Fretwell, Jim Ryan, James B. Parham. (2013). Faculty Use of Established and Emerging Technologies in Higher Education: A Unified Theory of Acceptance and Use of Technology Perspective. *International Journal of Higher Education*, 22-34.

[2] Dapper, G. (n.d.). *User acceptance of Enterprise 2.0 - A case study at an internationally operating private bank.*

[3] Il Im, Seongtae Hong, Myung Soo Kang. (2011). An international comparison of technology adoption Testing the UTAUT model. *Information & Management*, 48, 1-8

[4] Lemuria Carter, Ludwig Christian Shaupp, Jeffrey Hobbs, Ronald Campbell. (2011). The role of security and trust in the adoption of online tax filing. *Emerald*, 303-318

[5] Mike Wade, Scott Schneberger. (2005, September 30). Retrieved from The Theories Used in IS Research : http://www.istheory.yorku.ca/УТАУТ.htm

[6] Oye N. D., A.Iahad N., Ab.Rahim N. (2012). Acceptance and Usage of ICT by University Academicians Using УТАУТ Model: A Case Study of University of Port Harcourt, Nigeria. *Journal of Emerging Trends in Computing and Information Sciences*, 81-89.

[7] N.D. Oye, N. A. Iahad, Zairah Ab. Rabin. (2011). A Model of ICT Acceptance and Use for Teachers in Higher Education Institutions. *International Journal of Computer Science & Communication Networks*, 22-40.

[8] Ton A.M.Spil, Roel W.Schuring. (2006). *E-Health Systems: Diffusion and use: The inovation, the user and the use IT model.* Hershey, London, Melbourne, Singapore: Idea Group.

[9] Venkatesh, V. (n.d.). *Walton college of business*. Retrieved from Theoretical Models: http://www.vvenkatesh.com/organizations/Theoretical_Models.asp#УТАУТ

[10] Viswanath Venkatesh, James Y. L. Thong, Xin Xu. (2012). CONSUMER ACCEPTANCE AND USE OF INFORMATION TECHNOLOGY: EXTENDING THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY. *MIS Quarterly*, 157-178.

[11] Viswanath Venkatesh, James Y. L. Thong, Frank K. Y. Chan, Paul Jen-Hwa Hu, Susan A. Brown. (2011). Extending the two-stage information systems continuance model: incorporating УТАУТ predictors and the role of context. *Information Systems Journal*, 527–555.

[12] Viswanath Venkatesh, Susan A. Brown, Likoebe M. Maruping, Hillol Bala. (2008). PREDICTING DIFFERENT CONCEPTUALIZATIONS OF SYSTEM USE: THE COMPETING ROLES OF BEHAVIORAL INTENTION, FACILITATING CONDITIONS, AND BEHAVIORAL EXPECTATION. *MIS Quarterly*, 483-502.

[13] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, Fred D. Davis. (2003). USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW. *MIS Quarterly*, 425-478.

[14] Yu-LungWu, Yu-Hui Tao, Pei-Chi Yang. (2008). The use of unified theory of acceptance and use of technology to confer. *Journal of Statistics & Management Systems*, 919–949.