BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 3–12
ISSN 1024–7696

Estimates for the number of vertices with an interval spectrum in proper edge colorings of some graphs

R. R. Kamalian

Abstract. For an undirected, simple, finite, connected graph G, we denote by $V(G)$ and $E(G)$ the sets of its vertices and edges, respectively. A function $\varphi : E(G) \to \{1, 2, \ldots, t\}$ is called a proper edge t-coloring of a graph G if all colors are used and no two adjacent edges receive the same color. An arbitrary nonempty subset of consecutive integers is called an interval. The set of all proper edge t-colorings of G is denoted by $\alpha(G, t)$. The minimum value of t for which there exists a proper edge t-coloring of a graph G is denoted by $\chi'(G)$. Let

$$\alpha(G) \equiv \bigcup_{t=\chi'(G)}^{|E(G)|} \alpha(G, t).$$

If G is a graph, $\varphi \in \alpha(G)$, $x \in V(G)$, then the set of colors of edges of G incident with x is called a spectrum of the vertex x in the coloring φ of the graph G and is denoted by $S_G(x, \varphi)$. If $\varphi \in \alpha(G)$ and $x \in V(G)$, then we say that φ is interval (persistent-interval) for x if $S_G(x, \varphi)$ is an interval (an interval with 1 as its minimum element). For an arbitrary graph G and any $\varphi \in \alpha(G)$, we denote by $f_{G,i}(\varphi)(f_{G,pi}(\varphi))$ the number of vertices of the graph G for which φ is interval (persistent-interval). For any graph G, let us set

$$\eta_i(G) \equiv \max_{\varphi \in \alpha(G)} f_{G,i}(\varphi), \quad \eta_{pi}(G) \equiv \max_{\varphi \in \alpha(G)} f_{G,pi}(\varphi).$$

For graphs G from some classes of graphs, we obtain lower bounds for the parameters $\eta_i(G)$ and $\eta_{pi}(G)$.

Mathematics subject classification: 05C15.
Keywords and phrases: Proper edge coloring, interval spectrum.

1 Introduction

We consider undirected, simple, finite, connected graphs. For a graph G, we denote by $V(G)$ and $E(G)$ the sets of its vertices and edges, respectively. For any $x \in V(G)$, $d_G(x)$ denotes the degree of the vertex x in G. For a graph G, we denote by $\Delta(G)$ the maximum degree of a vertex of G. A function $\varphi : E(G) \to \{1, 2, \ldots, t\}$ is called a proper edge t-coloring of a graph G if all colors are used and no two adjacent edges receive the same color. The set of all proper edge t-colorings of G is denoted by $\alpha(G, t)$. The minimum value of t for which there exists a proper edge t-coloring of a graph G is called a chromatic index [22] of G and is denoted by $\chi'(G)$.

Let us also define the set $\alpha(G)$ of all proper edge colorings of the graph G

$$\alpha(G) \equiv \bigcup_{t=\chi'(G)}^{|E(G)|} \alpha(G,t).$$

If G is a graph, $\varphi \in \alpha(G)$, $x \in V(G)$, then the set of colors of edges of G incident with x is called a spectrum of the vertex x in the coloring φ of the graph G and is denoted by $S_G(x,\varphi)$.

An arbitrary nonempty subset of consecutive integers is called an interval. An interval with the minimum element p and the maximum element q is denoted by $[p,q]$. An interval D is called an h-interval if $|D| = h$.

For any real number ξ, we denote by $\lfloor \xi \rfloor$ ($\lceil \xi \rceil$) the maximum (minimum) integer which is less (greater) than or equal to ξ.

If G is a graph, $\varphi \in \alpha(G)$, and $x \in V(G)$, then we say that φ is interval (persistent-interval) for x if $S_G(x,\varphi)$ is a $d_G(x)$-interval (a $d_G(x)$-interval with 1 as its minimum element). For an arbitrary graph G and any $\varphi \in \alpha(G)$, we denote by $f_{G,i}(\varphi)(f_{G,pi}(\varphi))$ the number of vertices of the graph G for which φ is interval (persistent-interval). For any graph G, let us [17] set

$$\eta_i(G) \equiv \max_{\varphi \in \alpha(G)} f_{G,i}(\varphi), \quad \eta_{pi}(G) \equiv \max_{\varphi \in \alpha(G)} f_{G,pi}(\varphi).$$

The terms and concepts that we do not define can be found in [23].

It is clear that if for any graph G $\eta_{pi}(G) = |V(G)|$, then $\chi'(G) = \Delta(G)$. For a regular graph G, these two conditions are equivalent: $\eta_{pi}(G) = |V(G)| \Leftrightarrow \chi'(G) = \Delta(G)$. It is known [15, 19] that for a regular graph G, the problem of deciding whether or not the equation $\chi'(G) = \Delta(G)$ is true is NP-complete. It means that for a regular graph G, the problem of deciding whether or not the equation $\eta_{pi}(G) = |V(G)|$ is true is also NP-complete. For any tree G, some necessary and sufficient condition for fulfilment of the equation $\eta_{pi}(G) = |V(G)|$ was obtained in [8]. In this paper, for an arbitrary regular graph G, we obtain a lower bound for the parameter $\eta_{pi}(G)$.

If G is a graph, $R_0 \subseteq V(G)$, and the coloring $\varphi \in \alpha(G)$ is interval (persistent-interval) for any $x \in R_0$, then we say that φ is interval (persistent-interval) on R_0.

$\varphi \in \alpha(G)$ is called an interval coloring of a graph G if φ is interval on $V(G)$.

We define the set $\mathfrak{N}$ as the set of all graphs for which there is an interval coloring. Clearly, for any graph G, $G \in \mathfrak{N}$ if and only if $\eta_i(G) = |V(G)|$.

The notion of an interval coloring was introduced in [6]. In [6, 7, 16] it is shown that if $G \in \mathfrak{N}$, then $\chi'(G) = \Delta(G)$. For a regular graph G, these two conditions are equivalent: $G \in \mathfrak{N} \Leftrightarrow \chi'(G) = \Delta(G)$ [6, 7, 16]. Consequently, for a regular graph G, four conditions are equivalent: $G \in \mathfrak{N}$, $\chi'(G) = \Delta(G)$, $\eta_i(G) = |V(G)|$, $\eta_{pi}(G) = |V(G)|$. It means that for any regular graph G,

1) the problem of deciding whether G has or not an interval coloring is NP-complete,

2) the problem of deciding whether the equation $\eta_i(G) = |V(G)|$ is true or not is NP-complete.

In this paper, for an arbitrary regular graph G, we obtain a lower bound for the parameter $\eta_i(G)$.

We also obtain some results for bipartite graphs. The complexity of the problem of existence of an interval coloring for bipartite graphs is investigated in [3, 9, 21]. In [16] it is shown that for a bipartite graph G with bipartition (X, Y) and $\Delta(G) = 3$ the problem of existence of a proper edge 3-coloring which is persistent-interval on $X \cup Y$ (or even only on Y [6, 16]) is NP-complete.

Suppose that G is an arbitrary bipartite graph with bipartition (X, Y) [3]. Then $\eta_i(G) \geq \max\{|X|, |Y|\}$.

Suppose that G is a bipartite graph with bipartition (X, Y) for which there exists a coloring $\varphi \in \alpha(G)$ persistent-interval on Y. Then $\eta_{pi}(G) \geq 1 + |Y|$.

Some attention is paid to (α, β)-biregular bipartite graphs [4, 13, 14, 18] in the case when $|\alpha - \beta| = 1$.

We show that if G is a $(k-1, k)$-biregular bipartite graph, $k \geq 4$, then

$$\eta_i(G) \geq \frac{k-1}{2k-1} \cdot |V(G)| + \left\lceil \frac{k}{\lceil \frac{k}{2} \rceil \cdot (2k-1)} \cdot |V(G)| \right\rceil.$$

We show that if G is a $(k-1, k)$-biregular bipartite graph, $k \geq 3$, then

$$\eta_{pi}(G) \geq \frac{k}{2k-1} \cdot |V(G)|.$$

2 Results

Theorem 1 (see [17]). *If G is a regular graph with $\chi'(G) = 1 + \Delta(G)$, then*

$$\eta_{pi}(G) \geq \left\lceil \frac{|V(G)|}{1 + \Delta(G)} \right\rceil.$$

Proof. Suppose that $\beta \in \alpha(G, 1 + \Delta(G))$. For any $j \in [1, 1 + \Delta(G)]$, define

$$V_{G,\beta,j} \equiv \{x \in V(G) / j \notin S_G(x, \beta)\}.$$

For arbitrary integers j', j'', where $1 \leq j' < j'' \leq 1 + \Delta(G)$, we have

$$V_{G,\beta,j'} \cap V_{G,\beta,j''} = \varnothing \quad \text{and} \quad \bigcup_{j=1}^{1+\Delta(G)} V_{G,\beta,j} = V(G).$$

Hence, there exists $j_0 \in [1, 1 + \Delta(G)]$ for which

$$|V_{G,\beta,j_0}| \geq \left\lceil \frac{|V(G)|}{1 + \Delta(G)} \right\rceil.$$

Set $R_0 \equiv V_{G,\beta,j_0}$.
Case 1. $j_0 = 1 + \Delta(G)$.
Clearly, β is persistent-interval on R_0.
Case 2. $j_0 \in [1, \Delta(G)]$.
Define a function $\varphi : E(G) \to [1, 1 + \Delta(G)]$. For any $e \in E(G)$, set:

$$\varphi(e) \equiv \begin{cases} \beta(e) & \text{if } \beta(e) \notin \{j_0, 1 + \Delta(G)\}, \\ j_0 & \text{if } \beta(e) = 1 + \Delta(G), \\ 1 + \Delta(G) & \text{if } \beta(e) = j_0. \end{cases}$$

It is not difficult to see that $\varphi \in \alpha(G, 1 + \Delta(G))$ and φ is persistent-interval on R_0. □

Corollary 1 (see [17]). *If G is a cubic graph, then there exists a coloring from $\alpha(G, \chi'(G))$ which is persistent-interval for at least $\left\lceil \frac{|V(G)|}{4} \right\rceil$ vertices of G.*

Theorem 2 (see [17]). *If G is a regular graph with $\chi'(G) = 1 + \Delta(G)$, then*

$$\eta_i(G) \geq \left\lceil \frac{|V(G)|}{\lceil \frac{1+\Delta(G)}{2} \rceil} \right\rceil.$$

Proof. Suppose that $\beta \in \alpha(G, 1 + \Delta(G))$. For any $j \in [1, 1 + \Delta(G)]$, define

$$V_{G,\beta,j} \equiv \{x \in V(G)/j \notin S_G(x, \beta)\}.$$

For arbitrary integers j', j'', where $1 \leq j' < j'' \leq 1 + \Delta(G)$, we have

$$V_{G,\beta,j'} \cap V_{G,\beta,j''} = \varnothing \quad \text{and} \quad \bigcup_{j=1}^{1+\Delta(G)} V_{G,\beta,j} = V(G).$$

For any $i \in [1, \lceil \frac{1+\Delta(G)}{2} \rceil]$, let us define the subset $V(G, \beta, i)$ of the set $V(G)$ as follows:

$$V(G, \beta, i) \equiv \begin{cases} V_{G,\beta,2i-1} \cup V_{G,\beta,2i} & \text{if } \Delta(G) \text{ is odd and } i \in [1, \frac{1+\Delta(G)}{2}] \\ & \text{or } \Delta(G) \text{ is even and } i \in [1, \frac{\Delta(G)}{2}], \\ V_{G,\beta,1+\Delta(G)} & \text{if } \Delta(G) \text{ is even and } i = 1 + \frac{\Delta(G)}{2}. \end{cases}$$

For arbitrary integers i', i'', where $1 \leq i' < i'' \leq \lceil \frac{1+\Delta(G)}{2} \rceil$, we have

$$V(G, \beta, i') \cap V(G, \beta, i'') = \varnothing \quad \text{and} \quad \bigcup_{i=1}^{\lceil \frac{1+\Delta(G)}{2} \rceil} V(G, \beta, i) = V(G).$$

Hence, there exists $i_0 \in \left[1, \lceil \frac{1+\Delta(G)}{2} \rceil\right]$ for which

$$|V(G, \beta, i_0)| \geq \left\lceil \frac{|V(G)|}{\lceil \frac{1+\Delta(G)}{2} \rceil} \right\rceil.$$

Set $R_0 \equiv V(G, \beta, i_0)$.
Case 1. $i_0 = \lceil \frac{1+\Delta(G)}{2} \rceil$.
Case 1.a. $\Delta(G)$ is even.
Clearly, β is interval on R_0.
Case 1.b. $\Delta(G)$ is odd.
Define a function $\varphi : E(G) \to [1, 1 + \Delta(G)]$. For any $e \in E(G)$, set:

$$\varphi(e) \equiv \begin{cases} (\beta(e) + 1)(\mathrm{mod}(1 + \Delta(G))) & \text{if } \beta(e) \neq \Delta(G), \\ 1 + \Delta(G) & \text{if } \beta(e) = \Delta(G). \end{cases}$$

It is not difficult to see that $\varphi \in \alpha(G, 1 + \Delta(G))$ and φ is interval on R_0.
Case 2. $1 \leq i_0 \leq \lceil \frac{\Delta(G)-1}{2} \rceil$.
Define a function $\varphi : E(G) \to [1, 1 + \Delta(G)]$. For any $e \in E(G)$, set:

$$\varphi(e) \equiv \begin{cases} (\beta(e) + 2 + \Delta(G) - 2i_0)(\mathrm{mod}(1 + \Delta(G))) & \text{if } \beta(e) \neq 2i_0 - 1, \\ 1 + \Delta(G) & \text{if } \beta(e) = 2i_0 - 1. \end{cases}$$

It is not difficult to see that $\varphi \in \alpha(G, 1 + \Delta(G))$ and φ is interval on R_0. □

Corollary 2 (see [17]). *If G is a cubic graph, then there exists a coloring from $\alpha(G, \chi'(G))$ which is interval for at least $\frac{|V(G)|}{2}$ vertices of G.*

Theorem 3 (see [6,7,16]). *Let G be a bipartite graph with bipartition (X, Y). Then there exists a coloring $\varphi \in \alpha(G, |E(G)|)$ which is interval on X.*

Corollary 3. *Let G be a bipartite graph with bipartition (X, Y). Then $\eta_i(G) \geq \max\{|X|, |Y|\}$.*

Theorem 4 (see [1,6,7]). *Let G be a bipartite graph with bipartition (X, Y) where $d_G(x) \leq d_G(y)$ for each edge $(x, y) \in E(G)$ with $x \in X$ and $y \in Y$. Then there exists a coloring $\varphi_0 \in \alpha(G, \Delta(G))$ which is persistent-interval on Y.*

Theorem 5. *Suppose G is a bipartite graph with bipartition (X, Y), and there exists a coloring $\varphi_0 \in \alpha(G, \Delta(G))$ which is persistent-interval on Y. Then, for an arbitrary vertex $x_0 \in X$, there exists $\psi \in \alpha(G, \Delta(G))$ which is persistent-interval on $\{x_0\} \cup Y$.*

Proof. Case 1. $S_G(x_0, \varphi_0) = [1, d_G(x_0)]$. In this case ψ is φ_0.

Case 2. $S_G(x_0, \varphi_0) \neq [1, d_G(x_0)]$.

Clearly, $[1, d_G(x_0)] \backslash S_G(x_0, \varphi_0) \neq \emptyset$, $S_G(x_0, \varphi_0) \backslash [1, d_G(x_0)] \neq \emptyset$. Since $|S_G(x_0, \varphi_0)| = |[1, d_G(x_0)]| = d_G(x_0)$, there exists $\nu_0 \in [1, d_G(x_0)]$ satisfying the condition $|[1, d_G(x_0)] \backslash S_G(x_0, \varphi_0)| = |S_G(x_0, \varphi_0) \backslash [1, d_G(x_0)]| = \nu_0$.

Now let us construct the sequence $\Theta_0, \Theta_1, \ldots, \Theta_{\nu_0}$ of proper edge $\Delta(G)$-colorings of the graph G, where for any $i \in [0, \nu_0]$, Θ_i is persistent-interval on Y.

Set $\Theta_0 \equiv \varphi_0$.

Suppose that for some $k \in [0, \nu_0 - 1]$, the subsequence $\Theta_0, \Theta_1, \ldots, \Theta_k$ is already constructed.

Let

$$t_k \equiv \max(S_G(x_0, \Theta_k) \backslash [1, d_G(x_0)]),$$

$$s_k \equiv \min([1, d_G(x_0)] \backslash S_G(x_0, \Theta_k)).$$

Clearly, $t_k > s_k$. Consider the path $P(k)$ in the graph G of maximum length with the initial vertex x_0 whose edges are alternatively colored by the colors t_k and s_k. Let Θ_{k+1} be obtained from Θ_k by interchanging the two colors t_k and s_k along $P(k)$.

It is not difficult to see that Θ_{ν_0} is persistent-interval on $\{x_0\} \cup Y$. Set $\psi \equiv \Theta_{\nu_0}$. □

Corollary 4. *Let G be a bipartite graph with bipartition (X, Y) where $d_G(x) \leq d_G(y)$ for each edge $(x, y) \in E(G)$ with $x \in X$ and $y \in Y$. Let x_0 be an arbitrary vertex of X. Then there exists a coloring $\varphi_0 \in \alpha(G, \Delta(G))$ which is persistent-interval on $\{x_0\} \cup Y$.*

Corollary 5 (see [17])**.** *Let G be a bipartite graph with bipartition (X, Y) where $d_G(x) \leq d_G(y)$ for each edge $(x, y) \in E(G)$ with $x \in X$ and $y \in Y$. Then $\eta_{pi}(G) \geq 1 + |Y|$.*

Remark 1. Notice that the complete bipartite graph $K_{n+1,n}$ for an arbitrary positive integer n satisfies the conditions of Corollary 5. Is is not difficult to see that $\eta_{pi}(K_{n+1,n}) = 1 + n$. It means that the bound obtained in Corollary 5 is sharp since in this case $|Y| = n$.

Remark 2. Let G be a bipartite $(k-1, k)$-biregular graph with bipartition (X, Y), where $k \geq 3$. Assume that all vertices in X have the degree $k-1$ and all vertices in Y have the degree k. Then the numbers $\frac{|X|}{k}$, $\frac{|Y|}{k-1}$, and $\frac{|V(G)|}{2k-1}$ are integer. It follows from the equalities $\gcd(k-1, k) = 1$ and $|E(G)| = |X| \cdot (k-1) = |Y| \cdot k$.

Theorem 6 (see [17])**.** *Let G be a bipartite $(k-1, k)$-biregular graph, where $k \geq 4$. Then*

$$\eta_i(G) \geq \frac{k-1}{2k-1} \cdot |V(G)| + \left\lceil \frac{k}{\lceil \frac{k}{2} \rceil \cdot (2k-1)} \cdot |V(G)| \right\rceil.$$

Proof. Suppose that (X, Y) is a bipartition of G. Without loss of generality we assume that all vertices in X have the degree $k-1$ and all vertices in Y have the degree k. Clearly, $\chi'(G) = \Delta(G) = k$. Suppose that $\beta \in \alpha(G, k)$. For any $j \in [1, k]$, define:

$$V_{G,\beta,j} \equiv \{x \in X / j \notin S_G(x, \beta)\}.$$

For arbitrary integers j', j'', where $1 \leq j' < j'' \leq k$, we have

$$V_{G,\beta,j'} \cap V_{G,\beta,j''} = \varnothing \quad \text{and} \quad \bigcup_{j=1}^{k} V_{G,\beta,j} = X.$$

For any $i \in [1, \lceil \frac{k}{2} \rceil]$, let us define the subset $V(G, \beta, i)$ of the set X as follows:

$$V(G,\beta,i) \equiv \begin{cases} V_{G,\beta,2i-1} \cup V_{G,\beta,2i} & \text{if } k \text{ is odd and } i \in [1, \frac{k-1}{2}] \\ & \text{or } k \text{ is even and } i \in [1, \frac{k}{2}], \\ V_{G,\beta,k} & \text{if } k \text{ is odd and } i = \frac{1+k}{2}. \end{cases}$$

For arbitrary integers i', i'', where $1 \le i' < i'' \le \lceil \frac{k}{2} \rceil$, we have

$$V(G,\beta,i') \cap V(G,\beta,i'') = \varnothing \quad \text{and} \quad \bigcup_{i=1}^{\lceil \frac{k}{2} \rceil} V(G,\beta,i) = X.$$

Hence, there exists $i_0 \in \left[1, \lceil \frac{k}{2} \rceil\right]$ for which

$$|V(G,\beta,i_0)| \ge \left\lceil \frac{|X|}{\lceil \frac{k}{2} \rceil} \right\rceil.$$

Set $R_0 \equiv Y \cup V(G, \beta, i_0)$.
It is not difficult to verify that

$$|R_0| \ge \frac{k-1}{2k-1} \cdot |V(G)| + \left\lceil \frac{k}{\lceil \frac{k}{2} \rceil \cdot (2k-1)} \cdot |V(G)| \right\rceil.$$

Case 1. $i_0 = \lceil \frac{k}{2} \rceil$.
Case 1.a. k is odd.
Clearly, β is interval on R_0.
Case 1.b. k is even.
Define a function $\varphi : E(G) \to [1, k]$. For any $e \in E(G)$, set:

$$\varphi(e) \equiv \begin{cases} (\beta(e)+1) (\mathrm{mod} k) & \text{if } \beta(e) \ne k-1, \\ k & \text{if } \beta(e) = k-1. \end{cases}$$

It is not difficult to see that $\varphi \in \alpha(G, k)$ and φ is interval on R_0.
Case 2. $i_0 \in \left[1, \lceil \frac{k}{2} \rceil - 1\right]$.
Define a function $\varphi : E(G) \to [1, k]$. For any $e \in E(G)$, set:

$$\varphi(e) \equiv \begin{cases} (\beta(e)+1+k-2i_0) (\mathrm{mod} k) & \text{if } \beta(e) \ne 2i_0-1, \\ k & \text{if } \beta(e) = 2i_0-1. \end{cases}$$

It is not difficult to see that $\varphi \in \alpha(G, k)$ and φ is interval on R_0. □

Corollary 6 (see [17]). *Let G be a bipartite $(k-1, k)$-biregular graph, where k is even and $k \ge 4$. Then*

$$\eta_i(G) \ge \frac{k+1}{2k-1} \cdot |V(G)|.$$

Corollary 7 (see [17]). *Let G be a bipartite $(3,4)$-biregular graph. Then there exists a coloring from $\alpha(G,4)$ which is interval for at least $\frac{5}{7}|V(G)|$ vertices of G.*

Remark 3. For an arbitrary bipartite graph G with $\Delta(G) \leq 3$, there exists an interval coloring of G [10–12]. Consequently, if G is a bipartite $(2,3)$-biregular graph, then $\eta_i(G) = |V(G)|$.

Remark 4. Some sufficient conditions for existence of an interval coloring of a $(3,4)$-biregular bipartite graph were obtained in [2, 5, 20].

Theorem 7 (see [17]). *Let G be a bipartite $(k-1,k)$-biregular graph, where $k \geq 3$. Then*

$$\eta_{pi}(G) \geq \frac{k}{2k-1} \cdot |V(G)|.$$

Proof. Suppose that (X,Y) is a bipartition of G. Without loss of generality we assume that all vertices in X have the degree $k-1$ and all vertices in Y have the degree k. Clearly, $\chi'(G) = \Delta(G) = k$. Suppose that $\beta \in \alpha(G,k)$.

For any $j \in [1,k]$, define:

$$V_{G,\beta,j} \equiv \{x \in X / j \notin S_G(x,\beta)\}.$$

For arbitrary integers j', j'', where $1 \leq j' < j'' \leq k$, we have

$$V_{G,\beta,j'} \cap V_{G,\beta,j''} = \varnothing \quad \text{and} \quad \bigcup_{j=1}^{k} V_{G,\beta,j} = X.$$

Hence, there exists $j_0 \in [1,k]$ for which

$$|V_{G,\beta,j_0}| \geq \frac{|X|}{k}.$$

Set $R_0 \equiv Y \cup V_{G,\beta,j_0}$.

It is not difficult to verify that

$$|R_0| \geq \frac{k}{2k-1} \cdot |V(G)|.$$

Case 1. $j_0 = k$.

Clearly, β is persistent-interval on R_0.

Case 2. $j_0 \in [1, k-1]$.

Define a function $\varphi : E(G) \to [1,k]$. For any $e \in E(G)$, set:

$$\varphi(e) \equiv \begin{cases} \beta(e) & \text{if } \beta(e) \notin \{j_0, k\}, \\ j_0 & \text{if } \beta(e) = k, \\ k & \text{if } \beta(e) = j_0. \end{cases}$$

It is not difficult to see that $\varphi \in \alpha(G,k)$ and φ is persistent-interval on R_0. □

Corollary 8 (see [17]). *Let G be a bipartite $(3,4)$-biregular graph. Then there exists a coloring from $\alpha(G,4)$ which is persistent-interval for at least $\frac{4}{7}|V(G)|$ vertices of G.*

Acknowledgment. The author thanks professors A. S. Asratian and P. A. Petrosyan for their attention to this work.

References

[1] Asratian A. S. *Investigation of some mathematical model of Scheduling Theory.* Doctoral dissertation, Moscow University, 1980 (in Russian).

[2] Asratian A. S., Casselgren C. J. *A sufficient condition for interval edge colorings of* $(4,3)$*-biregular bipartite graphs.* Research report LiTH-MAT-R-2006-07, Linköping University, 2006.

[3] Asratian A. S., Casselgren C. J. *Some results on interval edge colorings of* (α,β)*-biregular bipartite graphs.* Research report LiTH-MAT-R-2006-09, Linköping University, 2006.

[4] Asratian A. S., Casselgren C. J. *On interval edge colorings of* (α,β)*-biregular bipartite graphs.* Discrete Math., 2007, **307**, 1951–1956.

[5] Asratian A. S., Casselgren C. J., Vandenbussche J., West D. B. *Proper path-factors and interval edge-coloring of* $(3,4)$*-biregular bigraphs.* J. of Graph Theory, 2009, **61**, 88–97.

[6] Asratian A. S., Kamalian R. R. *Interval colorings of edges of a multigraph.* Appl. Math., 1987, **5**, Yerevan State University, 25–34 (in Russian).

[7] Asratian A. S., Kamalian R. R. *Investigation of interval edge-colorings of graphs.* Journal of Combinatorial Theory, Series B, 1994, **62**, No. 1, 34–43.

[8] Caro Y., Schönheim J. *Generalized* 1*-factorization of trees.* Discrete Math., 1981, **33**, 319–321.

[9] Giaro K. *The complexity of consecutive* Δ*-coloring of bipartite graphs:* 4 *is easy,* 5 *is hard.* Ars Combin., 1997, **47**, 287–298.

[10] Giaro K. *Compact Task Scheduling on Dedicated Processors with no Waiting Periods.* Ph. D. Thesis, Technical University of Gdańsk, ETI Faculty, Gdańsk, 1999, (in Polish).

[11] Giaro K., Kubale M., Małafiejski M. *Compact scheduling in open shop with zero-one time operations.* INFOR, 1999, **37**, 37–47.

[12] Hansen H. *Scheduling with minimum waiting periods.* Master Thesis, Odense University, Odense, Denmark, 1992 (in Danish).

[13] Hanson D., Loten C. O. M. *A lower bound for Interval colouring bi-regular bipartite graphs.* Bulletin of the ICA, 1996, **18**, 69–74.

[14] Hanson D., Loten C. O. M., Toft B. *On interval colourings of bi-regular bipartite graphs.* Ars Combin., 1998, **50**, 23–32.

[15] Holyer I. *The* NP*-completeness of edge-coloring.* SIAM J. Comput., 1981, **10**, 718–720.

[16] Kamalian R. R. *Interval Edge Colorings of Graphs.* Doctoral dissertation, the Institute of Mathematics of the Siberian Branch of the Academy of Sciences of USSR, Novosibirsk, 1990 (in Russian).

[17] Kamalian R. R. *On a number of vertices with an interval spectrum in proper edge colorings of some graphs.* Research report LiTH-MAT-R-2011/03-SE, Linköping University, 2011.

[18] Kostochka A. V. *Unpublished manuscript*, 1995.

[19] Leven D., Galil Z. *NP-completeness of finding the chromatic index of regular graphs*. J. Algorithms, 1983, **4**, 35–44.

[20] Pyatkin A. V. *Interval coloring of* $(3,4)$*-biregular bipartite graphs having large cubic subgraphs*. J. of Graph Theory, 2004, **47**, 122–128.

[21] Sevast'janov S. V. *Interval colorability of the edges of a bipartite graph*. Metody Diskret. Analiza, 1990, **50**, 61–72 (in Russian).

[22] Vizing V. G. *The chromatic index of a multigraph*. Kibernetika, 1965, **3**, 29–39.

[23] West D. B. *Introduction to Graph Theory*. Prentice-Hall, New Jersey, 1996.

R. R. Kamalian
Institute for Informatics and Automation Problems
National Academy of Sciences of RA
0014 Yerevan, Republic of Armenia

E-mail: *rrkamalian@yahoo.com*

Received April 30, 2013

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 13–22
ISSN 1024–7696

Closure operators in the categories of modules. Part IV (Relations between the operators and preradicals)

A. I. Kashu

Abstract. In this work (which is a continuation of [1–3]) the relations between the class $\mathbb{CO}$ of the closure operators of a module category R-Mod and the class $\mathbb{PR}$ of preradicals of this category are investigated. The transition from $\mathbb{CO}$ to $\mathbb{PR}$ and backwards is defined by three mappings $\Phi : \mathbb{CO} \to \mathbb{PR}$ and $\Psi_1, \Psi_2 : \mathbb{CO} \to \mathbb{PR}$. The properties of these mappings are studied.

Some monotone bijections are obtained between the preradicals of different types (idempotent, radical, hereditary, cohereditary, etc.) of $\mathbb{PR}$ and the closure operators of $\mathbb{CO}$ with special properties (weakly hereditary, idempotent, hereditary, maximal, minimal, cohereditary, etc.).

Mathematics subject classification: 16D90, 16S90, 06B23.
Keywords and phrases: ring, module, closure operator, preradical, torsion, radical filter, idempotent ideal.

1 Introduction. Preliminary notions and results

The purpose of this work is the investigation of the relations between the preradicals of the module category R-Mod and the closure operators of this category. For that three known mappings are used, which provide the connection between the closure operators and preradicals of R-Mod. We will study the properties of these mappings for different classes of preradicals and of closure operators of R-Mod.

This article is a continuation of [1–3], where the necessary notions are indicated. Nevertheless, for completeness and independence of this part, we would remind shortly the main notions and results which are used in continuation.

Let R be a ring with unity and R-Mod be the category of unitary left R-modules. For every module $M \in R$-Mod we denote by $\mathbb{L}(M)$ the lattice of submodules of M.

A *preradical* of R-Mod is a subfunctor r of the identity functor of R-Mod, i.e. $r(M) \subseteq M$ for every $M \in R$-Mod and $f\big(r(M)\big) \subseteq r(M')$ for every R-morphism $f : M \to M'$. We denote by $\mathbb{PR}$ the class of all preradicals of the category R-Mod. We remind the *principal types* of preradicals [4–6]. The preradical $r \in \mathbb{PR}$ is called:

– *idempotent* if $r\big(r(M)\big) = r(M)$ for every $M \in R$-Mod;
– *radical* if $r\big(M/\,r(M)\big) = O$ for every $M \in R$-Mod;
– *hereditary* (*pretorsion*) if $r(N) = r(M) \cap N$ for every $N \subseteq M$;
– *cohereditary* if $r(M/\,N) = \big(r(M) + N\big)/\,N$ for every $N \subseteq M$;

– *torsion* if it is a hereditary radical;
– *cotorsion* if it is idempotent and cohereditary.

It is well known that some types of preradicals of R-Mod can be characterized by special ring constructions, such as preradical filters (i.e. linear topologies), radical filters, ideals, idempotent ideals, etc. (see [4–6]). Some results of such type are included in the following statement.

Proposition 1.1. *There exist the bijections between:*

1) *the* ***pretorsions*** *of R-Mod and preradical filters of R;*
2) *the* ***torsions*** *of R-Mod and radical filters of R;*
3) *the* ***cohereditary preradicals*** *of R-Mod and ideals of R;*
4) *the* ***cotorsions*** *of R-Mod and idempotent ideals of R;*
5) *the* ***hereditary and cohereditary*** *preradicals of R-Mod and still ideals of R, i.e. the ideals with the condition (a) : $a \in Ia$ for every $a \in I$ (see* [4]*, p.* 12; [5]*, p.* 467*).* □

A *closure operator* of R-Mod is a mapping C which associates to every pair $N \subseteq M$, where $N \in \mathbb{L}(M)$, a submodule of M denoted by $C_M(N)$ which satisfies the conditions:

(c_1) $N \subseteq C_M(N)$;

(c_2) if $N_1 \subseteq N_2$ for $N_1, N_2 \in \mathbb{L}(M)$, then $C_M(N_1) \subseteq C_M(N_2)$ (the monotony);

(c_3) for every R-morphism $f : M \to M'$ and $N \in \mathbb{L}(M)$ we have

$$f\big(C_M(N)\big) \subseteq C_{M'}(N)\big(f(M)\big) \quad \text{(the continuity)} \quad [6–9].$$

We denote by $\mathbb{CO}$ the class of all closure operators of R-Mod.

A closure operator $C \in \mathbb{CO}$ is called:

– *weakly hereditary* if $C_{C_M(N)}(N) = C_M(N)$ for every $N \subseteq M$;

– *idempotent* if $C_M\big(C_M(N)\big) = C_M(N)$ for every $N \subseteq M$;

– *hereditary* if $C_N(L) = C_M(L) \cap N$ for every $L \subseteq N \subseteq M$;

– *cohereditary* if $\big(C_M(N) + K\big)/K = C_{M/K}\big((N + K)/K\big)$ for every $K, N \in \mathbb{L}(M)$;

– *maximal* if $C_M(N)/N = C_{M/N}(\bar{0})$ for every $N \subseteq M$ (or: $C_M(N)/K = C_{M/K}(N/K)$ for every $K \subseteq N \subseteq M$);

– *minimal* if $C_M(N) = C_M(O)+N$ for every $N \subseteq M$ (or: $C_M(N) = C_M(L)+N$ for every $L \subseteq N \subseteq M$).

The investigations of the present work are based on the following mappings between the classes $\mathbb{CO}$ and $\mathbb{PR}$ [7–9]:

1) $\Phi : \mathbb{CO} \to \mathbb{PR}$, where we denote $\Phi(C) = r_C$, for every $C \in \mathbb{CO}$, and define:

$$r_C(M) = C_M(O) \tag{1.1}$$

for every $M \in R$-Mod;

2) $\Psi_1 : \mathbb{PR} \to \mathbb{CO}$, where $\Psi_1(r) = C^r$ for every $r \in \mathbb{PR}$ and

$$[(C^r)_M(N)]/\,N = r(M/\,N) \tag{1.2}$$

for every $N \subseteq M$;

3) $\Psi_2 : \mathbb{PR} \to \mathbb{CO}$, where $\Psi_2(r) = C_r$ for every $r \in \mathbb{PR}$ and

$$(C_r)_M(N) = N + r(M) \tag{1.3}$$

for every $N \subseteq M$.

Proposition 1.2. (See [7,8]). *Let $r \in \mathbb{PR}$. Then:*

a) $\Phi(C^r) = r$ *and* C^r *is the* ***largest*** *closure operator $C \in \mathbb{CO}$ with the property $\Phi(C) = r$;*

b) $\Phi(C_r) = r$ *and* C_r *is the* ***least*** *closure operator $C \in \mathbb{CO}$ with the property $\Phi(C) = r$.* □

Let $r \in \mathbb{PR}$. Then for the closure operator $C \in \mathbb{CO}$ we have:

$$\Phi(C) = r \Leftrightarrow C_r \leq C \leq C^r \quad (\text{i.e. } \Phi^{-1}(r) = [C_r, C^r]).$$

The closure operators of the from C^r, where $r \in \mathbb{PR}$, are exactly the *maximal* closure operators and, similarly, the closure operators of the form C_r coincide with the *minimal* closure operators of R-Mod. We denote by $\mathbb{M}ax(\mathbb{CO})$ the class of all maximal closure operators of R-Mod, and by $\mathbb{M}in(\mathbb{CO})$ the class of all minimal closure operators of R-Mod.

For every closure operator $C \in \mathbb{CO}$ we have the maximal closure operator C^{r_C} associated to C, as well as the associated minimal closure operator C_{r_C}. The previous facts in other form can be expressed as follows. In the class $\mathbb{CO}$ we define the binary relation by the rule:

$$C \sim D \Leftrightarrow \Phi(C) = \Phi(D) \quad (\text{i.e. } r_C = r_D).$$

Then we obtain an equivalence in $\mathbb{CO}$ such that every closure operator $C \in \mathbb{CO}$ defines the equivalence class $[C_r, C^r]$. If we denote by $\mathbb{CO}\,/\sim$ the family of equivalence classes of $\mathbb{CO}$, then it is clear that $\mathbb{PR} \cong \mathbb{CO}\,/\sim$.

The following statements in continuation will serve as starting point of our investigation [7–9].

Proposition 1.3. *The mappings (Φ, Ψ_1) define a monotone bijection between the* ***maximal*** *closure operators of $\mathbb{CO}$ and preradicals of R-Mod: $\mathbb{M}ax(\mathbb{CO}) \cong \mathbb{PR}$.* □

Proposition 1.4. *The mappings (Φ, Ψ_2) define a monotone bijection between the* ***minimal*** *closure operators of $\mathbb{CO}$ and preradicals of R-Mod: $\mathbb{M}in(\mathbb{CO}) \cong \mathbb{PR}$.* □

2 The mappings (Φ, Ψ_1) and their effects

The restriction of the bijection of Proposition 1.3, defined by the mappings (Φ, Ψ_1), leads to some new monotone bijections which connect the closure operators of special types of $\mathbb{M}ax(\mathbb{CO})$ with the preradicals of $\mathbb{PR}$ which possess the respective properties.

We begin with a preliminary statement which shows the relations between some properties of the closure operators of R-Mod ([2], Lemmas 5.2 and 6.2).

Lemma 2.1. *Every minimal closure operator is idempotent. The closure operator $C \in \mathbb{CO}$ is cohereditary if and only if it is maximal and minimal.* □

Remark. If the closure operator $C \in \mathbb{CO}$ is cohereditary, then for the respective preradical $r = r_C$ we have $C^r = C_r$, therefore the corresponding equivalence class of $\mathbb{CO}$ consists of only one element. Obviously, the condition $C^r = C_r$ means that this closure operator is cohereditary.

In continuation we consider the monotone bijection of Proposition 1.3, defined by Φ and Ψ_1, analyzing its effect on some important classes of closure operators and of preradicals.

Proposition 2.2. *If the closure operator $C \in \mathbb{CO}$ is **weakly hereditary**, then the preradical $\Phi(C) = r_C$ is idempotent. If the preradical $r \in \mathbb{PR}$ is idempotent, then the associated maximal closure operator C^r is weakly hereditary. Therefore the mappings (Φ, Ψ_1) define a monotone bijection between the maximal weakly hereditary closure operators of $\mathbb{CO}$ and idempotent preradicals of R-Mod.*

Proof. Let $C \in \mathbb{CO}$ be a weakly hereditary closure operator. Then $C_{C_M(O)}(O) = C_M(O)$ for every module $M \in R$-Mod, therefore

$$r_C\big(r_C(M)\big) = r_C\big(C_M(O)\big) = C_{C_M(O)}(O) = C_M(O) = r_C(M),$$

i.e. r_C is an idempotent preradical.

Conversely, let $r \in \mathbb{PR}$ be an idempotent preradical. Then the associated maximal closure operator $\Psi_1(r) = C^r$, defined by the rule $[(C^r)_M(N)]/\,N = r(M/\,N)$ for every $N \subseteq M$, possesses the property:

$$[(C^r)_{(C^r)_M(N)}(N)]\,/\,N = r\big[\big((C^r)_M(N)\big)/\;N\big] =$$

$$= r\big(r(M/\,N)\big) = r(M/\,N) = [(C^r)_M(N)]\,/\,N.$$

Therefore $(C^r)_{(C^r)_M(N)}(N) = (C^r)_M(N)$ for every $N \subseteq M$, which means that the operator C^r is weakly hereditary. The last statement now follows from Proposition 1.3. □

Corollary 2.3. *If the closure operator $C \in \mathbb{CO}$ is weakly hereditary, then the associated maximal closure operator C^{r_C} also is weakly hereditary.*

With the intention to study the closure operators of $\mathbb{CO}$ which correspond to *radicals* of R-Mod, we introduce the following notion.

Definition 2.1. The closure operator $C \in \mathbb{CO}$ will be called **zero-idempotent** if $C_M\big(C_M(O)\big) = C_M(O)$ for every $M \in R$-Mod.

Proposition 2.4. *If r is a **radical** of $\mathbb{PR}$, then the associated maximal closure operator C^r is zero-idempotent. If the operator $C \in \mathbb{CO}$ is maximal and zero-idempotent, then the corresponding preradical $\Phi(C) = r_C$ is a radical. Therefore the mappings (Φ, Ψ_1) define a monotone bijection between the radicals of R-Mod and the maximal zero-idempotent closure operators of $\mathbb{CO}$.*

Proof. Let r be a radical of $\mathbb{PR}$ and C^r be the corresponding maximal closure operator, i.e. $[(C^r)_M(N)]/\,N = r(M/\,N)$ for every $N \subseteq M$. If $N = r(M)$, then $\big[(C^r)_M\big(r(M)\big)\big]/\,r(M) = r\big(M/\,r(M)\big) = \bar{0}$, since r is a radical. But $r(M) = (C^r)_M(O)$, and so

$$\big[(C^r)_M\big((C^r)_M(O)\big)\big]\,/\,[(C^r)_M(O)] = \bar{0},$$

therefore $(C^r)_M\big((C^r)_M(O)\big) = (C^r)_M(O)$, which means that C^r is a zero-idempotent closure operator.

Let now C be an arbitrary maximal zero-idempotent closure operator of $\mathbb{CO}$. Then $C_M\big(C_M(O)\big) = C_M(O)$ for every $M \in R$-Mod, i.e. $C_M\big(r_C(M)\big) = r_C(M)$ and $C_M\big(r_C(M)\big)/\,r_C(M) = \bar{0}$.

From the other hand, since C is maximal, by definition $\big[C_M\big(r_C(M)\big)\big]/r_C(M) = C_{M/r_C(M)}(\bar{0})$. Therefore $C_{M/r_C(M)}(\bar{0}) = \bar{0}$, i.e. $r_C\big(M/\,r_C(M)\big) = \bar{0}$, which means that r_C is a radical.

The proof is finished by the application of Proposition 1.3. □

Corollary 2.5. *If the operator $C \in \mathbb{CO}$ is maximal and idempotent, then $\Phi(C) = r_C$ is a radical of R-Mod.*

Combining Propositions 2.2 and 2.4 we obtain

Corollary 2.6. *The mappings (Φ, Ψ_1) define a monotone bijection between the **idempotent radicals** of R-Mod and the maximal, weakly hereditary, zero-idempotent closure operators of $\mathbb{CO}$.*

Now we will show the closure operators of $\mathbb{CO}$ which correspond to hereditary preradicals (pretorsions) of R-Mod.

Proposition 2.7. *If the closure operator $C \in \mathbb{CO}$ is **hereditary**, then the preradical $\Phi(C) = r_C$ is hereditary. If $r \in \mathbb{PR}$ is a hereditary preradical (pretorsion) of R-Mod, then the associated maximal closure operator $\Psi_1(r) = C^r$ is hereditary. Therefore the mappings (Φ, Ψ_1) define a monotone bijection between the pretorsions of R-Mod and the maximal hereditary closure operators of $\mathbb{CO}$.*

Proof. Let $C \in \mathbb{CO}$ be a hereditary closure operator. Then in the sitution $L \subseteq N \subseteq M$ we have $C_N(L) = C_M(L) \cap N$. For $L = O$ we obtain $C_N(O) = C_M(O) \cap N$, i.e. $r_C(N) = r_C(M) \cap N$, which means that the preradical r_C is hereditary.

Conversely, let r be a hereditary preradical of R-Mod, i.e. $r(N) = r(M) \cap N$ for every $N \subseteq M$. In the situation $L \subseteq N \subseteq M$ by heredity of r we have:

$$\big[\big((C^r)_M(L)\big) \cap N\big]/\,L = \big[\big((C^r)_M(L)\,\big)/\,L\big] \cap (N/\,L) =$$

$$= [r(M/\,L)] \cap (N/\,L) = r(N/\,L) = [(C^r)_N(L)]\,/\,L.$$

Therefore $[(C^r)_M(L)] \cap N = (C^r)_N(L)$, i. e. the operator C^r is hereditary. □

Corollary 2.8. *If the closure operator $C \in \mathbb{CO}$ is hereditary, then the associated maximal closure operator C^{r_C} also is hereditary.*

Taking into account the description of hereditary preradicals by the preradical filters of R $\big($Proposition 1.1, 1)$\big)$, from Proposition 2.7 follows

Corollary 2.9. *There exists a bijection between the preradical filters of the ring R and the maximal hereditary closure operators of $\mathbb{CO}$.*

More concretely, if $\mathcal{E}$ is a preradical filter of R (see [6]), then it defines a pretorsion $r_{\mathcal{E}}$ in R-Mod by the rule:

$$r_{\mathcal{E}}(M) = \{m \in M \mid (0 : m) \in \mathcal{E}\},$$

for every $M \in R$-Mod. The corresponding maximal closure operator $C^{r_{\mathcal{E}}}$ is defined as

$$(C^{r_{\mathcal{E}}})_M(N) = \{m \in M \mid (N : m) \in \mathcal{E}\}$$

for every $N \subseteq M$, where $(N : m) = \{a \in R \mid am \in N\}$.

From the other hand, if C is a maximal hereditary closure operator of $\mathbb{CO}$, then the associated preradical filter is $\mathcal{F}_1({}_RR) = \{I \in \mathbb{L}({}_RR) \mid C_R(I) = R\}$, i. e. the set of *C-dense* left ideals of R.

A very important type of preradicals of R-Mod are the *torsions* of this category and now we will indicate the closure operators of $\mathbb{CO}$ which correspond to the torsions of R-Mod. Since the torsions are hereditary radicals, the result follows by combining Propositions 2.4 and 2.7.

Corollary 2.10. *The mappings (Φ, Ψ_1) define a monotone bijection between the* ***torsions*** *of R-Mod and maximal, zero-idempotent, hereditary closure operators of $\mathbb{CO}$.*

The torsions of R-Mod are described by the radical filters of the ring R $\big($Proposition 1.1, 2)$\big)$, therefore is true

Corollary 2.11. *There exists a bijection between the* ***radical filters*** *of the ring R and the maximal, zero-idempotent, hereditary closure operators of $\mathbb{CO}$.*

The cases related to the cohereditary preradicals are considered in the following section, since for such preradicals the mappings Ψ_1 and Ψ_2 coincide.

3 The mappings (Φ, Ψ_2) and their effects

Now we will study the relations between the classes $\mathbb{CO}$ and $\mathbb{PR}$, defined by the mappings $\Phi : \mathbb{CO} \to \mathbb{PR}$ and $\Psi_2 : \mathbb{PR} \to \mathbb{CO}$, where $\Psi_2(r) = C_r$ and $(C_r)_M(N) = N + r(M)$. Every minimal closure operator is idempotent (Lemma 2.1). By Proposition 1.4 we have the monotone bijection $\mathbb{M}in(\mathbb{CO}) \cong \mathbb{PR}$ defined by (Φ, Ψ_2). We will restrict this bijection, considering various types of preradicals and showing properties of the corresponding closure operators.

We begin with the idempotent preradicals of R-Mod. Firstly we remind that by Proposition 2.2 if $C \in \mathbb{CO}$ is weakly hereditary, then the preradical $\Phi(C) = r_{_C}$ is idempotent. Now we verify the inverse transition: from $r \in \mathbb{PR}$ to $\Psi_2(r) = C_r$.

Proposition 3.1. *Let $r \in \mathbb{PR}$ be an **idempotent preradical** of R-Mod. Then the associated minimal closure operator $\Psi_2(r) = C_r$ is weakly hereditary. Therefore the mappings (Φ, Ψ_2) define a monotone bijection between the idempotent preradicals of R-Mod and the minimal weakly hereditary closure operators of $\mathbb{CO}$.*

Proof. If a preradical $r \in \mathbb{PR}$ is idempotent and $N \subseteq M$, then $r\big(r(M)\big) = r(M)$ and by definitions we have:

$$(C_r)_{(C_r)_{_M}(N)}(N) = N + r[(C_r)_M(N)] =$$

$$= N + r\big(N + r(M)\big) \supseteq N + r\big(r(M)\big) = N + r(M) = (C_r)_M(N).$$

Therefore $(C_r)_{(C_r)_{_M}(N)}(N) \supseteq (C_r)_M(N)$, and the inverse inclusion follows from the monotony of C_r, since $(C_r)_M(N) \subseteq M$. So we have $(C_r)_{(C_r)_{_M}(N)}(N) = (C_r)_M(N)$, i.e. the minimal closure operator C_r is weakly hereditary.

Taking into account the first statement of Proposition 2.2, from Proposition 1.4 now we obtain the indicated monotone bijection. □

Corollary 3.2. *If the closure operator $C \in \mathbb{CO}$ is weakly hereditary, then the associated minimal closure operator $C_{r_{_C}}$ also is weakly hereditary.*

We consider in continuation the *radicals* of R-Mod and look for the effect of the mapping Ψ_2 on the preradicals of such type. For that we need the following notion.

Definition 3.1. An operator $C \in \mathbb{CO}$ will be called **zero-radical** closure operator if $C_{M/C_M(O)}(\bar{0}) = \bar{0}$ for every $M \in R$-Mod.

Proposition 3.3. *If $r \in \mathbb{PR}$ is a **radical** of R-Mod, then the associated minimal closure operator $\Psi_2(r) = C_r$ is a zero-radical operator. If $C \in \mathbb{CO}$ is a zero-radical operator, then $\Phi(C) = r_{_C}$ is a radical. Therefore the mappings (Φ, Ψ_2) define a monotone bijection between the radicals of R-Mod and the minimal, zero-radical closure operators of $\mathbb{CO}$.*

Proof. If $r \in \mathbb{PR}$ is a radical of R-Mod, then for every $M \in R$-Mod we have:

$$(C_r)_{M/\,[(C_r)_{_M}(O)]}(\bar{0}) = (C_r)_{M/\,r(M)}(\bar{0}) = \bar{0} + r\big(M/\,r(M)\big) = \bar{0},$$

so C_r is a zero-radical closure operator.

Conversely, if $C \in \mathbb{CO}$ is a zero-radical closure operator, then by definition $r_C\big(M/\,r_C(M)\big) = C_{M/\,C_M(O)}(\bar{0}) = \bar{0}$ for every $M \in R$-Mod, i.e. r_C is a radical.

The conclusion of our statement now follows from Proposition 1.4. □

Remark. If $C \in \mathbb{CO}$ is a zero-radical closure operator, then each operator of the interval $[C_{r_C}, C^{r_C}]$ also is zero-radical, since the corresponding preradical coincides with r_C, which is a radical.

Combining Propositions 3.1 and 3.3 now we obtain

Corollary 3.4. *The mappings (Φ, Ψ_2) define a monotone bijection between the* ***idempotent radicals*** *of R-Mod and the minimal, weakly hereditary, zero-radical closure operators of $\mathbb{CO}$.*

The following step of our investigation is the consideration of the *hereditary preradicals* (*pretorsions*) of R-Mod. We remind that if an operator $C \in \mathbb{CO}$ is hereditary, then the preradical $\Phi(C) = r_C$ is hereditary (Proposition 2.7).

Proposition 3.5. *If a preradical $r \in \mathbb{PR}$ is* ***hereditary****, then the associated minimal closure operator $\Psi_2(r) = C_r$ is hereditary. Therefore the mappings (Φ, Ψ_2) define a monotone bijection between the hereditery preradicals (pretorsions) of R-Mod and the minimal hereditary closure operators of $\mathbb{CO}$.*

Proof. Let $r \in \mathbb{PR}$ be a hereditary preradical of R-Mod. Then in the situation $L \subseteq N \subseteq M$ by definition we have:

$$(C_r)_N(L) = L + (C_r)_N(O) = L + r(N), \quad (C_r)_M(L) = L + (C_r)_M(O) = L + r(M).$$

By the modularity of $\mathbb{L}(M)$ and the inclusion $L \subseteq N$, we obtain:

$$\big(L + r(M)\big) \cap N = L + \big(r(M) \cap N\big),$$

and by the heredity of r we have $r(M) \cap N = r(N)$. Therefore

$$[(C_r)_M(L)] \cap N = \big(L + r(M)\big) \cap N = L + \big(r(M) \cap N\big) = L + r(N) = (C_r)_N(L),$$

hence the closure operator C_r is hereditary.

The conclusion of our statement now follows from Propositions 2.7 and 1.4. □

Corollary 3.6. *If the closure operator $C \in \mathbb{CO}$ is hereditary, then the associated minimal closure operator C_{r_C} also is hereditary.*

Using Proposition 1.1, 1), now from Proposition 3.5 follows

Corollary 3.7. *There exist a bijection between the* ***preradical filters*** *of the ring R and the minimal hereditary closure operators of $\mathbb{CO}$.*

Similarly, from Proposition 1.1, 2), using Propositions 3.3 and 3.5, we obtain

Corollary 3.8. *There exists a bijection between the* ***radical filters*** *of the ring* R *(i.e. the* ***torsions*** *of* R*-Mod) and the minimal, zero-radical, hereditary closure operators of* $\mathbb{CO}$.

In continuation we consider the similar questions for the *cohereditary preradicals* of R-Mod. As was mentioned above, for such preradicals the mappings Ψ_1 and Ψ_2 coincide.

Proposition 3.9. *If* r *is a cohereditary preradical of* R*-Mod, then* $\Psi_1(r) = \Psi_2(r)$ *(i.e.* $C^r = C_r$*) and this closure operator is cohereditary. If* $C \in \mathbb{CO}$ *is a cohereditary closure operator (i.e. is maximal and minimal), then the preradical* $\Phi(C) = r_C$ *is cohereditary. Therefore the mappings* (Φ, Ψ_1) $\big($*or* $(\Phi, \Psi_2)\big)$ *define a monotone bijection between the cohereditary preradicals of* R*-Mod and the cohereditary closure operators of* $\mathbb{CO}$.

Proof. If a preradical $r \in \mathbb{PR}$ is cohereditary, then by the definition of C^r we have:

$$[(C^r)_M(N)] \,/\, N = r(M/N) = \big(r(M) + N\big)/\, N,$$

hence $(C^r)_M(N) = r(M) + N = (C_r)_M(N)$ for every $N \subseteq M$, and so $C^r = C_r$. Since this closure operator is maximal and minimal, it is cohereditary (Lemma 2.1).

Conversely, if $C \in \mathbb{CO}$ is a cohereditary closure operator, then by the maximality of C we have $r_C(M/N) = C_{M/N}(\bar{0}) = C_M(N)/\, N$. Further, from the minimality of C it follows that $C_M(O) + N = C_M(N)$, therefore

$$\big(r_C(M) + N\big)/\, N = \big(C_M(O) + N\big)/\, N = C_M(N)/\, N$$

for every $N \subseteq M$. From the foregoing now follows that $r_C(M/N) = \big(r_C(M)+N\big)/\, N$, i.e. the preradical r_C is cohereditary.

Applying Proposition 1.3 (or 1.4) now we obtain the announced bijection. □

Using Proposition 1.1, 3), we have

Corollary 3.10. *There exists a bijection between the* ***ideals*** *of the ring* R *and the cohereditary closure operators of* $\mathbb{CO}$.

The case of *cotorsions* of R-Mod is reduced to the combination of Proposition 3.9 with Proposition 2.2 (or 3.1), which give

Corollary 3.11. *The mappings* (Φ, Ψ_1) $\big($*or* $(\Phi, \Psi_2)\big)$ *define a monotone bijection between the* ***cotorsions*** *of* R*-Mod and weakly hereditary, cohereditary closure operators of* $\mathbb{CO}$.

The description of cotorsions of R-Mod by idempotent ideals of R $\big($Proposition 1.1, 4$\big)$ now implies

Corollary 3.12. *There exists a bijection between the* ***idempotent ideals*** *of the ring* R *and the weakly hereditary, cohereditary closure operators of* $\mathbb{CO}$.

Finally, we consider the case of *hereditary and cohereditary preradicals* of R-Mod (see Propositions 2.7 or 3.5, and 3.9).

Corollary 3.13. *The mappings* (Φ, Ψ_1) $\big($*or* $(\Phi, \Psi_2)\big)$ *define a monotone bijection between the hereditary and cohereditary preradicals of* R*-Mod and the hereditary, cohereditary closure operators of* $\mathbb{CO}$.

From Proposition 1.1, 5) now follows

Corollary 3.14. *There exists a bijection between the* ***still ideals*** *of the ring* R *and the hereditary, cohereditary closure operators of* $\mathbb{CO}$.

References

[1] Kashu A. I. *Closure operators in the categories of modules. Part* I (*Weakly hereditary and idempotent operators*). Algebra and Discrete Mathematics, 2013, **15**, No. 2, 213–228.

[2] Kashu A. I. *Closure operators in the categories of modules. Part* II (*Hereditary and cohereditary operators*). Algebra and Discrete Mathematics, 2013, **16**, No. 1, 81–95.

[3] Kashu A. I. *Closure operators in the categories of modules. Part* III (*Operations in* $\mathbb{CO}$ *and their properties*). Bul. Acad. Ştiinţe. Repub. Moldova, Mat., 2014, No. 1(74), 90–100.

[4] Bican L., Kepka T., Nemec P. *Rings, modules and preradicals*. Marcel Dekker, New York, 1982.

[5] Golan J. S. *Torsion theories*. Longman Scientific and Technical, New York, 1976.

[6] Kashu A. I. *Radicals and torsions in modules*. Kishinev, Ştiinţa, 1983 (in Russian).

[7] Dikranjan D., Giuli E. *Factorizations, injectivity and compactness in categories of modules*. Commun. in Algebra, 1991, **19**, No. 1, 45–83.

[8] Dikranjan D., Giuli E. *Closure operators* I. Topology and its Applications, 1987, **27**, 129–143.

[9] Dikranjan D., Tholen W. *Categorical structure of closure operators*. Kluwer Academic Publishers, 1995.

A. I. Kashu
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str. Chişinău, MD−2028
Moldova

E-mail: *kashuai@math.md*

Received March 3, 2014

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 23–29
ISSN 1024–7696

Bi-Deniable Public-Key Encryption Protocol which is Secure against Active Coercive Adversary

A. A. Moldovyan, N. A. Moldovyan, V. A. Shcherbacov

Abstract. We consider a practical public-key deniable encryption protocol based on the RSA cryptosystem. The protocol begins with the authentication of the both parties participating in the protocol (the sender and the receiver of secret message). The authentication is performed by exchanging random values and the RSA signatures to them. Due to this stage of the protocol the security against coercive attacks of the active adversary is provided. After the mutual authentication the protocol specifies performing the deniable encryption of the secret message, like the probabilistic ciphering of some fake message by using the RSA encryption algorithm. The novelty of the proposed protocol consists in using random values as single-use public keys that are used to generate single-use shared key with which the sender encrypts the secret message and the receiver discloses it. The coercive adversary provided with private keys of the both parties can only disclose the fake message. Proving that the sent cryptogram contains a message different from the fake one is computationally infeasible for the adversary.

Mathematics subject classification: 11T71, 94A60.
Keywords and phrases: Cryptographic protocols, public-key encryption, deniable encryption, probabilistic ciphering, factoring problem, entity authentication.

1 Introduction

When considering security of the encryption algorithms used in the communication protocols against potential attacks performed by the adversary that has power to force sender, receiver, or the both parties to open the shared secret key (if symmetric encryption algorithm is used), the private key (if asymmetric encryption algorithm is used), or both the shared key and the private one (if some combined encryption algorithm is used) one can state that conversional encryption algorithms do not provide security against the mentioned coercive attacks. Paper [1] introduces the notion of deniable encryption as the cryptographic primitive of cryptographic protocols that resist the coercive attacks. The deniable encryption is a procedure of ciphering a secret message such that the produced ciphertext can be decrypted with opened keys into a fake message. To provide such property (deniability) random values or additional secret key (which is not opened to the coercive attacker) in the process of the deniable encryption are used. Besides the information protection in the telecommunication systems, the potential practical application of deniable encryption schemes relates to providing secure multiparty computations [2] and preventing vote buying in the internet-voting systems [3].

Majority of the papers related to the deniable encryption are devoted to the public-key deniable encryption [2, 4–6]. A possible deniable encryption scheme of such type is as follows. The secret message T is encrypted with public-encryption algorithm E and public key P using a random value R : $C = E_P(T, R)$, where C is the produced cryptogram. While being coerced the sender (receiver) opens to adversary the fake message M and another random value r such that $E_P(M, r) = C$, where $r \neq R$ (the receiver additionally opens his private key connected with the public key P). Thus, it is supposed that the coercer is not able to disclose the value R, i.e. the last value plays role of the single-use secret key that is shared by the sender and the receiver. In this paper we propose a deniable encryption protocol which provides bi-deniability in the case of opening *all used random values send via communication channel*.

In the known papers different types of the coercive attacks are considered in which the adversary is passive, i. e. he approaches the parties of the secret communication protocol after the ciphertext has been sent. The sender-deniable, receiver-deniable, and sender- and receive-deniable (bi-deniable) protocols are possible in which coercive adversary attacks only the sender, only the receiver, and the both parties, respectively. It is supposed that a party or the both parties simultaneously should open to adversary all the private information related to the cryptogram (ciphertext) after it has been sent. The encryption is deniable if both the sender and receiver have possibility not to open the secret message, i. e. to lie, and the coercer is not able to disclose their lies.

However the coercive adversary can undertake an active attack in which he will play the role of the sender or of the receiver and after sending the secret message he will demand to open him the message contained in the cryptogram and the private key. For example, acting as sender in the protocol the attacker can generate and send two messages, the secret one and the fake one. Then he can demand the receiver's opening the cryptogram and private key. If the receiver opens only one message, then the attack is considered successful, since the attacker is able to argue that the receiver lies, presenting alternative message contained in the cryptogram. The deniable encryption protocol proposed in the present paper provides security against the active attacks (here we not use the term *deniability* since authentic party stops the protocol before performing encryption of messages if an adversary tries to perform an active attack). The security is provided with the RSA signatures to random values send via the channel.

The present paper is organized as follows. Section 2 describes the model of the coercive attack and the design criteria for constructing the deniable encryption protocol. Section 3 describes the constructed deniable encryption protocol deniability of which is based on the computational indistinguishability between the deniable encryption procedure and the probabilistic ciphering of the fake message. The described protocol is based on the RSA cryptosystem (that is briefly described) to perform several passes of the protocol. Section 4 discusses the security and bi-deniability provided by the protocol. Section 5 concludes the paper.

2 Model of the coercive adversary and design criteria

The assumed model of the coercive attack is described by the following four items.

1. The adversary can impersonate some sender and initiate the deniable encryption protocol by using public key of the receiver and after a ciphertext has been sent he can force the receiver to open the received message and receiver's private key.

2. The adversary can impersonate some receiver and after the protocol terminates can force the sender to open the sent message and sender's private key (in the constructed protocol public keys of both the sender and the receiver of the message are used).

3. All data (cryptogram, random values et. al.) sent via communication channels become known to the adversary.

4. The adversary is not able to force a party to open private key before the deniable encryption protocol terminates.

To resist the attacks of the assumed adversary the deniable encryption protocol has been constructed with the following design criteria:

i) the protocol should include the stage of verifying the authenticity of both the sender and the receiver with using random values and the RSA digital signature scheme;

ii) the random values used at the authentication stage should be used as single-use public keys of the sender and of the receiver at the stage of deniable encryption; disclosing such use of the random values should be computationally infeasible for the coercive attacker;

iii) the single-use public keys should serve to compute single-use shared key;

iv) the single-use shared keys should be used for pseudo-randomizing the encryption process;

v) a probabilistic public-key encryption algorithm should be associated with the deniable encryption algorithm; the encryption should be performed using the RSA public key of the receiver;

vi) the ciphertext produced by the deniable encryption algorithm should be computationally indistinguishable from the ciphertext produced by the probabilistic encryption algorithm.

3 Proposed protocol

3.1 Cryptosystem RSA

The RSA public key cryptosystem [7] can be used for public encryption and for signing electronic messages. This cryptosystem is described as follows. The public key is represented by a pair of numbers $(n,\ e)$, where $n\ =\ pq$ is the product of two randomly chosen primes and e is a random number that is relatively prime with Euler phi function $\phi(n)\ =\ (p\ -\ 1)(q\ -\ 1)$. The triple $(p,\ q,\ d)$ is secret, where $d\ =\ e^{-1}\ \bmod \phi(n)$ is a private key. The encryption of some message $M\ <\ n$ is

performed using the public key as the computation of the value $C = M^e \mod n$ that is the output ciphertext of the public-key encryption procedure. The decryption of the cryptogram C is performed using the private key and the formula $M = C^d \mod n$. The RSA signature S to the message M is computed using the private key and the formula $S = M^d \mod n$. The verification of the signature is performed using public key and formula $M = S^e \mod n$. If the last equation holds, then the signature is accepted as a valid one.

Usually the documents to be signed have arbitrary size and are comparatively long. In such cases some specified hash-function F_H is used and the signature S to document M is generated as signature to the hash-value $H = F_H(M)$: $S = H^d \mod n$. The security of the RSA cryptosystem is based on the difficulty of factoring modulus n. Factoring n is a computationally difficult problem if the primes p and q are strong ones [8] and have large size. For example, using 512-bit (1232-bit) strong primes p and q one gets the security equal to 2^{80} (2^{128}) modulo n multiplication operations.

3.2 Public-key deniable encryption protocol

Let Alice be a sender of the secret message T and Bob be a receiver. Suppose also they are users of the RSA cryptosystem; the pair of numbers (n_1, e_1) is Alice's public key; d_1 is her private key; (n_2, e_2) is Bob's public key; d_2 is his private key. Besides, Bob public key is such that the number $P = 2n_2 + 1$ is prime and order of the number 3 is equal to $2n_2$ or n_2. Earlier primes with such structure were used in papers [9, 10]. The protocol designed using the design criteria declared in Section 2 includes the following steps:

1. Alice generates a random value k_1 and computes $R_1 = 3^{k_1} \mod P$ and sends the value R_1 to Bob as her random choice.

2. Bob generates a random value k_2, computes the value $R_2 = 3^{k_2} \mod P$ and his signature S_2 to the sum $(R_1 + R_2 \bmod n_2) : S_2 = (R_1 + R_2)^{d_2} \mod n_2$. Then he sends the values R_2 and S_2 to Alice.

3. Alice verifies Bob's signature to the value $(R_1 + R_2 \bmod n_2)$. If the signature S_2 is false she terminates the protocol. If the signature S_2 is valid, she computes her signature S_1 to the value $(R_1 + R_2 \mod n_2) : S_1 = (R_1 + R_2)^{d_1} \mod n_1$. Then Alice generates a fake message M, computes the values $Z_1 = R_2^{k_1} \mod P$, $V = TZ_1 \mod n_2$, $C_1 = (M + V)^{e_2} \mod n_2$, and $C_2 = V^{e_2} \mod n_2$, and sends the ciphertext (C_1, C_2) and signature S_1 to Bob.

4. Bob verifies Alice's signature to the value $(R_1 + R_2 \bmod n_2)$. If the signature S_1 is false he terminates the protocol. If the signature S_1 is valid, he computes the values $Z_2 = R_1^{k_2} \mod P$ and $V = C_2^{d_2} \mod n_2$. Then he computes the value $T' = VZ_2^{-1} \mod n_2$ that is equal to T, i.e. he discloses the secret message T sent by Alice. (Indeed we have the following: $Z_2 \equiv R_1^{k_2} \equiv 3^{k_1 k_2} \bmod P; Z_1 \equiv R_2^{k_1} \equiv 3^{k_2 k_1} \bmod P \Rightarrow Z_2 = Z_1 \Rightarrow T' \equiv VZ_2^{-1} \equiv VZ_1^{-1} \equiv TZ_1Z_1^{-1} \equiv T \mod n_2 \Rightarrow T' \equiv T$.)

4 Discussion

The presented protocol satisfies the design criteria formulated in Section 2:

i) Alice (Bob) proves her (his) authenticity by signing the value $(R_1+R_2 \bmod n_2)$ that depends on Bob's (Alice's) random choice; the signatures are computed using the RSA cryptoscheme;

ii) the random values R_1 and R_2 are connected with the single-use private keys k_1 and k_2 and actually represent the single-use public keys generated by Alice and Bob, correspondingly;

iii) the single-use public keys R_1 and R_2 are used at the stage of deniable encryption for computing the single-use shared key $Z = Z_1 = Z_2$;

iv) the single-use shared key Z is used for computing pseudo-random value $V = TZ \mod n_2$ that contains the secret message T and is used for randomizing the encryption of the fake message M;

v) a probabilistic public-key encryption algorithm associated with the deniable encryption algorithm is as follows:
– generate random value W,
– encrypt the message M with formula $C_1 = (M + W)^{e_2} \mod n_2$,
– encrypt the value W using formula $C_2 = W^{e_2} \mod n_2$;

vi) if $W = V$, then the associated probabilistic encryption algorithm generates the same ciphertext as that produced by the public-key deniable encryption algorithm; to distinguish between the probabilistic encryption and the deniable encryption one should open the value V and disclose the secret message T, however this is computationally infeasible. The security of the proposed protocol against active attacks is provided due to performing the authentication stage. Alice sends the ciphertext to Bob only after his proving ability to sign correctly a random value. Respectively, Bob decrypts the ciphertext only after Alice's proving her authenticity with her signature to a value depending on Bob's random choice R_2. Thus, the active coercive attacker is detected before performing procedures connected directly with the deniable encryption. In the case of passive coercive attack the public-key encryption stage of the protocol is performed and the sender opens to coercer the fake message M. The receiver opens to coercer both the message M and private key d_2. However the coercer can open only the randomization parameter V that connects the fake message M and the ciphertext (C_1, C_2). For an arbitrary plaintext T' there exists a single-use key Z' such that $V = T'Z' \mod n_2$. To disclose the secret message coercer need to know at least one of the values k_1 and k_2, i.e. he should compute the discrete logarithm $\log_3 R_1 \mod P$ or $\log_3 R_2 \mod P$.

Since the prime P has a large size (more than 1025 bits (2465 bits) in the case of 80-bit (128-bit) security), the number $P-1$ contains large prime factors (numbers p and q), and number 3 has a large order ω ($\omega \geq pq$), the discrete logarithm problem is computationally difficult and it is supposed the coercer is not able to find discrete logarithms modulo P. Thus, the proposed protocol provides bi-deniability.

The considered protocol has the following merits:

– it is bi-deniable;

– it is sufficiently fast (its performance if only about two times lower than the rate of the RSA public-key encryption);

– its overhead in terms of the ciphertext size is comparatively low (only 100% larger than the ciphertext produced by the RSA encryption algorithm);

– it can be easily implemented in practice using the RSA public-key infrastructure.

5 Conclusion

A practical and computationally efficient bi-deniable public-key encryption protocol has been proposed. The bi-deniability of the method is based on associating a probabilistic public-key encryption algorithm with the deniable encryption algorithm in such a way that both algorithms produce the same ciphertext. One can suppose that the computational indistinguishability between the probabilistic and deniable encryption can serve as a novel design concept for constructing deniable encryption schemes of different types. Due to performing the authentication of the both parties of the protocol provides the security against active coercive attacks. Including in the protocol the user's authentication mechanism provides also a natural argumentation for using random values in the protocol. A novel item applied in the proposed protocol consists in using the mentioned random values as single-use public keys R_1 and R_2 and performing hidden key agreement subprotocol with which the sender and the receiver of the message obtain the single-use shared key Z. To distinguish the random values R_1 and R_2 from the random values that are generated directly the coercer should compute the discrete logarithm modulo P. The last means the deniability of the proposed protocol is based on the computational difficulty of finding discrete logarithms.

The first author was supported by Government of Russian Federation, Grant 074-U01 and the second author supported by the Board of Education of Russia.

References

[1] Canetti R., Dwork C., Naor M., Ostrovsky R. *Deniable Encryption.* Proceedings Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer–Verlag. Berlin, Heidelberg, New York, 1997, vol. 1294, 90–104.

[2] Ishai Yu., Kushilevits E., Ostrovsky R. *Efficient Non-interactive Secure Computation.* Advances in Cryptology – EUROCRYPT 2011. Lectute Notes in Computer Science. Springer–Verlag. Berlin, Heidelberg, New York, 2011, vol. 6632, 406–425.

[3] Bo Meng. *A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext.* Journal of Networks. 2009, **4**, No. 5, 370–377.

[4] O'Neil A., Peikert C., Waters B. *Bi-Deniable Public-Key Encryption.* Advances in Cryptology – CRYPTO 2011. Lectute Notes in Computer Science. Springer–Verlag. Berlin, Heidelberg, New York, 2011, vol. 6841, 525–542.

[5] Klonowski M., Kubiak P., Kutylowsk M. *Practical Deniable Encryption* SOFSEM 2008: Theory and Practice of Computer Science, 34th Conference on Current Trends in Theory and Practice of Computer Science, Novy Smokovec, Slovakia, January 19–25, 2008, 599–609.

[6] Bo Meng, Jiang Qing Wang. *A Receiver Deniable Encryption Scheme*. Proceedings of the 2009 International Symposium on Information Processing (ISOP'09), Huangshan, China, August 21–23, 2009, 254–257.

[7] Rivest R.L., Shamir A., and Adleman L.M. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*. Communications of the ACM, 1978, **21**, No. 2, 120–126.

[8] Gordon J. *Strong primes are easy to find*. Advances in cryptology – EUROCRYPT'84, Springer-Verlag LNCS, 1985, vol. 209, 216–223.

[9] Moldovyan N. A. *An approach to shorten digital signature length*. Computer Science Journal of Moldova, 2006, **14**, No. 3(42), 390–396.

[10] Moldovyan A. A., Moldovyan N. A., Shcherbacov V. A. *Short signatures from difficulty of the factoring problem*. Bul. Acad. Ştiinţe Repub. Moldova, Mat., 2013, No. 2(72)–3(73), 27–36.

Received April 2, 2014

A. A. Moldovyan
Saint-Petersburg National Research University
of Information Technologies, Mechanics and Optics
Kronverksky pr., 10, St.Petersburg, 197101
Russia
E-mail: *maa1305@yandex.ru*;

N. A. Moldovyan
Saint-Petersburg Electrotechnical University "LETI"
Prof. Popova str., 5, St.Petersburg, 197342
Russia
E-mail: *nmold@mail.ru*;

V. A. Shcherbacov
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD−2028 Chişinău
Moldova
E-mail: *scerb@math.md*; Web: *www.scerb.com*

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 30–37
ISSN 1024–7696

The endomorphism semigroup of a free dimonoid of rank 1

Yurii V. Zhuchok

Abstract. We describe all endomorphisms of a free dimonoid of rank 1 and construct a semigroup which is isomorphic to the endomorphism semigroup of this free dimonoid. Also, we give an abstract characteristic for the endomorphism semigroup of a free dimonoid of rank 1.

Mathematics subject classification: 08A05.
Keywords and phrases: Free dimonoid, endomorphism semigroup, isomorphism.

1 Introduction

The notion of a dimonoid was introduced by Jean-Louis Loday in [1]. An algebra $(D, \dashv, \vdash)$ with two binary associative operations $\dashv$ and $\vdash$ is called *a dimonoid* if for all $x, y, z \in D$ the following conditions hold:

$$(x\dashv y)\dashv z = x\dashv(y\vdash z),$$
$$(x\vdash y)\dashv z = x\vdash(y\dashv z),$$
$$(x\dashv y)\vdash z = x\vdash(y\vdash z).$$

Algebras of dimension one play a special role in studying different properties of algebras of an arbitrary dimension. For example, free triods of rank 1 were described in [2] and used for building free trialgebras. Semigroups of cohomological dimension one are used in algebraic topology [3]. With the help of properties of free dimonoids (in particular, of rank 1), free dialgebras were described and a cohomology of dialgebras was investigated [1]. More general information on dimonoids and examples of some dimonoids can be found, e. g., in [1, 4–6].

Observe that if the operations of a dimonoid coincide, then the dimonoid becomes a semigroup. For a free dimonoid the operations are distinct, however every free semigroup can be obtained from the free dimonoid by a suitable factorization. It is well known that the endomorphism semigroup of a free semigroup (free monoid) of rank one is isomorphic to the multiplicative semigroup of positive (nonnegative) integers. Endomorphism semigroups of a free monoid and a free semigroup of a nontrivial rank were described by G. Mashevitzky and B. M. Schein [7]. The structure of the endomorphism semigroup of a free group was investigated by E. Formanek [8]. In this paper, we study the endomorphism semigroup of a free dimonoid of rank 1.

The paper is organized as follows. In Section 2, we give necessary definitions and auxiliary assertions. In Section 3, we describe all endomorphisms of a free dimonoid of rank 1 and construct a semigroup which is isomorphic to the endomorphism semigroup of the given free dimonoid. In Section 4, we prove that free dimonoids of rank 1 are determined by their endomorphism semigroups and give an abstract characteristic for the endomorphism semigroup of a free dimonoid of rank 1.

2 Preliminaries

Let $\mathfrak{D}_1 = (D_1, \dashv_1, \vdash_1)$ and $\mathfrak{D}_2 = (D_2, \dashv_2, \vdash_2)$ be arbitrary dimonoids. A mapping $\varphi : D_1 \to D_2$ is called *a homomorphism* of $\mathfrak{D}_1$ into $\mathfrak{D}_2$ if for all $x, y \in D_1$ we have:

$$(x \dashv_1 y)\varphi = x\varphi \dashv_2 y\varphi, \;\; (x \vdash_1 y)\varphi = x\varphi \vdash_2 y\varphi.$$

A bijective homomorphism $\varphi : D_1 \to D_2$ is called *an isomorphism* of $\mathfrak{D}_1$ into $\mathfrak{D}_2$. In this case dimonoids $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are called *isomorphic* .

Let X be an arbitrary set and $\overline{X} = \{\overline{x} \mid x \in X\}$. Define two binary operations on the set

$$Fd(X) = \overline{X} \cup \left(\overline{X} \times X\right) \cup \left(X \times \overline{X}\right) \cup$$

$$\cup(\overline{X} \times X \times X) \cup (X \times \overline{X} \times X) \cup (X \times X \times \overline{X}) \cup \ldots$$

as follows:

$$(x_1, \ldots, \overline{x_i}, \ldots, x_k) \dashv (y_1, \ldots, \overline{y_j}, \ldots, y_l) = (x_1, \ldots, \overline{x_i}, \ldots, x_k, y_1, \ldots, y_l)\,,$$

$$(x_1, \ldots, \overline{x_i}, \ldots, x_k) \vdash (y_1, \ldots, \overline{y_j}, \ldots, y_l) = (x_1, \ldots, x_k, y_1, \ldots, \overline{y_j}, \ldots, y_l)\,.$$

The algebra $(Fd(X), \dashv, \vdash)$ is *a free dimonoid* (see [1]). Elements of $Fd(X)$ are called *words* and $\overline{X}$ is *the generating set* of $(Fd\,(X)\,, \dashv, \vdash)$. By $|\omega|$ we denote *the length* of a word $\omega \in Fd(X)$.

Note that a free dimonoid can be defined in another way. Let X^+ be the free semigroup on an alphabet X and $|w|$ be the length of $w \in X^+$. By N we denote the set of all positive integers.

On the set

$$\tilde{F}[X] = \{(w; m) \in X^+ \times N : |w| \geq m\}$$

we define operations $\dashv', \vdash'$ by the rule:

$$(w_1, m_1) \dashv' (w_2, m_2) = (w_1 w_2, m_1),$$

$$(w_1, m_1) \vdash' (w_2, m_2) = (w_1 w_2, |w_1| + m_2).$$

Proposition 1 (see [9, Lemma 3])**.** *The free dimonoid* $(Fd(X), \dashv, \vdash)$ *is isomorphic to the dimonoid* $(\tilde{F}[X], \dashv', \vdash')$.

We denote the free dimonoid $(Fd(X), \dashv, \vdash)$ on an n-element set X by Fd_n. Now we consider the structure of the free dimonoid Fd_1.

Let $X = \{x\}$, then

$$Fd_1 = \{\overline{x}, (\overline{x}, x), (x, \overline{x}), (\overline{x}, x, x), (x, \overline{x}, x), (x, x, \overline{x}), ...\}.$$

Define on the set

$$P = \{(a; b) \in N \times N \mid a \geq b\}$$

two binary operations $\prec$ and $\succ$ as follows:

$$(\ a; b) \prec (c; d) = (a + c; b),$$

$$(\ a; b) \succ (c; d) = (a + c; a + d).$$

Proposition 2 (see [9, Lemma 4])**.** *The free dimonoid $(Fd_1, \dashv, \vdash)$ of rank 1 is isomorphic to the dimonoid $(P, \prec, \succ)$.*

Further we will identify elements of the free dimonoid $(Fd_1, \dashv, \vdash)$ with respective elements of the dimonoid $(P, \prec, \succ)$.

3 Endomorphisms of a free dimonoid of rank 1

For an arbitrary dimonoid $\mathfrak{D} = (D, \dashv, \vdash)$, by $End(\mathfrak{D})$ we denote the semigroup of all endomorphisms of the dimonoid $\mathfrak{D}$. First of all, we describe the structure of endomorphisms of a free dimonoid of rank 1.

Theorem 1. *For any $(k; l) \in P$ a transformation $\xi_{k,l}$ of the free dimonoid $(Fd_1, \dashv, \vdash)$ defined by $(a; b)\xi_{k,l} = (ak; (b - 1)k + l)$ is a monomorphism. Also every endomorphism of $(Fd_1, \dashv, \vdash)$ has the above form.*

Proof. Fix an arbitrary pair $(k; l) \in P$ and take $(a; b), (c; d) \in Fd_1$. Then

$$((a; b) \prec (c; d))\xi_{k,l} = (a + c; b)\xi_{k,l} =$$

$$= ((a + c)k; (b - 1)k + l) =$$

$$= (ak; (b - 1)k + l) \prec (ck; (d - 1)k + l) =$$

$$= (a; b)\xi_{k,l} \prec (c; d)\xi_{k,l}$$

and

$$((a; b) \succ (c; d))\xi_{k,l} = (a + c; a + d)\xi_{k,l} =$$

$$= ((a + c)k; (a + d - 1)k + l) =$$

$$= (ak; (b - 1)k + l) \succ (ck; (d - 1)k + l) =$$

$$= (a; b)\xi_{k,l} \succ (c; d)\xi_{k,l}.$$

Therefore, $\xi_{k,l} \in End(Fd_1)$ for all $(k; l) \in P$.

Suppose that $(a;b)\xi_{k,l} = (c;d)\xi_{k,l}$ for some $(a;b),(c;d) \in Fd_1$. Then

$$(ak;(b-1)k+l) = (ck;(d-1)k+l),$$

whence $a = c, b = d$. Thus, $\xi_{k,l}$ is a monomorphism for all $(k;l) \in P$.

Now, let ξ be an arbitrary endomorphism of $(Fd_1, \dashv, \vdash)$ and $(1;1)\xi = (k;l)$. By induction on a, we show that

$$(a;a)\xi = (ak;(a-1)k+l)$$

for all $(a;a) \in Fd_1$.

For $a = 1$ this is obvious and for $a = 2$ we have

$$(2;2)\xi = ((1;1) \succ (1;1))\xi = (k;l) \succ (k;l) = (2k;k+l).$$

Assume that $(n;n)\xi = (nk;(n-1)k+l)$ for some $n \in N, n \geq 3$. Then for $a = n+1$ we obtain

$$(n+1;n+1)\xi = ((n;n) \succ (1;1))\xi =$$

$$= (n;n)\xi \succ (1;1)\xi = (nk;(n-1)k+l) \succ (k;l) =$$

$$= ((n+1)k;nk+l).$$

So, by induction $(a;a)\xi = (ak;(a-1)k+l)$ for all $a \in N$.

Finally, for all $(a;b) \in Fd_1$, where $a > b$,

$$(a;b)\xi = ((b;b) \prec (a-b;a-b))\xi =$$

$$= (b;b)\xi \prec (a-b;a-b)\xi =$$

$$= (bk;(b-1)k+l) \prec ((a-b)k;(a-b-1)k+l) =$$

$$= (ak;(b-1)k+l).$$

Thus, $\xi = \xi_{k,l}$ and the theorem is proved. □

Further we consider a binary operation $\circ$ on N defined as follows:

$$(a;b) \circ (c;d) = (ac;(b-1)c+d).$$

Note that if $a \geq b, c \geq d$, then $ac = (a-1)c + c \geq (b-1)c + d$. Therefore, the operation $\circ$ is completed on the set $P = \{(a;b) \in N \times N \mid a \geq b\}$ and so the algebra $(P, \circ)$ is a semigroup.

Theorem 2. *The endomorphism semigroup $End(Fd_1)$ of the free dimonoid $(Fd_1, \dashv, \vdash)$ is isomorphic to the semigroup $(P, \circ)$.*

Proof. Define a mapping Θ of $End(Fd_1)$ into $(P, \circ)$ by $\xi_{k,l}\Theta = (k; l)$ for all $\xi_{k,l} \in End(Fd_1)$. Obviously, Θ is a bijection.

Let $\xi_{k,l}, \xi_{p,q} \in End(Fd_1)$ and $(a; b) \in P$. Then

$$(a; b)\xi_{k,l}\xi_{p,q} = (ak; (b-1)k + l)\xi_{p,q} =$$

$$= (akp; bkp - kp + lp - p + q) =$$

$$= (akp; ((b-1)k + l - 1)p + q) =$$

$$= (a; b)\xi_{kp,lp-p+q}.$$

Hence $\xi_{k,l}\xi_{p,q} = \xi_{kp,lp-p+q}$ and so

$$(\xi_{k,l}\xi_{p,q})\Theta = \xi_{kp,lp-p+q}\Theta = (kp; lp - p + q) =$$

$$= (k; l) \circ (p; q) = \xi_{k,l}\Theta \circ \xi_{p,q}\Theta.$$

□

We will identify elements of $End(Fd_1)$ with respective elements of $(P, \circ)$.

It is obvious that the automorphism group of $(Fd_1, \dashv, \vdash)$ is trivial.

4 Characteristics of the monoid $End(Fd_1)$

There is a number of algebras properties of which are determined by properties of their endomorphism semigroups. Definability conditions and some other characteristics for the endomorphism semigroup of a free semigroup (free monoid) and a free group were obtained in [7] and [8], respectively. An abstract characteristic for the endomorphism semigroup of a free group was described by V. M. Usenko [10].

Theorem 3. *Let X be a singleton set, Y be an arbitrary set and there exists an isomorphism $\Theta : End(Fd(X)) \to End(Fd(Y))$. Then free dimonoids $(Fd(X) \dashv, \vdash)$ and $(Fd(Y), \dashv, \vdash)$ are isomorphic.*

Proof. Assume that $|\overline{Y}| \geq 2$ and $y \in \overline{Y}$. By $E(Fd(X))$ and $E(Fd(Y))$ we denote the set of all idempotents of $End(Fd(X))$ and, respectively, $End(Fd(Y))$. Since Θ is an isomorphism, then $E(Fd(X))\Theta = E(Fd(Y))$.

For arbitrary $(k; l) \in Fd(X)$, we have $(k; l) \in E(Fd(X))$ if and only if $(k^2; (l-1)k + l) = (k; l)$, whence $k = l = 1$. Thus, $|E(Fd(X))| = 1$.

Define a transformation φ_y of $\overline{Y}$ by the rule: $t\varphi_y = y$ for all $t \in \overline{Y}$. Further we extend φ_y to a transformation Φ_y of the dimonoid $(Fd(Y), \dashv, \vdash)$ which is defined as follows:

$$(u_1, ..., \overline{u_i}, ..., u_k)\Phi_y = u_1\varphi_y \vdash ... \vdash \overline{u_i\varphi_y} \dashv ... \dashv u_k\varphi_y$$

for all $(u_1, ..., \overline{u_i}, ..., u_k) \in Fd(Y)$.

Thus, for all $t \in \overline{Y}$ we have

$$t\Phi_y^2 = (t\Phi_y)\Phi_y = y\Phi_y = y = t\Phi_y,$$

whence $\Phi_y^2 = \Phi_y$. Taking into account the identity automorphism of $End(Fd(Y))$, we obtain $|E(Fd(Y))| \geq 3$ that contradicts the condition $E(Fd(X))\Theta = E(Fd(Y))$. So, $|\overline{Y}| = 1$ and $(Fd(X)\ \dashv, \vdash)$, $(Fd(Y), \dashv, \vdash)$ are isomorphic dimonoids. □

In addition, the semigroup $End(Fd_1)$ can be represented as a semilattice of some their subsemigroups. Indeed, let

$$P_1 = \{(1;1)\}, P_2 = (N \setminus \{1\}) \times \{1\},$$

$$P_3 = \{(n;n) | n \in N, n \neq 1\}$$

and

$$P_4 = \{(m;n) \in N \times N | m > n, n \neq 1\}.$$

It is obvious that each of sets $P_i, 1 \leq i \leq 4$, is a subsemigroup of the monoid $End(Fd_1)$. We put $\Omega = \{1, 2, 3, 4\}$ and define on Ω the following operation:

$$1 \cdot i = i = i \cdot 1,\ \ 4 \cdot i = 4 = i \cdot 4 \text{ and}$$

$$i \cdot i = i,\ \ 2 \cdot 3 = 4 = 3 \cdot 2\ \ (1 \leq i \leq 4).$$

It is easy to see that $(\Omega, \cdot)$ is a commutative semigroup of idempotents, that is a semilattice.

Proposition 3. *The monoid $End(Fd_1)$ is a semilattice $(\Omega, \cdot)$ of semigroups P_i, $i \in \Omega$. Moreover, P_2 and P_3 are isomorphic to the free commutative semigroup with the countably infinite set of free generators that are prime numbers.*

Proof. Define a mapping η of $End(Fd_1)$ onto $(\Omega, \cdot)$ as follows:

$$(a;b)\eta = i,\ \text{ if } (a;b) \in P_i.$$

A direct check shows that η is a homomorphism and semigroups P_2, P_3 and the multiplicative semigroup $(N \setminus \{1\}, \cdot)$ are isomorphic. □

Further we describe an abstract characteristic of $End(Fd_1)$. Recall that an ideal I of a semigroup S is called *densely embedded* (see [11, 12]) if every nontrivial homomorphism (that is not an isomorphism) of S induces a nontrivial homomorphism of I, and for every semigroup T such that $S \subset T$ and I is an ideal of T, there exists a nontrivial homomorphism of T which induces an isomorphism on I.

A semigroup S is called *reductive on the left* if for $a, b \in S$ the condition $ua = ub$ for all $u \in S$, implies $a = b$. If for a semigroup S there do not exist distinct a_1, a_2 such that $a_1 x = a_2 x, xa_1 = xa_2$ for all $x \in S$, then S is called *a weakly reductive semigroup*. It is clear that every reductive on the left semigroup is weakly reductive.

Let $\Im(X)$ be the symmetric semigroup of all transformations on X and S be an arbitrary semigroup. As is well known, a homomorphism

$$\rho : S \to \Im(S) : t \mapsto \rho_t,$$

where $u\rho_t = ut$ for all $u \in S$, is called *a regular representation* of S.

For every ideal I of a semigroup S, a regular representation ρ induces the following representation:

$$\rho^I : S \to \Im(I) : t \mapsto \rho_t|_I,$$

where $\rho_t|_I$ is the restriction of $\rho_t \in \Im(S)$ to I.

An ideal I of a semigroup S is called *essential* [10] if the induced regular representation ρ^I is an injective mapping.

Proposition 4 (see [10])**.** *For an ideal I of a semigroup S the following conditions are equivalent:*

(i) I is essential;

(ii) I is densely embedded and reductive on the left.

For an arbitrary semigroup S, by $T(S)$ we denote the translation hull (see, e. g., [12]) of S and by $T_0(S)$ the inner part of $T(S)$. If S is a weakly reductive semigroup, then S is isomorphic to $T_0(S)$.

Finally, we obtain an abstract characteristic for the endomorphism semigroup of a free dimonoid of rank 1.

Theorem 4. *An arbitrary semigroup S is isomorphic to the endomorphism semigroup $End(Fd_1)$ of the free dimonoid $(Fd_1, \dashv, \vdash)$ if and only if S contains a densely embedded ideal isomorphic to the semigroup P_4.*

Proof. Let $S \cong End(Fd_1)$, then S contains up to isomorphism the semigroup P_4. From Proposition 3 it follows that P_4 is an ideal of $End(Fd_1)$. We show that the ideal P_4 is essential.

Suppose there exist $(a; b), (c; d) \in End(Fd_1)$ for which $(a; b)\rho^{P_4} = (c; d)\rho^{P_4}$, that is $\rho_{(a;b)}|_{P_4} = \rho_{(c;d)}|_{P_4}$.

Then for all $(x; y) \in P_4$ we have

$$(a; b)(x; y) = (c; d)(x; y),$$

$$(ax; (b-1)x + y) = (cx; (d-1)x + y),$$

whence $a = c$, $b = d$ by reductivity of the multiplicative monoid $(N, \cdot)$. Therefore, ρ^{P_4} is injective and then P_4 is an essential ideal. Thus, by Proposition 4, P_4 is a densely embedded ideal for the semigroup $End(Fd_1)$.

Conversely, let a semigroup S contain a densely embedded ideal I isomorphic to P_4. Then as is known [11], $T(P_4) \cong End(Fd_1)$ and $T(I) \cong S$, whence S and $End(Fd_1)$ are isomorphic. □

References

[1] Loday J.-L. *Dialgebras, In: Dialgebras and related operads.* Lecture Notes in Math. **1763**, Springer, Berlin, 2001, 7–66.

[2] Loday J.-L., Ronco M. O. *Trialgebras and families of polytopes.* Contemp. Math., 2004, **346**, 369–398.

[3] Novikov B. V. *Semigroups of cohomological dimension one.* J. Algebra, 1998, **204**, No. 2, 386–393.

[4] Pozhidaev A. P. *0-dialgebras with bar-unity and nonassociative Rota-Baxter algebras.* Siberian Math. J., 2009, **50**:6, 1070–1080.

[5] Zhuchok A. V. *Dimonoids.* Algebra and Logic, 2011, **50**:4, 323–340.

[6] Zhuchok Yu. V. *Representations of ordered dimonoids by binary relations.* Asian-Eur. J. Math., 2014, **07**, No. 1, 1450006, 13 pp.

[7] Mashevitzky G., Schein B. M. *Automorphisms of the endomorphism semigroup of a free monoid or a free semigroup.* Proc. Amer. Math. Soc., 2003, **131**, No. 6, 1655–1660.

[8] Formanek E. *A question of B. Plotkin about the semigroup of endomorphisms of a free group.* Proc. Amer. Math. Soc., 2002, **130**, 935–937.

[9] Zhuchok A. V. *Free dimonoids.* Ukrain. Math. J., 2011, **63**, No. 2, 196–208.

[10] Usenko V. M. *Semigroups of endomorphisms of free groups.* Problems in Algebra, Gomel: Izv. Gomelskogo universiteta, 2000, **3**:16, 182–185 (in Russian).

[11] Gluskin L. M. *Ideals of semigroups.* Mat. Sb., 1961, **55(97)**:4, 421–448 (in Russian).

[12] Shevrin L. N. *Densely embedded ideals of semigroups.* Mat. Sb., 1969, **79(121)**:3(7), 425–432 (in Russian).

Yurii V. Zhuchok
Kyiv Taras Shevchenko National University
Department of Mechanics and Mathematics
Volodymyrska str., 64, 01033 Kyiv
Ukraine

E-mail: *zhuchok_y@mail.ru*

Received May 5, 2014

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 38–48
ISSN 1024–7696

Equivalence of pairs of matrices with relatively prime determinants over quadratic rings of principal ideals

Natalija Ladzoryshyn, Vasyl' Petrychkovych

Abstract. A special equivalence of matrices and their pairs over quadratic rings is investigated. It is established that for the pair of $n \times n$ matrices A, B over the quadratic rings of principal ideals $\mathbb{Z}[\sqrt{k}]$, where $(detA, detB) = 1$, there exist invertible matrices $U \in GL(n, \mathbb{Z})$ and $V^A, V^B \in GL(n, \mathbb{Z}[\sqrt{k}])$ such that $UAV^A = T^A$ and $UBV^B = T^B$ are the lower triangular matrices with invariant factors on the main diagonals.

Mathematics subject classification: 15A21, 11R04.

Keywords and phrases: Quadratic ring, matrices over quadratic rings, equivalence of pairs of matrices.

1 Introduction

Many problems in the representation theory of finite-dimensional algebras, in matrix factorizations over polynomial and other rings, etc. require to study some types of equivalences of matrices and their finite collections over various domains and to construct their canonical forms with respect to these equivalences [1–7]. These equivalences of matrices are such that their appropriate transformation matrices belong to certain subgroups of the general linear group.

In the analytical number theory concerning the study of arithmetic functions, in particular, the Kloosterman sum and its generalizations in matrix rings [8, 9], in the group theory [10], in the graph theory [11–13], etc. in [14, 15] it is necessary to investigate the structure of matrices over quadratic rings, in particular, over the ring of Gaussian integers.

In this paper we investigate the equivalence of matrices and their pairs: $A \to UAV^A$, $(A, B) \to (UAV^A, UBV^B)$ over quadratic rings $\mathbb{Z}[\sqrt{k}]$, where $U \in GL(n, \mathbb{Z})$, $V^A, V^B \in GL(n, \mathbb{Z}[\sqrt{k}])$. It is established that a pair of matrices A, B with relatively prime determinants over the quadratic principal ideal ring can be reduced by means of such equivalent transformations to the pair T^A, T^B of triangular forms with invariant factors on the main diagonals. Note that in [16] such a form was established with respect to this equivalence for matrices over the Euclidean quadratic rings.

2 Preliminaries

Let $\mathbb{Z}$ be a ring of integers. Then $\mathbb{K} = \mathbb{Z}[\sqrt{k}]$ is a quadratic ring, where $k \neq 0, 1$ is a square-free element of $\mathbb{Z}$. Elements $a \in \mathbb{Z}[\sqrt{k}]$ and their algebraic norm $N(a) \in \mathbb{Z}$ are determined in the following way [17]:

– if $k \equiv 2, 3 \pmod 4$, then

$$\mathbb{Z}[\sqrt{k}] = \{x + y\sqrt{k} | \ \ x, y \in \mathbb{Z}\}, \quad N(x + y\sqrt{k}) = x^2 - ky^2;$$

– if $k \equiv 1 \pmod 4$, then

$$\mathbb{Z}[\sqrt{k}] = \left\{ \frac{x}{2} + \frac{y}{2}\sqrt{k} \ \middle| \ x, y \in \mathbb{Z}, x - y \text{ divided by } 2 \right\}, \ N\left(\frac{x}{2} + \frac{y}{2}\sqrt{k}\right) = \frac{1}{4}(x^2 - ky^2).$$

If $\mathbb{K}$ is a Euclidean quadratic ring, then the Euclidean norm $E(a) \in \mathbb{N}$ of an element $a \in \mathbb{K}$ can be expressed as:

$$E(a) = \begin{cases} N(a) \ \text{ if } \ \mathbb{K} \ \text{ is imaginary,} \\ \\ |N(a)| \ \text{ if } \ \mathbb{K} \ \text{ is a real Euclidean quadratic ring.} \end{cases} \tag{1}$$

The quadratic ring $\mathbb{K} = \mathbb{Z}[\sqrt{k}]$ is called real if $k > 0$. If $k < 0$, then it is called an imaginary quadratic ring. Note that the algebraic and Euclidean norms of elements of the quadratic ring are completely multiplicative, i. e. $N(ab) = N(a)N(b)$, $E(ab) = E(a)E(b)$ for any $a, b \in \mathbb{K}$.

It is known that among quadratic rings there is a finite number of Euclidean quadratic rings [18, 19], among them there are quadratic principal ideal rings which are non-Euclidean, for example, the rings $\mathbb{Z}[\sqrt{k}]$, for $k = -19, -43, -67, -163$. There are some quadratic rings that are not principal ideal rings, for example, the ring $\mathbb{Z}[\sqrt{-5}]$.

In what follows $\mathbb{K}$ will denote a quadratic principal ideal ring, $U(\mathbb{K})$ a group of units of $\mathbb{K}$ and $\mathbb{K}_a$ will denote a complete set of residues modulo $a \in \mathbb{K}$.

Lemma 1. *Let $a_1, a_2, a_3 \in \mathbb{K}$ and let $d = (a_1, a_2, a_3)$ be their greatest common divisor. Then there exist elements $x_1, x_2 \in \mathbb{Z}$, $(x_1, x_2) = 1$, such that*

$$(x_1 a_1 + x_2 a_2, \, a_3) = d. \tag{2}$$

Proof. Obviously, it is sufficient to prove the lemma for the case where d equals 1. Write a_3 as a product of primes of $\mathbb{K}$, namely, $a_3 = ubc$, where $u \in U(\mathbb{K})$, $b = \prod\limits_{i=1}^{l} p_i^{r_i}$, $p_i \neq \bar{p}_j$, $i \neq j$, $i, j = 1, \ldots, l$, i.e. among p_i there are no pairwise conjugate elements, $c = \prod\limits_{i=1}^{f} q_i^{s_i} \bar{q}_i^{t_i}$, i.e. all the divisors of c are pairwise conjugate elements.

Putting $d = 1$ in (2) yields

$$(x_1 a_1 + x_2 a_2, \, b) = 1 \ \text{ and } \ (x_1 a_1 + x_2 a_2, \, c) = 1.$$

Since $(a_1, a_2, b) = 1$, then both a_1 and a_2 are not divisible by p_i, $i = 1, \dots, l$. Let

$$\mathrm{P}_1 = \prod_{i=1}^{l_1} p_i, \quad \mathrm{P}_2 = \prod_{i=l_1+1}^{l_2} p_i, \quad \mathrm{P}_3 = \prod_{i=l_2+1}^{l} p_i,$$

where $p_i \mid a_1$, (p_i divides a_1), $i = 1, \dots, l_1$, $p_i \mid a_2$, $i = l_1 + 1, \dots, l_2$, $p_i \nmid a_1 a_2$, (p_i does not divide $a_1 a_2$), $i = l_2 + 1, \dots, l$.

If $(x_1, x_2) = 1$ and

$$x_2 \not\equiv 0 \pmod{N(p_i)}, \quad i = 1, \dots, l_1, \tag{3}$$

the equality $(x_1 a_1 + x_2 a_2, \mathrm{P}_1) = 1$ holds.

Let us assume that some elements $\bar{p}_{l_1+1}, \dots, \bar{p}_{l_{21}}$, $l_{21} \le l_2$ divide a_1 and $\bar{p}_{l_{21}+1}, \dots, \bar{p}_{l_2}$ do not divide a_1, where $\bar{p}_i$, $i = l_1 + 1, \dots, l_2$, are conjugate elements to the corresponding primes p_i of the product P_2.

If

$$x_1 \not\equiv 0 \pmod{N(p_i)}, \ i = l_1 + 1, \dots, l_2, \tag{4}$$

$$\begin{cases} x_2 \not\equiv 0 \pmod{N(p_i)} \ \text{ if } \ i = l_1 + 1, \dots, l_{21}, \\ \\ x_2 \equiv 0 \pmod{N(p_i)} \ \text{ if } \ i = l_{21} + 1, \dots, l_2, \end{cases} \tag{5}$$

then $(x_1 a_1 + x_2 a_2, \mathrm{P}_2) = 1$.

Suppose that some prime elements $\bar{p}_{l_2+1}, \dots, \bar{p}_{l_{31}}$, $l_{31} \le l$, divide a_1 and $\bar{p}_{l_{31}+1}, \dots, \bar{p}_l$ do not divide a_1, where $\bar{p}_i$, $i = l_2 + 1, \dots, l$, are conjugate elements to the corresponding prime divisors p_i of the product P_3.

If

$$\begin{cases} x_2 \not\equiv 0 \pmod{N(p_i)}, \quad x_1 \equiv 0 \pmod{N(p_i)} \ \text{ if } \ i = l_2 + 1, \dots, l_{31}, \\ \\ x_2 \equiv 0 \pmod{N(p_i)} \ \text{ if } \ i = l_{31} + 1, \dots, l, \end{cases} \tag{6}$$

then $(x_1 a_1 + x_2 a_2, \mathrm{P}_3) = 1$.

Note that in the conditions (3)–(5) we considered that all prime divisors p_i, $i = 1, \dots, l_2$, of the products $\mathrm{P}_1, \mathrm{P}_2$ are not integers, i.e. $p_i \in \mathbb{K}$, but $p_i \notin \mathbb{Z}$. If some prime divisors p_i, $1 \le i \le l_2$, of the products $\mathrm{P}_1, \mathrm{P}_2$ are integers, i.e. $p_i \in \mathbb{Z}$, then in these conditions we consider the congruence (or incongruence) modulo p_i of these prime integer divisors.

Consequently, for the indicated $x_1, x_2 \in \mathbb{Z}$, we have $(x_1 a_1 + x_2 a_2, b) = 1$.

From $(a_1, a_2, c) = 1$ it follows that both a_1 and a_2 are not divisible by q_i and $\bar{q}_i$, $i = 1, \dots, f$. Write c as a product of primes of $\mathbb{K}$, i.e.

$$\mathrm{Q}_i = \prod_{j=f_{i-1}+1}^{f_i} q_j \ \text{ and } \ \bar{\mathrm{Q}}_i = \prod_{j=f_{i-1}+1}^{f_i} \bar{q}_j, \quad i = 1, \dots, 6, \quad f_6 = f,$$

where we set $f_0 = 0$ and $(\mathrm{Q}_1\bar{\mathrm{Q}}_1\mathrm{Q}_2\bar{\mathrm{Q}}_3, a_1) = \mathrm{Q}_1\bar{\mathrm{Q}}_1\mathrm{Q}_2\bar{\mathrm{Q}}_3$, $(\bar{\mathrm{Q}}_2\bar{\mathrm{Q}}_4\mathrm{Q}_5\bar{\mathrm{Q}}_5, a_2) = \bar{\mathrm{Q}}_2\bar{\mathrm{Q}}_4\mathrm{Q}_5\bar{\mathrm{Q}}_5$, $(\mathrm{Q}_6\bar{\mathrm{Q}}_6, a_1a_2) = 1$.

Then

i) $(x_1a_1 + x_2a_2,\ \mathrm{Q}_1\bar{\mathrm{Q}}_1\mathrm{Q}_2\bar{\mathrm{Q}}_2\mathrm{Q}_3\bar{\mathrm{Q}}_3) = 1$ if

$$x_2 \not\equiv 0 \pmod{N(\mathrm{Q}_1\mathrm{Q}_2\mathrm{Q}_3)}, \tag{7}$$

$$\begin{cases} x_1 \not\equiv 0 \pmod{N(\mathrm{Q}_2)}, \\ x_1 \equiv 0 \pmod{N(\mathrm{Q}_3)}; \end{cases} \tag{8}$$

ii) $(x_1a_1 + x_2a_2,\ \mathrm{Q}_4\bar{\mathrm{Q}}_4\mathrm{Q}_5\bar{\mathrm{Q}}_5\mathrm{Q}_6\bar{\mathrm{Q}}_6) = 1$ if

$$x_2 \equiv 0 \pmod{N(\mathrm{Q}_4\mathrm{Q}_5\mathrm{Q}_6)}. \tag{9}$$

Consequently, under the imposed conditions, $(x_1a_1+x_2a_2,\ c) = 1$ holds and completes the proof. □

3 Equivalence of matrices

Let $M(m, n, \mathbb{K})$ and $M(n, \mathbb{K})$ be the sets of $m \times n$ and $n \times n$ matrices over the quadratic principal ideal ring $\mathbb{K}$, respectively; d_k^A be the greatest common divisor of minors of order k of the matrix A and $A^{(m,n)}$ be an $m \times n$ matrix.

It is known that an $n \times n$ matrix A over the commutative principal ideal domain R is equivalent to the canonical diagonal form (the Smith normal form) [20], i. e. there exist invertible matrices $U, V \in GL(n, R)$ such that

$$D^A = UAV = diag(\mu_1^A, \dots, \mu_r^A, 0, \dots, 0),$$

$\mu_i^A | \mu_{i+1}^A$, $i = 1, \dots, r-1$, μ_i^A are called invariant factors of matrix A.

Lemma 2. *Let $A \in M(m, n, \mathbb{K})$, $m \le n$, $rang A = m$. Then there exists a row $\mathbf{x} = \|x_1 \quad \dots \quad x_m\|$, $x_1, \dots, x_m \in \mathbb{Z}$, such that*

$$\mathbf{x}A = \|a'_{11} \quad \dots \quad a'_{1n}\|,$$

where $(a'_{11}, \dots, a'_{1n}) = d_1^A$.

Proof. We proceed by induction on m. Without loss of generality, we may assume that $d_1^A = 1$.

Let $m = 2$, i. e.

$$A^{(2,n)} = \begin{Vmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{Vmatrix}.$$

It is known [20] that there exists a matrix $V \in GL(n, \mathbb{K})$ such that

$$A^{(2,n)}V = \begin{Vmatrix} a_1 & 0 & 0 & \dots & 0 \\ a_2 & a_3 & 0 & \dots & 0 \end{Vmatrix}.$$

Since $\left\| \begin{array}{cc} x_1 & x_2 \end{array} \right\| A^{(2,n)}V = \left\| \begin{array}{ccccc} x_1a_1 + x_2a_2 & x_2a_3 & 0 & \dots & 0 \end{array} \right\|$, then we prove that there exist $x_1, x_2 \in \mathbb{Z}$ such that $(x_1a_1 + x_2a_2,\, x_2a_3) = 1$.

By Lemma 1 there exist $x_1, x_2 \in \mathbb{Z}$, $(x_1, x_2) = 1$, such that $(x_1a_1 + x_2a_2,\, a_3) = 1$. If $(x_2, a_1) = 1$ and x_1, x_2 satisfy the conditions (3)–(9), then $(x_1a_1 + x_2a_2,\, x_2a_3) = 1$.

Note that if the only prime divisors of a_3 and their conjugates $p_i, \bar{p}_i,\ q_j, \bar{q}_j$, $i = 1, \dots, l$, $j = 1, \dots, f$, are the divisors of a_1 then, under the imposed conditions, the equality $(x_2, a_1) = 1$ holds.

Let us assume that $g_1, \dots, g_s$, among g_i, $i = 1, \dots, s$, there are non-conjugate elements and $h_1, \bar{h}_1, \dots, h_t, \bar{h}_t$ are the prime divisors of a_1, moreover $g_i, \bar{g}_i, h_j, \bar{h}_j$, $i = 1, \dots, s$, $j = 1, \dots, t$ do not divide a_3.

If

$$x_2 \not\equiv 0 \pmod{N(h_j)}, \quad j = 1, \dots, t, \tag{10}$$

$$x_2 \not\equiv 0 \pmod{N(g_i)} \text{ if } g_i \in \mathbb{K},\ g_i \notin \mathbb{Z}, \quad i = 1, \dots, s, \tag{11}$$

then $(x_2, a_1) = 1$.

If some primes $g_1, \dots, g_v \in \mathbb{Z}$, $v \le s$ and if

$$x_2 \not\equiv 0 \pmod{g_i}, \quad i = 1, \dots, v, \tag{12}$$

then the equality $(x_2, a_1) = 1$ holds. Consequently, under the imposed integers $x_1, x_2 \in \mathbb{Z}$ the equality $(x_1a_1 + x_2a_2,\, x_2a_3) = 1$ holds. It is obvious that $d_1^{A^{(2,n)}} = (a_1, a_2, a_3)$, and hence lemma is true for $m = 2$.

Let us assume that the lemma is true for $m - 1$, i.e. for the matrix

$$A^{(m-1,n)} = \left\| \begin{array}{ccc} a_{21} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{array} \right\|$$

there exists a row $\left\| \begin{array}{ccc} x_2' & \dots & x_m' \end{array} \right\|$, $x_i' \in \mathbb{Z}$, $i = 2, \dots, m$, such that

$$\left\| \begin{array}{ccc} x_2' & \dots & x_m' \end{array} \right\| A^{(m-1,n)} = \left\| \begin{array}{ccc} a_{21}' & \dots & a_{2n}' \end{array} \right\|,$$

where $(a_{21}', \dots, a_{2n}') = d_1^{A^{(m-1,n)}}$ and $a_{2j}' = \sum\limits_{i=2}^{m} x_i' a_{ij}$, $j = 1, \dots, n$.

Let us prove the lemma for any arbitrary m. Consider the matrix

$$A_1^{(2,n)} = \left\| \begin{array}{ccc} a_{11} & \dots & a_{1n} \\ a_{21}' & \dots & a_{2n}' \end{array} \right\|.$$

By the induction hypothesis the lemma is true for $m = 2$, i. e. there exists the row $\left\| \begin{array}{cc} x & y \end{array} \right\|$, $x, y \in \mathbb{Z}$, such that

$$\left\| \begin{array}{cc} x & y \end{array} \right\| A_1^{(2,n)} = \left\| \begin{array}{ccc} a_{11}' & \dots & a_{1n}' \end{array} \right\|,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^{A_1^{(2,n)}}$, $a'_{1j} = xa_{11} + y\sum\limits_{i=2}^{m} x'_i a_{ij}$, $j = 1,\dots,n$. Since $d_1^{A_1^{(2,n)}} = d_1^A$, then there exists the row $\mathbf{x} = \left\|x_1 \quad \dots \quad x_m\right\|$, where $x_1 = x$, $x_i = yx'_i$, $i = 2,\dots,m$, such that

$$\mathbf{x}A = \left\|a'_{11} \quad \dots \quad a'_{1n}\right\|$$

and $(a'_{11},\dots,a'_{1n}) = d_1^A$. Hence, the lemma is proved for any m, and the induction is completed. □

Theorem 1. *Let $A \in M(n,\mathbb{K})$, $detA \neq 0$. Then there exist invertible matrices $U \in GL(n,\mathbb{Z})$ and $V \in GL(n,\mathbb{K})$ such that*

$$UAV = \left\| \begin{matrix} \mu_1^A & 0 & \dots & 0 \\ t_{21}^A\mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^A\mu_1^A & t_{n2}^A\mu_2^A & \dots & \mu_n^A \end{matrix} \right\| = T^A, \tag{13}$$

where $t_{ij}^A \in \mathbb{K}_{\delta_{ij}^A}$, $\delta_{ij}^A = \frac{\mu_i^A}{\mu_j^A}$, $i,j = 1,\dots,n$, $i > j$.

Proof. Let $A = \left\|a_{ij}\right\|_1^n$, $a_{ij} \in \mathbb{K}$, $i,j = 1,\dots,n$. By Lemma 2 there exists a row $\mathbf{x} = \left\|x_1 \quad \dots \quad x_n\right\|$, $x_1,\dots,x_n \in \mathbb{Z}$, such that

$$\mathbf{x}A = \left\|a'_{11} \quad \dots \quad a'_{1n}\right\|,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^A$. There exists an invertible matrix $U = \left\| \begin{matrix} x_1 & \dots & x_n \\ & * & \end{matrix} \right\|$ such that

$$UA = \left\| \begin{matrix} a'_{11} & \dots & a'_{1n} \\ & * & \end{matrix} \right\| = A_1,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^A$ and $*$ are some elements. Then for some matrix $V_1 \in GL(n,\mathbb{K})$ we obtain:

$$A_1V_1 = UAV_1 = \left\| \begin{array}{c|c} \mu_1^A & \mathbf{0} \\ \hline \tilde{a}_{21}\mu_1^A & \\ \vdots & A^{(n-1,n-1)} \\ \tilde{a}_{n1}\mu_1^A & \end{array} \right\|,$$

where $\mu_1^A = d_1^{A_1} = d_1^A$ and μ_1^A divides all the elements of matrix $A^{(n-1,n-1)}$. Hence, μ_1^A is the first invariant factor of A.

Applying the similar reasoning to matrix $A^{(n-1,n-1)}$, after a finite number of steps we reduce matrix A by these transformations to the following triangular form with invariant factors on the main diagonal:

$$\tilde{A} = \left\| \begin{matrix} \mu_1^A & 0 & \dots & 0 \\ \tilde{a}_{21}\mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{a}_{n1}\mu_1^A & \tilde{a}_{n2}\mu_2^A & \dots & \mu_n^A \end{matrix} \right\|.$$

Let $\mathbb{K}_{\delta_{21}^A}$ be a prescribed complete set of residues modulo $\delta_{21}^A = \frac{\mu_2^A}{\mu_1^A}$. Since $\mu_2^A = \mu_1^A \delta_{21}^A$, then $\tilde{a}_{21} \equiv t_{21}^A \pmod{\delta_{21}^A}$, where $t_{21}^A \in \mathbb{K}_{\delta_{21}^A}$. Then $\tilde{a}_{21} = t_{21}^A + q\delta_{21}^A$, where $q \in \mathbb{K}$. Let us construct the invertible matrix $W_1 = \begin{Vmatrix} 1 & 0 \\ -q & 1 \end{Vmatrix} \oplus I^{(n-2)}$, where $I^{(n-2)}$ is an identity matrix of order $n-2$. Thus, we get matrix $\tilde{A}W_1$ whose $(2,1)$ element is equal to $t_{21}^A \mu_1^A$. Now we carry out a similar reasoning for non-diagonal elements of the third and the last rows of matrix $\tilde{A}$, and reduce this matrix to matrix T^A of the form (13). Therefore, the proof of the theorem is completed. □

4 Equivalence of pairs of matrices

Lemma 3. *Let $A, B \in M(m, n, \mathbb{K})$, $m \le n$ and $(d_m^A, d_m^B) = 1$. Then there exists a row $\mathbf{x} = \|x_1 \quad \dots \quad x_m\|$, $x_1, \dots, x_m \in \mathbb{Z}$, such that*

$$\mathbf{x}A = \|a'_{11} \quad \dots \quad a'_{1n}\|, \quad \mathbf{x}B = \|b'_{11} \quad \dots \quad b'_{1n}\|,$$

where $(a'_{11}, \dots, a'_{1n}) = d_1^A$, $(b'_{11}, \dots, b'_{1n}) = d_1^B$.

Proof. Let $A = \|a_{ij}\|_1^{m,n}$, $B = \|b_{ij}\|_1^{m,n}$, $a_{ij}, b_{ij} \in \mathbb{K}$, $i = 1, \dots, m$, $j = 1, \dots, n$. Without loss of generality, we may assume that $d_1^A = d_1^B = 1$. Let us prove the lemma for $m = 2$. Consider the matrices

$$A^{(2,n)} = \begin{Vmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{Vmatrix}, \quad B^{(2,n)} = \begin{Vmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \end{Vmatrix}.$$

By Theorem 1 for the matrix $B^{(2,n)}$ there exist matrices $U \in GL(2, \mathbb{Z})$ and $V_1 \in GL(n, \mathbb{K})$ such that

$$UB^{(2,n)}V_1 = \begin{Vmatrix} 1 & 0 & 0 & \dots & 0 \\ b_1 & b_2 & 0 & \dots & 0 \end{Vmatrix} = B_1.$$

Then for the matrix $UA^{(2,n)}$ there exists a matrix $V_2 \in GL(n, \mathbb{K})$ such that

$$UA^{(2,n)}V_2 = \begin{Vmatrix} a_1 & 0 & 0 & \dots & 0 \\ a_2 & a_3 & 0 & \dots & 0 \end{Vmatrix} = A_1.$$

We need to prove that for the pair of matrices A_1, B_1 there exists a row $\|x_1 \quad x_2\|$, $x_1, x_2 \in \mathbb{Z}$, such that

$$\| \; x_1 \quad x_2 \; \| A_1 = \| \; x_1 a_1 + x_2 a_2 \quad x_2 a_3 \quad 0 \quad \dots \quad 0 \; \|,$$

$$\| \; x_1 \quad x_2 \; \| B_1 = \| \; x_1 + x_2 b_1 \quad x_2 b_2 \quad 0 \quad \dots \quad 0 \; \|,$$

where

$$(x_1 a_1 + x_2 a_2, \, x_2 a_3) = 1, \tag{14}$$

$$(x_1 + x_2b_1,\, x_2b_2) = 1. \tag{15}$$

By Lemma 1 and by Lemma 2, the equality (14) holds if x_1, x_2 satisfy the conditions (3)–(12).

Now we choose such $x_1, x_2 \in \mathbb{Z}$, $(x_1, x_2) = 1$, that both (14) and (15) hold.

It is sufficient to prove (14), (15) for the case of $\bar{p}_1, \ldots, \bar{p}_{l_{11}}$, $1 \le l_{11} \le l_1$; $\bar{p}_{l_{21}+1}, \ldots, \bar{p}_{l_{22}}$, $l_{21}+1 \le l_{22} \le l_2$; $\bar{p}_{l_{31}+1}, \ldots, \bar{p}_{l_{32}}$, $l_{31}+1 \le l_{32} \le l$; $\bar{g}_1, \ldots, \bar{g}_{s_1}$, $1 \le s_1 \le s$, are prime divisors of b_2, where $\bar{p}_i$ and $\bar{g}_j$ are conjugate primes to the corresponding prime divisors p_i, g_j of the elements a_3 and a_1 of matrix A_1.

If

$$\begin{cases} x_1 \equiv 0 \pmod{N(p_i)} \text{ if } \bar{p}_i \nmid b_1, \\ \\ x_1 \not\equiv 0 \pmod{N(p_i)} \text{ if } \bar{p}_i \mid b_1,\ i = 1, \ldots, l_{11}, \end{cases}$$

then $(x_1 + x_2b_1, \bar{p}_1 \ldots \bar{p}_{l_{11}}) = 1$.

The equalities $(x_1 + x_2b_1, \bar{p}_{l_{21}+1} \ldots \bar{p}_{l_{22}}) = 1$ and $(x_1 + x_2b_1, \bar{p}_{l_{31}+1} \ldots \bar{p}_{l_{32}}) = 1$ hold, in case x_1, x_2 satisfy the conditions (4)–(6).

Now if

$$\begin{cases} x_1 \equiv 0 \pmod{N(g_i)} \text{ if } \bar{g}_i \nmid b_1, \\ \\ x_1 \not\equiv 0 \pmod{N(g_i)} \text{ if } \bar{g}_i \mid b_1,\ \ i = 1, \ldots, s_1, \end{cases}$$

then $(x_1 + x_2b_1, \bar{g}_1 \ldots \bar{g}_{s_1}) = 1$.

Hence, there exists a row $\mathbf{x} = \left\| x_1 \quad x_2 \right\|$, where $x_1, x_2 \in \mathbb{Z}$, such that for the rows $\mathbf{x}A_1$ and $\mathbf{x}B_1$ the equalities (14), (15) are true. Then in Lemma 3 the mentioned row for matrices $A^{(2,n)}, B^{(2,n)}$ is the row $\tilde{\mathbf{x}} = \left\| x_1 \quad x_2 \right\| U$. The lemma is true for $m = 2$. Furthermore, we prove the lemma by induction, similarly as in the proof of Lemma 2. This completes the proof. □

Theorem 2. *Let $A, B \in M(n, \mathbb{K})$ and $(detA, detB) = 1$. Then there exist invertible matrices $U \in GL(n, \mathbb{Z})$ and $V^A, V^B \in GL(n, \mathbb{K})$ such that*

$$UAV^A = \begin{Vmatrix} \mu_1^A & 0 & \ldots & 0 \\ t_{21}^A\mu_1^A & \mu_2^A & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^A\mu_1^A & t_{n2}^A\mu_2^A & \ldots & \mu_n^A \end{Vmatrix} = T^A, \tag{16}$$

$$UBV^B = \begin{Vmatrix} \mu_1^B & 0 & \ldots & 0 \\ t_{21}^B\mu_1^B & \mu_2^B & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^B\mu_1^B & t_{n2}^B\mu_2^B & \ldots & \mu_n^B \end{Vmatrix} = T^B, \tag{17}$$

where $t_{ij}^A \in \mathbb{K}_{\delta_{ij}^A}$, $\delta_{ij}^A = \frac{\mu_i^A}{\mu_j^A}$, $t_{ij}^B \in \mathbb{K}_{\delta_{ij}^B}$, $\delta_{ij}^B = \frac{\mu_i^B}{\mu_j^B}$; $i, j = 1, \ldots, n$, $i > j$.

Proof. Let $A = \left\|a_{ij}\right\|_1^n$, $B = \left\|b_{ij}\right\|_1^n$, $a_{ij},\ b_{ij} \in \mathbb{K},\ i,j = 1,\dots,n$. By Lemma 3 there exists a row $\mathbf{x} = \left\|x_1 \quad \dots \quad x_n\right\|$, $x_1,\dots,x_n \in \mathbb{Z}$, such that

$$\mathbf{x}A = \left\|a'_{11} \quad \dots \quad a'_{1n}\right\|, \qquad \mathbf{x}B = \left\|b'_{11} \quad \dots \quad b'_{1n}\right\|,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^A$ and $(b'_{11},\dots,b'_{1n}) = d_1^B$. There is an invertible matrix $U \in GL(n,\mathbb{Z})$ with the first row $\left\|x_1 \quad \dots \quad x_n\right\|$. Thus,

$$UA = \left\|\begin{matrix} a'_{11} & \cdots & a'_{1n} \\ & * & \end{matrix}\right\| = A_1 \qquad \text{and} \qquad UB = \left\|\begin{matrix} b'_{11} & \cdots & b'_{1n} \\ & * & \end{matrix}\right\| = B_1.$$

Then there exist matrices $V_1, V_2 \in GL(n,K)$ such that

$$A_1V_1 = \left\|\begin{array}{c|c} \mu_1^A & \mathbf{0} \\ \hline \tilde{a}_{21}\mu_1^A & \\ \vdots & A^{(n-1,n-1)} \\ \tilde{a}_{n1}\mu_1^A & \end{array}\right\|, \qquad B_1V_2 = \left\|\begin{array}{c|c} \mu_1^B & \mathbf{0} \\ \hline \tilde{b}_{21}\mu_1^B & \\ \vdots & B^{(n-1,n-1)} \\ \tilde{b}_{n1}\mu_1^B & \end{array}\right\|,$$

where $\mu_1^A = d_1^A,\ \mu_1^B = d_1^B$.

We carry out a similar reasoning for matrices $A^{(n-1,n-1)}$ and $B^{(n-1,n-1)}$, after a finite number of steps we reduce matrices A and B by the indicated transformations to the triangular forms

$$\tilde{A} = \left\|\begin{matrix} \mu_1^A & 0 & \dots & 0 \\ \tilde{a}_{21}\mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{a}_{n1}\mu_1^A & \tilde{a}_{n2}\mu_2^A & \dots & \mu_n^A \end{matrix}\right\|, \qquad \tilde{B} = \left\|\begin{matrix} \mu_1^B & 0 & \dots & 0 \\ \tilde{b}_{21}\mu_1^B & \mu_2^B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{b}_{n1}\mu_1^B & \tilde{b}_{n2}\mu_2^B & \dots & \mu_n^B \end{matrix}\right\|.$$

Thus, we will reduce the pair of matrices $\tilde{A}, \tilde{B}$ to the pair T^A, T^B of the form (16), (17) by means of the indicated transformations in the same way as we reduced matrix $\tilde{A}$ to matrix T^A at the end of Theorem 1. This completes the proof of the theorem. □

Remark. Note that the pair of matrices $A, B \in M(n,\mathbb{K})$ such that $(detA, detB) = d \neq 1$ cannot be reduced by means of the indicated transformations to the pair of matrices T^A, T^B of the form (16), (17).

Example. Let

$$A = \left\|\begin{matrix} 1+\sqrt{-2} & 0 \\ 0 & 1-\sqrt{-2} \end{matrix}\right\|, \qquad B = \left\|\begin{matrix} 1 & 0 \\ 3+\sqrt{-2} & (1+\sqrt{-2})(1-\sqrt{-2}) \end{matrix}\right\|$$

be 2×2 matrices over the Euclidean quadratic ring $\mathbb{Z}[\sqrt{-2}]$. It is easy to verify that the pair of matrices A, B, $(detA, detB) = 1$ cannot be reduced by these transformations to pairs T^A, T^B of the form (16), (17).

Corollary. *Let $\mathbb{K}$ be a Euclidean quadratic ring, $A, B \in M(n, \mathbb{K})$, $(detA, detB) = 1$, $E(a)$ be the Euclidean norm of element $a \in \mathbb{K}$, determined by (1). Then there exist invertible matrices $U \in GL(n, \mathbb{Z})$ and $V^A, V^B \in GL(n, \mathbb{K})$ such that*

$$UAV^A = \begin{Vmatrix} \mu_1^A & 0 & \dots & 0 \\ t_{21}^A \mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^A \mu_1^A & t_{n2}^A \mu_2^A & \dots & \mu_n^A \end{Vmatrix}, \qquad UBV^B = \begin{Vmatrix} \mu_1^B & 0 & \dots & 0 \\ t_{21}^B \mu_1^B & \mu_2^B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^B \mu_1^B & t_{n2}^B \mu_2^B & \dots & \mu_n^B \end{Vmatrix},$$

where

$$\begin{cases} t_{ij}^A = 0 \quad if \quad \mu_i^A = \mu_j^A, \\ \\ E(t_{ij}^A) < E\left(\frac{\mu_i^A}{\mu_j^A}\right) \quad if \quad \mu_i^A \neq \mu_j^A \ and \ \ t_{ij}^A \neq 0, \ i, j = 1, \dots, n, \ i > j; \end{cases}$$

$$\begin{cases} t_{ij}^B = 0 \quad if \quad \mu_i^B = \mu_j^B, \\ \\ E(t_{ij}^B) < E\left(\frac{\mu_i^B}{\mu_j^B}\right) \quad if \quad \mu_i^B \neq \mu_j^B \ and \ \ t_{ij}^B \neq 0, \ i, j = 1, \dots, n, \ i > j. \end{cases}$$

References

[1] Dlab V., Ringel C. M. *Canonical forms of pairs of complex matrices*. Linear Algebra Appl., 1991, **147**, 387–410.

[2] Gaiduk T. N., Sergeichuk V. V. *Generic canonical form of pairs of matrices with zeros*. Linear Algebra Appl., 2004, **380**, 241—251.

[3] Petrichkovich V. M. *Semiscalar equivalence and the Smith normal form of polynomial matrices*. J. Sov. Math., 1993, **66**, No. 1, 2030–2033.

[4] Dias da Silva J. A., Laffey T. J. *On simultaneous similarity of matrices and related questions*. Linear Algebra Appl., 1999, **291**, 167–184.

[5] Petrichkovich V. M. *Semiscalar equivalence and factorization of polynomial matrices*. Ukrainian Math. J., 1990, **42**, No. , 570–574.

[6] Kazimirs'kii P. S. *Decomposition of matrix polynomials into factors*. Naukova Dumka, Kiev, 1981 (in Ukrainian).

[7] Petrychkovych V. *Generalized equivalence of pairs of matrices*. Linear and Multilinear Algebra, 2000, **48**, No. 2, 179–188.

[8] Varbanets S. P. *General Kloosterman sums over ring of Gaussian integers*. Ukrainian Math. J., 2007, **59**, No. 9, 1313–1341.

[9] Velichko I. N. *Generalized Kloosterman sum over the matrix ring $M_n(\mathbb{Z}[i])$*. Visn. Odes. Nats. Univ., Ser. Mat. and Mekh., 2010, **15**, No. 19, 9–20 (in Russian).

[10] Nica B. *The unreasonable slightness of E_2 over imaginary quadratic rings*. Amer. Math. Monthly, 2011, **118**, No. 5, 455–462.

[11] Taylor G. *Cyclotomic matrices and graphs over the ring of integers of some imaginary quadratic fields*. J. Algebra, 2011, **331**, No. 1, 523–545.

[12] Taylor G. *Lehmer's conjecture for matrices over the ring of integers of some imaginary quadratic fields*. J. Number Theory, 2012, **132**, No. 4, 590–607.

[13] Greaves G. *Cyclotomic matrices over the Eisenstein and Gaussian integers*. J. Algebra, 2012, **372**, 560–583.

[14] Sidorov S. V. *On similarity of* 2×2 *matrices over the ring of Gaussian integers with reducible characteristic polynomial*. Vestn. Nizhni Novgorod Univ., 2008, **4**, 122–126 (in Russian).

[15] Rodosskii K. A. *The Euclidean algorithm*. Nauka, Moscow, 1988 (in Russian).

[16] Zelisko V. R., Ladzoryshyn N. B., Petrychkovych V. M. *On equivalence of matrices over quadratic Euclidean rings*. Appl. Problems of Mechanics and Math., 2006, **4**, 16–21 (in Ukrainian).

[17] Hasse H. *Number theory*. Classics in Mathematics, Springer-Verlag, New York-Berlin, 1980.

[18] Clark David A. *A quadratic field which is Euclidean but not norm-Euclidean*. Manuscripta Math., 1994, **83**, No. 3–4, 327–330.

[19] Harper Malcolm. $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*. Canad. J. Math., 2004, **56**, No. 1, 55–70.

[20] Newman Morris. *Integral matrices*. Pure and Applied Mathematics, vol. 45, Academic Press, New York, 1972.

Natalija Ladzoryshyn, Vasyl' Petrychkovych
Pidstryhach Institute for Applied Problems of Mechanics
and Mathematics of the NAS of Ukraine
3b Naukova Str., 79060, L'viv
Ukraine

E-mail: *natalja.ladzoryshyn@gmail.com;*
vas_petrych@yahoo.com

Received May 30, 2014

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 49–64
ISSN 1024–7696

Limits of solutions to the singularly perturbed abstract hyperbolic-parabolic system

Andrei Perjan, Galina Rusu*

Abstract. We study the behavior of solutions to the problem

$$\begin{cases} \varepsilon u_\varepsilon''(t) + u_\varepsilon'(t) + A(t)u_\varepsilon(t) = f_\varepsilon(t), \quad t \in (0,T), \\ u_\varepsilon(0) = u_{0\varepsilon}, \quad u_\varepsilon'(0) = u_{1\varepsilon}, \end{cases}$$

in the Hilbert space H as $\varepsilon \to 0$, where $A(t), t \in (0,\infty)$, is a family of linear self-adjoint operators.

Mathematics subject classification: 35B25, 35K15, 35L15, 34G10.
Keywords and phrases: Singular perturbation, abstract second order Cauchy problem, boundary layer function, a priori estimate.

1 Introduction

Let H be a real Hilbert space endowed with the scalar product $(\cdot,\cdot)$ and the norm $|\cdot|$, and V is also a real Hilbert space endowed with the norm $||\cdot||$. Let $A(t) : V \subset H \to H$, $t \in [0,\infty)$, be a family of linear self-adjoint operators. Consider the following Cauchy problem:

$$\begin{cases} \varepsilon u_\varepsilon''(t) + u_\varepsilon'(t) + A(t)u_\varepsilon(t) = f_\varepsilon(t), \quad t \in (0,T), \\ u_\varepsilon(0) = u_{0\varepsilon}, \quad u_\varepsilon'(0) = u_{1\varepsilon}, \end{cases} \tag{P_ε}$$

where $\varepsilon > 0$ is a small parameter ($\varepsilon \ll 1$), $u_\varepsilon, f_\varepsilon : [0,T) \to H$.

We investigate the behavior of solutions u_ε to the problems (P_ε) when $u_{0\varepsilon} \to u_0$, $f_\varepsilon \to f$ as $\varepsilon \to 0$. We establish a relationship between solutions to the problems (P_ε) and the corresponding solution to the following unperturbed problem:

$$\begin{cases} v'(t) + A(t)v(t) = f(t), \quad t \in (0,T), \\ v(0) = u_0. \end{cases} \tag{P_0}$$

If in some topology the solutions u_ε to the perturbed problems (P_ε) tend to the corresponding solution v to the unperturbed problem (P_0) as $\varepsilon \to 0$, then the problem (P_0) is called *regularly perturbed.* In the opposite case the problem (P_0) is called *singularly perturbed.* In the last case a subset of $[0,\infty)$ arises in which solutions u_ε have a singular behavior relative to ε. This subset is called *the boundary layer.* The function which defines the singular behavior of solution u_ε within the boundary layer is called *the boundary layer function.*

*Research is in part supported by the Project 11.817.08.41F

In Theorems 5.1 and 5.2 we prove that solutions u_ε to the perturbed problem (P_ε) tend to the solution v to the unperturbed problem P_0 in the norm of the space $C([0,T];H)$, as $\varepsilon \to 0$. At the same time in the space $C^1([0,T];H)$ the solution u_ε has a singular behavior relative to parameter ε in the neighbourhood of $t=0$.

The problem (P_ε) is an abstract model of singularly perturbed problems of hyperbolic-parabolic type. Such kind of problems arises in the mathematical modeling of elasto-plasticity phenomena.

A large class of works is dedicated to the study of singularly perturbed Cauchy problems for differential equations of second order. Without pretending to a complete analysis of these works, we will mention some of them, which contain a rich bibliography. In [9, 10, 17], some asymptotic expansions of the solutions to linear wave equations and their derivatives have been obtained. In [1, 2, 4, 8, 15, 16] nonlinear problems of hyperbolic-parabolic type have been studied. Nonlinear abstract problems of hyperbolic-parabolic type have been studied in [5–7, 12].

Unlike other methods, our approach is based on two key points. The first one is the relationship between solutions to the problems (P_ε) and (P_0) in the linear case. The second key point consists of *a priori* estimates of solutions to the unperturbed problem, which are uniform with respect to small parameter ε. Moreover, the problem (P_ε) is studied for a larger class of functions f_ε, i. e. $f_\varepsilon \in W^{1,p}(0,T;H)$. Also we obtain the convergence rate, as $\varepsilon \to 0$.

In what follows we will need some notations. Let $k \in N^*$, $1 \le p \le +\infty$, $(a,b) \subset (-\infty,+\infty)$ and X be a Banach space. By $W^{k,p}(a,b;X)$ denote the Banach space of vectorial distributions $u \in D'(a,b;X)$, $u^{(j)} \in L^p(a,b;X)$, $j=0,1,\dots,k$, endowed with the norm

$$\|u\|_{W^{k,p}(a,b;X)} = \left(\sum_{j=0}^{k} \|u^{(j)}\|^p_{L^p(a,b;X)}\right)^{\frac{1}{p}} \quad \text{for} \quad p \in [1,\infty),$$

$$\|u\|_{W^{k,\infty}(a,b;X)} = \max_{0\le j\le k} \|u^{(j)}\|_{L^\infty(a,b;X)} \quad \text{for} \quad p=\infty.$$

In the particular case $p=2$ we put $W^{k,2}(a,b;X) = H^k(a,b;X)$. If X is a Hilbert space, then $H^k(a,b;X)$ is also a Hilbert space with the scalar product

$$(u,v)_{H^k(a,b;X)} = \sum_{j=0}^{k} \int_a^b \left(u^{(j)}(t), v^{(j)}(t)\right)_X dt.$$

For $s \in \mathbb{R}$, $k \in \mathbb{N}$ and $p \in [1,\infty]$ define the Banach spaces

$$W^{k,p}_s(a,b;H) = \{f : (a,b) \to H; f^{(l)}(\cdot)e^{-st} \in L^p(a,b;X),\ l=0,\dots,k\},$$

with the norms

$$\|f\|_{W^{k,p}_s(a,b;X)} = ||fe^{-st}||_{W^{k,p}(a,b;X)}.$$

The framework of our paper will be determined by the following conditions:

(H1) *V is separable and $V \subset H$ densely and continuously,* i. e.

$$|u|^2 \leq \gamma ||u||^2, \quad \forall u \in V;$$

(H2) *For each $u, v \in V$ the function $t \mapsto (A(t)u, v)$ is continuously differentiable on $(0, \infty)$ and*

$$\big|(A'(t)u, v)\big| \leq a_0 |u||v|, \quad \forall u, v \in V, \quad \forall t \in [0, \infty);$$

(H3) *The operators $A(t) : V \subset H \to H, t \in [0, \infty)$ are linear, self-adjoint and positive definite, i.e. there exists $\omega > 0$ such that*

$$(A(t)u, u) \geq \omega \, ||u||^2, \quad \forall u \in V, \quad \forall t \in [0, \infty).$$

(H4) *For each $u, v \in V$ the function $t \mapsto (A(t)u, v)$ is twice continuously differentiable on $(0, \infty)$ and*

$$\big|(A''(t)u, v)\big| \leq a_1 |u||v|, \quad \forall u, v \in V, \quad \forall t \in [0, \infty).$$

2 Existence of solutions to problems (P_ε) and (P_0)

In [11] the following results concerning the solvability of problems (P_ε) and (P_0) are proved.

Theorem 2.1. *Let $T > 0$. Let us assume that the conditions* **(H1)**, **(H2)** *and* **(H3)** *are fulfilled. If $u_{0\varepsilon} \in V$, $u_{1\varepsilon} \in H$ and $f_\varepsilon \in L^2(0, T; H)$, then there exists the unique function $u_\varepsilon \in W^{2,2}(0, T; H) \bigcap L^2(0, T; V)$, $A(\cdot)u_\varepsilon \in L^2(0, T; H)$ (strong solution) which satisfies the equation a.e. on $(0, T)$ and the initial conditions from (P_ε).*

If, in addition, $u_{1\varepsilon} \in V$, $f_\varepsilon(0) - A(0)u_{0\varepsilon} \in V$, $f_\varepsilon \in W^{2,1}(0, T; H)$, then $A(\cdot)u_\varepsilon \in W^{1,2}(0, T; H)$ and $u_\varepsilon \in W^{3,2}(0, T; H) \bigcap W^{1,2}(0, T; H)$.

Theorem 2.2. *Let $T > 0$. Let us assume that the conditions* **(H1)**, **(H2)** *and* **(H3)** *are fulfilled. If $u_{0\varepsilon} \in H$, and $f_\varepsilon \in L^2(0, T; H)$, then there exists the unique function $u_\varepsilon \in W^{2,2}(0, T; H) \bigcap L^2(0, T; V)$ which satisfies a. e. on $(0, T)$ the equation and the initial conditions from (P_0).*

3 A priori estimates for solutions to the problem (P_ε)

In what follows, we will give some *a priori* estimates of solutions to the problem (P_ε).

Lemma 3.1. *Let us assume that conditions* **(H1)**, **(H2)** *and* **(H3)** *are fulfilled. If $u_{0\varepsilon} \in V$, $u_{1\varepsilon} \in H$ and $f_\varepsilon \in L^2(0, \infty; H)$, then there exists a constant $C = C(\gamma, a_0, \omega) > 0$ such that for every solution u_ε to the problem (P_ε) the estimate*

$$||u_\varepsilon||_{C([0,t];H)} + ||A^{1/2}(\cdot)u_\varepsilon||_{L^2([0,t];H)} \leq C \; M_{0\varepsilon}, \quad \forall \varepsilon \in (0, \varepsilon_0), \quad \forall t \geq 0 \qquad (3.1)$$

is valid, where

$$M_{0\varepsilon} = |A^{1/2}(0)u_{0\varepsilon}| + \varepsilon|u_{1\varepsilon}| + ||f_\varepsilon||_{L^2(0,\infty;H)}, \quad \varepsilon_0 = \min\Big\{1, \frac{\omega}{2\gamma\, a_0}\Big\}.$$

If, in addition, $u_{1\varepsilon} \in V$ *and* $f_\varepsilon \in W^{1,2}(0,\infty;H)$ *then*

$$||u'_\varepsilon||_{C([0,t];H)} + ||A^{1/2}(\cdot)u'_\varepsilon||_{L^2([0,t];H)} \le C\ M_\varepsilon, \quad \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \ge 0, \tag{3.2}$$

$$M_\varepsilon = |A(0)u_{0\varepsilon}| + |A^{1/2}(0)u_{1\varepsilon}| + ||f_\varepsilon||_{W^{1,2}(0,\infty;H)}.$$

Proof. Proof of estimate (3.1). Denote by

$$E(u,t) = \varepsilon^2|u'(t)|^2 + \frac{1}{2}|u(t)|^2 + \varepsilon\Big(A(t)u(t), u(t)\Big) + \varepsilon\int_0^t |u'(\tau)|^2 d\tau$$

$$+\varepsilon\Big(u(t), u'(t)\Big) + \int_0^t \Big(A(\tau)u(\tau), u(\tau)\Big)d\tau. \tag{3.3}$$

For every strong solution u_ε to problem (P_ε) we have

$$\frac{d}{dt}E(u_\varepsilon,t) = 2\varepsilon^2\big(u''_\varepsilon(t), u'_\varepsilon(t)\big) + \big(u'_\varepsilon(t), u_\varepsilon(t)\big) + 2\varepsilon\big(A(t)u_\varepsilon(t), u'_\varepsilon(t)\big)$$

$$+\varepsilon\big(A'(t)u_\varepsilon(t), u_\varepsilon(t)\big) + \varepsilon|u_\varepsilon(t)|^2 + \varepsilon|u'_\varepsilon(t)|^2 + \varepsilon\big(u''_\varepsilon(t), u_\varepsilon(t)\big) + \big(A(t)u_\varepsilon(t), u_\varepsilon(t)\big)$$

$$= 2\varepsilon\big(u'_\varepsilon(t), f_\varepsilon(t) - u'_\varepsilon(t) - A(t)u_\varepsilon(t)\big) + \big(u'_\varepsilon(t), u_\varepsilon(t)\big)$$

$$+2\varepsilon\big(A(t)u_\varepsilon(t), u'_\varepsilon(t)\big) + \varepsilon\big(A'(t)u_\varepsilon(t), u_\varepsilon(t)\big) + 2\varepsilon|u'_\varepsilon(t)|^2 + \big(A(t)u_\varepsilon(t), u_\varepsilon(t)\big)$$

$$+\big(u_\varepsilon(t), f_\varepsilon(t) - u'_\varepsilon(t) - A(t)u_\varepsilon(t)\big)$$

$$= \big(f_\varepsilon(t), u_\varepsilon(t) + 2\varepsilon u'_\varepsilon(t)\big) + \varepsilon\big(A'(t)u_\varepsilon(t), u_\varepsilon(t)\big), \quad \forall t \ge 0.$$

Thus

$$\frac{d}{dt}E(u_\varepsilon,t) = \big(f_\varepsilon(t), u_\varepsilon(t) + 2\varepsilon u'_\varepsilon(t)\big) + \varepsilon\big(A'(t)u_\varepsilon(t), u_\varepsilon(t)\big), \quad \forall t \ge 0.$$

Integrating on $(0,t)$ we get

$$E(u_\varepsilon,t) = E(u_\varepsilon,0) + \int_0^t \big(f_\varepsilon(\tau), u_\varepsilon(\tau) + 2\varepsilon u'_\varepsilon(\tau)\big)\, d\tau$$

$$+\varepsilon\int_0^t \big(A'(\tau)u_\varepsilon(\tau), u_\varepsilon(\tau)\big)d\tau, \quad \forall t \ge 0.$$

Let us observe that

$$\int_0^t \big|f_\varepsilon(\tau)||u_\varepsilon(\tau)\big|\, d\tau \le \frac{1}{2}\int_0^t \big(A(\tau)u_\varepsilon(\tau), u_\varepsilon(\tau)\big)d\tau + \frac{\gamma}{2\omega}\int_0^t \big|f_\varepsilon(\tau)|^2 d\tau,$$

$$2\varepsilon \int_0^t \big|f_\varepsilon(\tau)||u'_\varepsilon(\tau)\big|\,d\tau \le \varepsilon^2 \int_0^t \big|u'_\varepsilon(\tau)\big|^2 d\tau + \int_0^t \big|f_\varepsilon(\tau)|^2 d\tau,$$

$$\varepsilon \int_0^t \Big|\big(A'(\tau)u_\varepsilon(\tau), u_\varepsilon(\tau)\big)\Big| d\tau \le \frac{a_0\gamma}{\omega}\,\varepsilon \int_0^t \big(A(\tau)u_\varepsilon(\tau), u_\varepsilon(\tau)\big) d\tau, \quad \forall t \ge 0.$$

Thus

$$E(u_\varepsilon, t) \le C(\gamma, a_0, \omega)\Big[E(u_\varepsilon, 0) + ||f_\varepsilon||^2_{L^2(0,t;H)}\Big],\ \forall t \ge 0,\ \forall 0 < \varepsilon < \varepsilon_0 = \min\Big\{1, \frac{\omega}{2\gamma\, a_0}\Big\}.$$

Using the Brézis' Lemma (see, e. g., [13]), the estimate (3.1) is a simple consequence of the last inequality.

The *proof of estimate* (3.2) is similar to the proof of (3.1) if we denote by $y_\varepsilon = u'_\varepsilon$, which is the solution to the problem

$$\begin{cases} \varepsilon y''_\varepsilon(t) + y'_\varepsilon(t) + A(t)y_\varepsilon(t) = f'_\varepsilon(t) - A'(t)u_\varepsilon(t), \quad t \in (0,\infty), \\ y_\varepsilon(0) = u_{1\varepsilon}, \quad y'_\varepsilon(0) = \dfrac{1}{\varepsilon}\Big(f_\varepsilon(0) - u_{1\varepsilon} - A(0)u_{0\varepsilon}\Big). \end{cases}$$

□

Let u_ε be the strong solution to the problem (P_ε) and let us denote by

$$z_\varepsilon(t) = u'_\varepsilon(t) + h_\varepsilon e^{-t/\varepsilon}, \quad h_\varepsilon = f_\varepsilon(0) - u_{1\varepsilon} - A(0)u_{0\varepsilon}. \tag{3.4}$$

Similarly to Lemma 3.1, for the function z_ε we obtain the following result:

Lemma 3.2. *Let us assume that conditions* **(H1)**—**(H4)** *are fulfilled. If* $f_\varepsilon(0) - A(0)u_{0\varepsilon}$, $u_{1\varepsilon} \in V$ *and* $f_\varepsilon \in W^{1,2}(0,\infty;H)$, *then there exist constants* $C = C(\gamma, \omega, a_0, a_1) > 0$ *and* $\varepsilon_0 = \varepsilon_0(\gamma, \omega, a_0, a_1) \in (0;1)$ *such that for* z_ε, *defined by* (3.4), *the estimate*

$$\big|\big|A^{1/2}(\cdot)z_\varepsilon\big|\big|_{C(0,\,t;\,H)} + \big|\big|z'_\varepsilon\big|\big|_{L^2(0,\,t;\,H)} \le C\, M_{1\varepsilon}, \quad \forall \varepsilon \in (0, \varepsilon_0), \quad \forall t \ge 0, \tag{3.5}$$

is valid, where

$$M_{1\varepsilon} = |A^{1/2}(0)\big(f_\varepsilon(0) - A(0)u_{0\varepsilon}\big)| + |A^{1/2}(0)u_{1\varepsilon}| + ||A(t)h_\varepsilon||_{L^2(0,\infty;H)} + ||f_\varepsilon||_{W^{2,2}(0,\infty;H)}.$$

4 The relationship between the solutions to the problems (P_ε) and (P_0) in the linear case

Now we are going to present the relationship between solutions to the problem (P_ε) and the corresponding solutions to the problem (P_0). This relationship was established in the work [14]. To this end we define the kernel of the transformation which realizes this relationship.

For $\varepsilon > 0$ denote

$$K(t, \tau, \varepsilon) = \frac{1}{2\sqrt{\pi}\varepsilon}\Big(K_1(t, \tau, \varepsilon) + 3K_2(t, \tau, \varepsilon) - 2K_3(t, \tau, \varepsilon)\Big),$$

where

$$K_1(t,\tau,\varepsilon)=\exp\Big\{\frac{3t-2\tau}{4\varepsilon}\Big\}\lambda\Big(\frac{2t-\tau}{2\sqrt{\varepsilon t}}\Big),$$

$$K_2(t,\tau,\varepsilon)=\exp\Big\{\frac{3t+6\tau}{4\varepsilon}\Big\}\lambda\Big(\frac{2t+\tau}{2\sqrt{\varepsilon t}}\Big),$$

$$K_3(t,\tau,\varepsilon)=\exp\Big\{\frac{\tau}{\varepsilon}\Big\}\lambda\Big(\frac{t+\tau}{2\sqrt{\varepsilon t}}\Big),\quad \lambda(s)=\int_s^\infty e^{-\eta^2}d\eta.$$

The properties of kernel $K(t,\tau,\varepsilon)$ are collected in the following lemma.

Lemma 4.1. *The function $K(t,\tau,\varepsilon)$ possesses the following properties:*

(i) $K\in C([0,\infty)\times[0,\infty))\cap C^2((0,\infty)\times(0,\infty))$*;*

(ii) $K_t(t,\tau,\varepsilon)=\varepsilon K_{\tau\tau}(t,\tau,\varepsilon)-K_\tau(t,\tau,\varepsilon),\quad \forall t>0,\quad \forall\tau>0;$

(iii) $\varepsilon K_\tau(t,0,\varepsilon)-K(t,0,\varepsilon)=0,\quad \forall t\ge 0$*;*

(iv) $K(0,\tau,\varepsilon)=\dfrac{1}{2\varepsilon}\exp\Big\{-\dfrac{\tau}{2\varepsilon}\Big\},\quad \forall\tau\ge 0$*;*

(v) *For every $t>0$ fixed and every $q,s\in\mathbb{N}$ there exist constants $C_1(q,s,t,\varepsilon)>0$ and $C_2(q,s,t)>0$ such that*

$$\big|\partial_t^s\partial_\tau^q K(t,\tau,\varepsilon)\big|\le C_1(q,s,t,\varepsilon)\exp\{-C_2(q,s,t)\tau/\varepsilon\},\quad \forall\tau>0;$$

Moreover, for $\gamma\in\mathbb{R}$ there exist C_1,C_2 and ε_0, all of them positive and depending on γ, such that the following estimates are fulfilled:

$$\int_0^\infty e^{\gamma\,\tau}\big|K_t(t,\tau,\varepsilon)\big|\,d\tau\le C_1\,\varepsilon^{-1}\,e^{C_2 t},\quad \forall\varepsilon\in(0,\varepsilon_0],\quad \forall t\ge 0,$$

$$\int_0^\infty e^{\gamma\,\tau}\big|K_\tau(t,\tau,\varepsilon)\big|\,d\tau\le C_1\,\varepsilon^{-1}\,e^{C_2 t},\quad \forall\varepsilon\in(0,\varepsilon_0],\quad \forall t\ge 0,$$

$$\int_0^\infty e^{\gamma\,\tau}\big|K_{\tau\,\tau}(t,\tau,\varepsilon)\big|\,d\tau\le C_1\,\varepsilon^{-2}\,e^{C_2 t},\quad \forall\varepsilon\in(0,\varepsilon_0],\quad \forall t\ge 0;$$

(vi) $K(t,\tau,\varepsilon)>0,\quad \forall t\ge 0,\quad \forall\tau\ge 0$*;*

(vii) *For every continuous function $\varphi:[0,\infty)\to H$ with $|\varphi(t)|\le M\exp\{\gamma\,t\}$ the following equality is true:*

$$\lim_{t\to 0}\Big|\int_0^\infty K(t,\tau,\varepsilon)\varphi(\tau)d\tau-\int_0^\infty e^{-\tau}\varphi(2\varepsilon\tau)d\tau\Big|=0,\ \textit{for every}\ \varepsilon\in\big(0,(2\,\gamma)^{-1}\big);$$

(viii)

$$\int_0^\infty K(t,\tau,\varepsilon)d\tau=1,\quad \forall t\ge 0,$$

(ix) *Let $\gamma > 0$ and $q \in [0,1]$. There exist C_1, C_2 and ε_0 all of them positive and depending on γ and q, such that the following estimates are fulfilled:*

$$\int_0^\infty K(t,\tau,\varepsilon)\, e^{\gamma\tau} |t-\tau|^q \, d\tau \le C_1\, e^{C_2 t}\, \varepsilon^{q/2}, \quad \forall \varepsilon \in (0,\varepsilon_0], \quad \forall t > 0.$$

If $\gamma \le 0$ and $q \in [0,1]$, then

$$\int_0^\infty K(t,\tau,\varepsilon)\, e^{\gamma\tau}\, |t-\tau|^q \, d\tau \le C\, \varepsilon^{q/2} \left(1+\sqrt{t}\right)^q, \quad \forall \varepsilon \in (0,1], \quad \forall t \ge 0;$$

(x) *Let $p \in (1,\infty]$ and $f : [0,\infty) \to H$, $f(t) \in W^{1,p}_\gamma(0,\infty;H)$. If $\gamma > 0$, then there exist C_1, C_2 and ε_0 all of them positive and depending on γ and p, such that*

$$\left| f(t) - \int_0^\infty K(t,\tau,\varepsilon) f(\tau) d\tau \right|$$
$$\le C_1\, e^{C_2 t}\, ||f'||_{L^p_\gamma(0,\infty;H)}\, \varepsilon^{(p-1)/2p}, \quad \forall \varepsilon \in (0,\varepsilon_0], \quad \forall t \ge 0.$$

If $\gamma \le 0$, then

$$\left| f(t) - \int_0^\infty K(t,\tau,\varepsilon) f(\tau) d\tau \right|$$
$$\le C(\gamma,p)\, \|f'\|_{L^p_\gamma(0,\infty;H)} \left(1+\sqrt{t}\right)^{\frac{p-1}{p}}\, \varepsilon^{(p-1)/2p}, \quad \forall \varepsilon \in (0,1], \quad \forall t \ge 0.$$

(xi) *For every $q > 0$ and $\alpha \ge 0$ there exists a constant $C(q,\alpha) > 0$ such that*

$$\int_0^t \int_0^\infty K(\tau,\theta,\varepsilon)\, e^{-q\,\theta/\varepsilon}\, |\tau-\theta|^\alpha \, d\theta\, d\tau \le C(q,\alpha)\, \varepsilon^{1+\alpha}, \ \forall \varepsilon > 0, \ \forall t \ge 0;$$

(xii) *Let $f \in W^{1,\infty}_\gamma(0,\infty;H)$ with $\gamma \ge 0$. There exist positive constants C_1, C_2 and ε_0, depending on γ, such that*

$$\Big| \int_0^\infty K_t(t,\tau,\varepsilon) f(\tau) d\tau \Big| \le C_1\, e^{C_2 t} \|f'\|_{L^\infty_\gamma(0,\infty;H)}, \quad \forall \varepsilon \in (0,\varepsilon_0], \quad \forall t \ge 0.$$

Theorem 4.1. *Let us assume that operators $A(t), t \in [0,\infty)$, verify conditions* **(H1)**–**(H3)** *and $f_\varepsilon \in L^\infty_\gamma(0,\infty;H)$ for some $\gamma \ge 0$. If u_ε is the strong solution to the problem (P_ε), with $u_\varepsilon \in W^{2,\infty}_\gamma(0,\infty;H) \cap L^\infty_\gamma(0,\infty;H)$, $Au_\varepsilon \in L^\infty_\gamma(0,\infty;H)$, then for every $0 < \varepsilon < (4\gamma)^{-1}$ the function w_ε, defined by*

$$w_\varepsilon(t) = \int_0^\infty K(t,\tau,\varepsilon)\, u_\varepsilon(\tau)\, d\tau,$$

is the strong solution in H to the problem

$$\begin{cases} w'_\varepsilon(t) + A(t) w_\varepsilon(t) = F_0(t,\varepsilon) + \displaystyle\int_0^\infty K(t,\tau,\varepsilon) \big[A(t) - A(\tau)\big] u_\varepsilon(\tau)\, d\tau, \text{ a. e. } t > 0, \\ w_\varepsilon(0) = \varphi_\varepsilon, \end{cases}$$

where

$$F_0(t,\varepsilon)=\frac{1}{\sqrt{\pi}}\Big[2\exp\Big\{\frac{3t}{4\varepsilon}\Big\}\lambda\Big(\sqrt{\frac{t}{\varepsilon}}\Big)-\lambda\Big(\frac{1}{2}\sqrt{\frac{t}{\varepsilon}}\Big)\Big]u_1+\int_0^\infty K(t,\tau,\varepsilon)\,f_\varepsilon(\tau)\,d\tau,$$

$$\varphi_\varepsilon=\int_0^\infty e^{-\tau}\,u_\varepsilon(2\varepsilon\tau)\,d\tau.$$

5 Limits of solutions to the problem (P_ε) as $\varepsilon \to 0$

In this section we will prove the convergence estimates for the difference of solutions to the problems (P_ε) and (P_0). These estimates will be uniform relative to small values of the parameter ε.

Theorem 5.1. *Let $T>0$. Let us assume that operators $A(t)$, $t\in[0,\infty)$, satisfy conditions* **(H1)**–**(H3)**. *If u_0, $u_{0\varepsilon}$, $u_{1\varepsilon}\in V$ and f, $f_\varepsilon\in W^{1,2}(0,T;H)$, then there exist constants $C=C(T,\gamma,a_0,\omega)>0$, $\varepsilon_0=\varepsilon_0(\gamma,a_0,\omega)$, $\varepsilon_0\in(0,1)$, such that*

$$||u_\varepsilon-v||_{C([0,T];H)}$$

$$\le C\Big(M(T,u_{0\varepsilon},u_{1\varepsilon},f_\varepsilon)\,\varepsilon^{1/4}+|u_{0\varepsilon}-u_0|+||f_\varepsilon-f||_{L^2(0,T;H)}\Big),\forall\varepsilon\in(0,\varepsilon_0),\quad(5.1)$$

where u_ε and v are strong solutions to problems (P_ε) and (P_0) respectively,

$$M(T,u_{0\varepsilon},u_{1\varepsilon},f_\varepsilon)=|A(0)u_{0\varepsilon}|+|A^{1/2}(0)u_{1\varepsilon}|+||f_\varepsilon||_{W^{1,2}(0,T;H)}.$$

Proof. During the proof we will agree to denote constants $C=C(T,\gamma,a_0,\omega)$, $M(T,u_{0\varepsilon},u_{1\varepsilon},f_\varepsilon)$ and $\varepsilon_0=\varepsilon_0(\gamma,a_0,\omega)$ by C, M and ε_0, respectively.

If f, $f_\varepsilon\in W^{k,p}(0,T;H)$ with $k\in\mathbb{N}$ and $p\in(1,\infty]$, then f, $f_\varepsilon\in C([0,T];H)$ (see, for example, [3]). Moreover, there exist extensions $\tilde f$, $\tilde f_\varepsilon\in W^{k,p}(0,\infty;H)$ such that

$$\begin{cases}||\tilde f||_{C([0,\infty);H)}+||\tilde f||_{W^{k,p}(0,\infty;H)}\le C(T,p)\,||f||_{W^{k,p}(0,T;H)},\\ ||\tilde f_\varepsilon||_{C([0,\infty);H)}+||\tilde f_\varepsilon||_{W^{k,p}(0,\infty;H)}\le C(T,p)\,||f_\varepsilon||_{W^{k,p}(0,T;H)}.\end{cases}\quad(5.2)$$

Let us denote by $\tilde u_\varepsilon$ the unique strong solution to the problem (P_ε), defined on $(0,\infty)$ instead of $(0,T)$ and $\tilde f_\varepsilon$ instead of f_ε.

From Lemma 3.1 it follows that $\tilde u_\varepsilon\in W^{2,\infty}(0,\infty;H)\cap L^\infty(0,\infty;H)$, $A(\cdot)\tilde u_\varepsilon\in L^\infty(0,\infty;H)$. Moreover, due to this lemma and inequalities (5.2), the following estimates hold

$$||u_\varepsilon||_{C([0,t];H)}+||A^{1/2}(\cdot)u_\varepsilon||_{L^2([0,t];H)}\le C\ M,\quad\forall\varepsilon\in(0,\varepsilon_0],\quad\forall t\ge0,\qquad(5.3)$$

$$||u'_\varepsilon||_{C([0,t];H)}+||A^{1/2}(\cdot)u'_\varepsilon||_{L^2([0,t];H)}\le C\ M,\quad\forall\varepsilon\in(0,\varepsilon_0],\quad\forall t\ge0.\qquad(5.4)$$

By Theorem 4.1, the function w_ε defined by

$$w_\varepsilon(t)=\int_0^\infty K(t,\tau,\varepsilon)\,\tilde u_\varepsilon(\tau)\,d\tau,$$

is the strong solution in H to the problem

$$\begin{cases} w_\varepsilon'(t) + A(t)w_\varepsilon(t) = F(t,\varepsilon), \quad \text{a. e.} \qquad t > 0, \\ w_\varepsilon(0) = w_0, \end{cases} \tag{5.5}$$

for every $\varepsilon \in (0, \varepsilon_0)$, where

$$F(t,\varepsilon) = f_0(t,\varepsilon)u_{1\varepsilon} + \int_0^\infty K(t,\tau,\varepsilon)\,\tilde{f}_\varepsilon(\tau)\,d\tau + \int_0^\infty K(t,\tau,\varepsilon)\,\big[A(t) - A(\tau)\big]u_\varepsilon(\tau)\,d\tau,$$

$$f_0(t,\varepsilon) = \frac{1}{\sqrt{\pi}}\Big[2\exp\Big\{\frac{3t}{4\varepsilon}\Big\}\lambda\Big(\sqrt{\frac{t}{\varepsilon}}\Big) - \lambda\Big(\frac{1}{2}\sqrt{\frac{t}{\varepsilon}}\Big)\Big],$$

$$w_0 = \int_0^\infty e^{-\tau}\,u_\varepsilon(2\varepsilon\tau)\,d\tau.$$

Using properties (**vi**), (**viii**), (**x**) from Lemma 4.1, and the estimate (5.4), we obtain that

$$||\tilde{u}_\varepsilon - w_\varepsilon||_{C([0,t];H)} \le C\,M\,\varepsilon^{1/4}, \quad \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \ge 0. \tag{5.6}$$

Denote by $R(t,\varepsilon) = \tilde{v}(t) - w_\varepsilon(t)$, where $\tilde{v}$ is the strong solution to the problem (P_0) with $\tilde{f}$ instead of f, $T = \infty$ and w_ε is the solution of (5.5). Then

$$\begin{cases} R'(t,\varepsilon) + A(t)R(t,\varepsilon) = \mathcal{F}(t,\varepsilon) + \displaystyle\int_0^\infty K(t,\tau,\varepsilon)\,\big[A(t) - A(\tau)\big]u_\varepsilon(\tau)\,d\tau, \text{ a.e. } t > 0, \\ R(0,\varepsilon) = R_0, \end{cases}$$

where $R_0 = u_0 - w_0$ and

$$\mathcal{F}(t,\varepsilon) = \tilde{f}(t) - \int_0^\infty K(t,\tau,\varepsilon)\tilde{f}_\varepsilon(\tau)\,d\tau - f_0(t,\varepsilon)\,u_{1\varepsilon}.$$

Taking the inner product in H by R and then integrating, we obtain

$$|R(t,\varepsilon)|^2 + 2\int_0^t \Big|A^{1/2}(s)R(s,\varepsilon)\Big|^2\,ds \le |R(0,\varepsilon)|^2$$

$$+2\int_0^t |\mathcal{F}(s,\varepsilon)|\,|R(s,\varepsilon)|\,ds$$

$$+2\int_0^t\int_0^\infty K(s,\tau,\varepsilon)\,\Big(\big[A(s) - A(\tau)\big]u_\varepsilon(\tau), R(s,\varepsilon)\Big)d\tau ds, \quad \forall t \ge 0.$$

Using condition **(H2)** and the property (**ix**) from Lemma 4.1 we get

$$|R(t,\varepsilon)|^2 + 2\int_0^t \Big|A^{1/2}(s)R(s,\varepsilon)\Big|^2\,ds \le |R(0,\varepsilon)|^2$$

$$+2\int_0^t \Big(|\mathcal{F}(s,\varepsilon)| + C\,M\,\varepsilon^{1/2}\Big)|R(s,\varepsilon)|\,ds, \quad \forall t \ge 0, \quad \forall \varepsilon \in (0,\varepsilon_0). \tag{5.7}$$

Applying Brézis' Lemma to (5.7), we get

$$|R(t,\varepsilon)| + \Big(\int_0^t \Big|A^{1/2}(t)R(s,\varepsilon)\Big|^2\, ds\Big)^{1/2}$$

$$\leq \sqrt{2}\,|R(0,\varepsilon)| + \sqrt{2}\int_0^t \Big(\,|\mathcal{F}(s,\varepsilon)| + C\,M\,\varepsilon^{1/2}\Big)\,ds, \quad \forall t \geq 0, \quad \forall \varepsilon \in (0,\varepsilon_0). \quad (5.8)$$

From (5.4) it follows that

$$\big|R_0\big| \leq |u_{0\varepsilon}-u_0| + \int_0^\infty e^{-\tau}\big|\tilde{u}_\varepsilon(2\varepsilon\tau)-u_{0\varepsilon}\big|\,d\tau \leq |u_{0\varepsilon}-u_0| + \int_0^\infty e^{-\tau}\int_0^{2\varepsilon\tau}\big|\tilde{u}'_\varepsilon(s)\big|\,ds\,d\tau$$

$$\leq |u_{0\varepsilon}-u_0| + C\,\varepsilon\,M\int_0^\infty \tau\, e^{-\tau+\gamma\,\varepsilon\,\tau}\,d\tau \leq |u_{0\varepsilon}-u_0| + C\,M\,\varepsilon, \quad \forall \varepsilon \in (0,\varepsilon_0). \quad (5.9)$$

In what follows we will estimate $\big|\mathcal{F}(t,\varepsilon)\big|$. Using the property $(\mathbf{x})$ from Lemma 4.1 and (5.2), we have

$$\Big|\tilde{f}(t) - \int_0^\infty K(t,\tau,\varepsilon)\,\tilde{f}_\varepsilon(\tau)\,d\tau\Big| \leq |\tilde{f}(t)-\tilde{f}_\varepsilon(t)| + \Big|\tilde{f}_\varepsilon(t) - \int_0^\infty K(t,\tau,\varepsilon)\,\tilde{f}_\varepsilon(\tau)\,d\tau\Big|$$

$$\leq |\tilde{f}(t)-\tilde{f}_\varepsilon(t)| + C(T,p)\|f'_\varepsilon\|_{L^2(0,T\,;\,H)}\,\varepsilon^{1/4},\ \forall \varepsilon \in (0,\varepsilon_0),\ \forall t \in [0,T]. \quad (5.10)$$

Since

$$e^{\tau}\lambda(\sqrt{\tau}) \leq C, \quad \forall \tau \geq 0,$$

the estimates

$$\int_0^t \exp\Big\{\frac{3\tau}{4\varepsilon}\Big\}\lambda\Big(\sqrt{\frac{\tau}{\varepsilon}}\Big)d\tau \leq C\,\varepsilon\int_0^\infty e^{-\tau/4}\,d\tau \leq C\varepsilon, \quad \forall t \geq 0,$$

$$\int_0^t \lambda\Big(\frac{1}{2}\sqrt{\frac{\tau}{\varepsilon}}\Big)\,d\tau \leq \varepsilon\int_0^\infty \lambda\Big(\frac{1}{2}\sqrt{\tau}\Big)\,d\tau \leq C\,\varepsilon, \quad \forall t \geq 0,$$

are true. Then

$$\Big|\int_0^t f_0(\tau,\varepsilon)\,d\tau\Big| \leq C\,\varepsilon, \quad \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \geq 0. \quad (5.11)$$

Using (5.2), (5.10) and (5.11) we obtain

$$\int_0^t \Big(\,|\mathcal{F}(s,\varepsilon)| + C\,M\,\varepsilon^{1/2}\Big)\,d\tau$$

$$\leq C\,\Big(M\,\varepsilon^{1/4} + ||f_\varepsilon - f||_{L^2(0,T;H)}\Big), \quad \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \in [0,T]. \quad (5.12)$$

From (5.8), using (5.9) and (5.12) we get the estimate

$$||R||_{C([0,\,t];\,H)} + ||A(\cdot)^{1/2}R||_{L^2(0,t;H)}$$

$$\leq C\left(M\,\varepsilon^{1/4} + |u_{0\varepsilon} - u_0| + ||f_\varepsilon - f||_{L^p(0,T;H)}\right),\ \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \in [0,T]. \quad (5.13)$$

In the consequence, from (5.6) and (5.13) we deduce

$$||\tilde{u}_\varepsilon - \tilde{v}||_{C([0,t];H)} \leq ||\tilde{u}_\varepsilon - w_\varepsilon||_{C([0,t];H)} + ||R||_{C([0,t];H)}$$

$$\leq C\left(M\,\varepsilon^{1/4} + |u_{0\varepsilon} - u_0| + ||f_\varepsilon - f||_{L^2(0,T;H)}\right), \quad \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \in [0,T]. \quad (5.14)$$

Since $u_\varepsilon(t) = \tilde{u}_\varepsilon(t)$ and $v(t) = \tilde{v}(t)$, for all $t \in [0,T]$, then the estimate (5.1) follows from (5.14). □

Theorem 5.2. *Let $T > 0$. Let us assume that operators $A(t), t \in [0,\infty)$, satisfy conditions* **(H1)**–**(H4)**. *If u_0, $u_{0\varepsilon}$, $A(0)u_{0\varepsilon}$, $u_{1\varepsilon}$, $f_\varepsilon(0) \in V$ and f, $f_\varepsilon \in W^{2,2}(0,T;H)$, then there exist constants $C = C(T,\omega,\gamma,a_0,a_1) > 0$, $\varepsilon_0 = \varepsilon_0(\omega,\gamma,a_0,a_1)$, $\varepsilon_0 \in (0,1)$, such that*

$$||u'_\varepsilon - v' + h_\varepsilon e^{-t/\varepsilon}||_{C([0,\,T]\,;H)}$$

$$\leq C\left(M_1(T,u_{0\varepsilon},u_{1\varepsilon},f_\varepsilon)\,\varepsilon^{1/4} + D_\varepsilon\right), \quad \forall \varepsilon \in (0,\varepsilon_0), \quad (5.15)$$

where u_ε and v are strong solutions to problems (P_ε) and (P_0) respectively, $h_\varepsilon = f_\varepsilon(0) - u_{1\varepsilon} - A(0)u_{0\varepsilon}$,

$$M_1 = |A^{1/2}(0)f_\varepsilon(0)| + |A^{3/2}(0)u_{0\varepsilon}| + |A^{1/2}(0)u_{1\varepsilon}| + ||A(t)h_\varepsilon||_{L^2(0,\infty;H)} + ||f_\varepsilon||_{W^{2,2}(0,\infty;H)},$$

$$D_\varepsilon = ||f_\varepsilon - f||_{W^{1,\,2}(0,\,T;\,H)} + |A_0(u_{0\varepsilon} - u_0)|.$$

Proof. In the proof of this theorem, we will agree to denote the constants $C = C(T,\omega,\gamma,a_0,a_1) > 0$, $\varepsilon_0 = \varepsilon_0(\omega,\gamma,a_0,a_1)$ and $M_1(T,u_{0\varepsilon},u_{1\varepsilon},f_\varepsilon)$ by C, ε_0 and M_1 respectively. Also we preserve for $\tilde{v}(t)$, $\tilde{u}_\varepsilon(t)$, $\tilde{f}(t)$ and $\tilde{f}_\varepsilon(t)$ the same notations as in Theorem 5.1.

By Lemma 3.2, we have that the function

$$\tilde{z}_\varepsilon(t) = \tilde{u}'_\varepsilon(t) + h_\varepsilon e^{-t/\varepsilon}, \ \text{ with } \ h_\varepsilon = f_\varepsilon(0) - u_{1\varepsilon} - A(0)u_{0\varepsilon},$$

is the solution to the problem

$$\begin{cases} \varepsilon\tilde{z}''_\varepsilon(t) + \tilde{z}'_\varepsilon(t) + A(t)\tilde{z}_\varepsilon(t) = \tilde{\mathcal{F}}(t,\varepsilon), \quad t > 0, \\ \tilde{z}_\varepsilon(0) = f_\varepsilon(0) - A(0)u_{0\,\varepsilon}, \quad \tilde{z}'_\varepsilon(0) = 0, \end{cases}$$

where

$$\tilde{\mathcal{F}}(t,\varepsilon) = \tilde{f}'_\varepsilon(t) - A'(t)\tilde{u}_\varepsilon(t) + e^{-t/\varepsilon}\,A(t)h_\varepsilon$$

and

$$||A_0^{1/2}(\cdot)\tilde{z}_\varepsilon||_{C([0,\,t];\,H)} + ||\tilde{z}'_\varepsilon||_{L^2(0,\,t;\,H)} \leq C\,M_1, \quad \forall t \geq 0. \quad (5.16)$$

Since $\tilde{z}'_\varepsilon(0) = 0$, from Theorem 4.1, the function $w_{1\varepsilon}(t)$, defined by

$$w_{1\varepsilon}(t) = \int_0^\infty K(t,\tau,\varepsilon)\,\tilde{z}_\varepsilon(\tau)\,d\tau, \quad (5.17)$$

satisfies in H the following conditions

$$\begin{cases} w'_{1\varepsilon}(t) + A(t)w_{1\varepsilon}(t) = F_1(t,\varepsilon), \quad \text{a. e.} \quad t > 0, \\ w_{1\varepsilon}(0) = \varphi_{1\varepsilon}, \end{cases}$$

for every $0 < \varepsilon < \varepsilon_0$, where

$$F_1(t,\varepsilon) = \int_0^\infty K(t,\tau,\varepsilon)\tilde{f}'_\varepsilon(\tau)\,d\tau - \int_0^\infty K(t,\tau,\varepsilon)\,A'(\tau)\tilde{u}_\varepsilon(\tau)\,d\tau$$

$$+ \int_0^\infty K(t,\tau,\varepsilon)\; e^{-\tau/\varepsilon}A(\tau)h_\varepsilon d\tau + \int_0^\infty K(t,\tau,\varepsilon)\,\big[A(t) - A(\tau)\big]\tilde{z}_\varepsilon(\tau)\,d\tau,$$

$$\varphi_{1\varepsilon} = \int_0^\infty e^{-\tau}\tilde{z}_\varepsilon(2\varepsilon\tau)\,d\tau.$$

Using (5.17), the properties (**vi**), (**viii**) and (**ix**) from Lemma 4.1 and (5.16), we get the estimate

$$\big|\tilde{z}_\varepsilon(t) - w_{1\varepsilon}(t)\big| \le \int_0^\infty K(t,\tau,\varepsilon)\,\big|\tilde{z}_\varepsilon(t) - \tilde{z}_\varepsilon(\tau)\big|\,d\tau$$

$$\le \int_0^\infty K(t,\tau,\varepsilon)\,\Big|\int_\tau^t \big|\tilde{z}'_\varepsilon(s)\big|\,ds\Big|\,d\tau \le C\,M_1\int_0^\infty K(t,\tau,\varepsilon)\,\big|t-\tau\big|^{1/2}\,d\tau$$

$$\le C\,M_1\,\varepsilon^{1/4}, \quad \forall\varepsilon \in (0,\varepsilon_0), \quad \forall t \ge 0,$$

which implies

$$\big|\big|\tilde{z}_\varepsilon - w_{1\varepsilon}\big|\big|_{C([0,t];\,H)} \le C\,M_1\,\varepsilon^{1/4}, \quad \forall\varepsilon \in (0,\varepsilon_0), \quad \forall t \ge 0. \tag{5.18}$$

Let $v_1(t) = \tilde{v}'(t)$, where $\tilde{v}$ is the strong solution to the problem (P_0) with $\tilde{f}$ instead of f and $T = \infty$.

Let us denote by $R_1(t,\varepsilon) = v_1(t) - w_{1\varepsilon}(t)$. The function $R_1(t,\varepsilon)$ verifies in H the following problem

$$\begin{cases} R'_1(t,\varepsilon) + A(t)R_1(t,\varepsilon) = \mathcal{F}_1(t,\varepsilon), \quad t > 0, \\ R_1(0,\varepsilon) = R_{10}, \end{cases}$$

where

$$R_{10} = f(0) - A_0u_0 - \varphi_{1\varepsilon},$$

$$\mathcal{F}_1(t,\varepsilon) = \tilde{f}\,'(t) - \int_0^\infty K(t,\tau,\varepsilon)\tilde{f}'_\varepsilon(\tau)\,d\tau + \int_0^\infty K(t,\tau,\varepsilon)\,A'(\tau)\tilde{u}_\varepsilon(\tau)\,d\tau - A'(t)v(t)$$

$$- \int_0^\infty K(t,\tau,\varepsilon)\; e^{-\tau/\varepsilon}A(\tau)h_\varepsilon d\tau - \int_0^\infty K(t,\tau,\varepsilon)\,\big[A(t) - A(\tau)\big]\tilde{z}_\varepsilon(\tau)\,d\tau. \tag{5.19}$$

Using the properties (**viii**), (**ix**) from Lemma 4.1 and the inequalities (5.2), we get

$$\Big|\tilde{f}'(t) - \int_0^\infty K(t,\tau,\varepsilon)\,\tilde{f}'_\varepsilon(\tau)\,d\tau\Big|$$

$$\leq |\tilde{f}'(t) - \tilde{f}'_\varepsilon(t)| + \int_0^\infty K(t,\tau,\varepsilon)\,\big|\tilde{f}'_\varepsilon(\tau) - \tilde{f}'_\varepsilon(t)\big|\,d\tau$$

$$\leq |\tilde{f}'(t) - \tilde{f}'_\varepsilon(t)| + ||\tilde{f}''_\varepsilon||_{L^2(0,\infty;\,H)} \int_0^\infty K(t,\tau,\varepsilon)\,|t-\tau|^{1/2}\,d\tau \leq |\tilde{f}'(t) - \tilde{f}'_\varepsilon(t)|$$

$$+C(T)\,||f''_\varepsilon||_{L^2(0,\,T;\,H)}\,\varepsilon^{1/2}, \quad \forall \varepsilon \in (0,\varepsilon_0), \quad \forall t \in [0,T]. \tag{5.20}$$

Taking the inner product in H by R_1 and then integrating, we obtain

$$|R_1(t,\varepsilon)|^2 + 2\int_0^t \Big|A^{1/2}(s)R_1(s,\varepsilon)\Big|^2\,ds = |R(0,\varepsilon)|^2$$

$$+2\int_0^t \Big(\mathcal{F}_1(s,\varepsilon), R_1(s,\varepsilon)\Big)ds, \quad \forall t \geq 0. \tag{5.21}$$

Using the properties (**viii**), (**ix**) from Lemma 4.1, conditions **(H2)**, **(H4)**, estimates (5.1), (5.3) and (5.4) we get

$$\Big(\int_0^\infty K(s,\tau,\varepsilon)\,A'(\tau)\tilde{u}_\varepsilon(\tau)\,d\tau - A'(s)v(s), R_1(s,\varepsilon)\Big)$$

$$= \int_0^\infty K(s,\tau,\varepsilon)\,\Big([A'(\tau) - A'(s)]\tilde{u}_\varepsilon(\tau)\,d\tau, R_1(s,\varepsilon)\Big)d\tau$$

$$+ \int_0^\infty K(s,\tau,\varepsilon)\,\Big(A'(s)[\tilde{u}_\varepsilon(\tau) - \tilde{u}_\varepsilon(s)]\,, R_1(s,\varepsilon)\Big)d\tau$$

$$+ \int_0^\infty K(s,\tau,\varepsilon)\,\Big(A'(s)[\tilde{u}_\varepsilon(s) - v(s)], R_1(s,\varepsilon)\Big)d\tau$$

$$\leq C\,\Big(M\,\varepsilon^{1/2} + M\varepsilon^{1/4} + |u_{0\varepsilon} - u_0| + ||f_\varepsilon - f||_{L^2(0,T;H)}\Big)\Big)\big|R_1(s,\varepsilon)\big|$$

$$\leq C\,\Big(M\,\varepsilon^{1/4} + |u_{0\varepsilon} - u_0| + ||f_\varepsilon - f||_{L^2(0,T;H)}\Big)\big|R_1(s,\varepsilon)\big|, \tag{5.22}$$

for every $\varepsilon \in (0,\varepsilon_0)$ and for all $s \in [0,t]$.

Using the property (**xi**) from Lemma 4.1, we can state

$$\int_0^t \int_0^\infty K(s,\tau,\varepsilon)\;e^{-\tau/\varepsilon}|A(\tau)h_\varepsilon|d\tau ds \leq C\,M_1\varepsilon, \quad \forall \varepsilon > 0,\ \forall t \geq 0. \tag{5.23}$$

Using the properties (**viii**), (**ix**) from Lemma 4.1, condition **(H2)** and estimate (5.16) we get

$$\int_0^\infty K(s,\tau,\varepsilon)\,\Big(\,\big[A(s) - A(\tau)\big]\tilde{z}_\varepsilon(\tau), R_1(s,\varepsilon)\Big)\,d\tau$$

$$\leq C\,M_1\,\varepsilon^{1/2}\big|R_1(s,\varepsilon)\big|, \quad \forall \varepsilon \in (0,\varepsilon_0). \tag{5.24}$$

For R_{10}, due to (5.16), we have

$$|R_{10}| \leq |f(0) - f_\varepsilon(0)| + |A_0(u_0 - u_{0\varepsilon})| + \int_0^\infty e^{-\tau}\,|\tilde{z}_\varepsilon(2\varepsilon\tau) - \tilde{z}_\varepsilon(0)|\,d\tau$$

$$\leq |f(0)-f_\varepsilon(0)| + |A_0(u_0-u_{0\varepsilon})| + \int_0^\infty e^{-\tau} \int_0^{2\varepsilon\tau} |\tilde{z}'_\varepsilon(s)|\, ds\, d\tau$$

$$\leq |f(0)-f_\varepsilon(0)| + |A_0(u_0-u_{0\varepsilon})|$$

$$+C\, M_1\, \varepsilon \int_0^\infty \tau\, e^{-\tau+2\,\gamma\,\varepsilon\,\tau}\, d\tau \leq C\, D_\varepsilon + C\, M_1\, \varepsilon, \quad \forall \varepsilon \in (0, \varepsilon_0]. \tag{5.25}$$

Applying Lemma of Brézis to (5.21) and using estimates (5.22), (5.23), (5.24), (5.25), we get

$$|R_1(t,\varepsilon)| + ||A_0^{1/2} R_1||_{L^2(0,t;\, H)}$$

$$\leq C\left(M_1(T, u_{0\varepsilon}, u_{1\varepsilon}, f_\varepsilon)\, \varepsilon^{1/4} + D_\varepsilon\right), \quad \forall \varepsilon \in (0, \varepsilon_0), \tag{5.26}$$

which together with (5.18) implies (5.15). □

6 An example

Let $\Omega \subset R^n$ be an open bounded set with smooth $\partial\Omega$. In the real Hilbert space $L^2(\Omega)$ with the scalar product

$$(u, v) = \int_\Omega u(x)\, v(x)\, dx.$$

we will consider the following Cauchy problem

$$\begin{cases} \varepsilon \partial_t^2\, u_\varepsilon(x,t) + \partial_t\, u_\varepsilon(x,t) + A(x,t) u_\varepsilon(x,t) = f(x,t), \quad x \in \Omega,\ \ t > 0, \\ u_\varepsilon(x,0) = u_{0\varepsilon}(x), \quad \partial_t\, u_\varepsilon(x,0) = u_{1\varepsilon}(x) \end{cases} \tag{6.1}$$

where $D(A(\cdot,t)) = H^2(\Omega) \cap H_0^1(\Omega), \quad t \in [0,\infty)$,

$$A(x,t)u(x) = -\sum_{i,j=1}^n \partial_{x_i}\big(a_{ij}(x,t)\partial_{x_j} u(x)\big) + a(x,t)u(x),\ u \in D(A(\cdot,t)),\ \forall t \in [0,\infty),$$

$$a_{ij}(\cdot,t) \in C^1(\overline{\Omega}),\ a(\cdot,t) \in C(\overline{\Omega}), \quad \forall t \in [0,\infty), \tag{6.2}$$

$$a(x,t) \geq 0,\ \ a_{ij}(x,t) = a_{ji}(x,t), \quad x \in \overline{\Omega}, \quad \forall t \in [0,\infty), \tag{6.3}$$

$$\sum_{i,j=1}^n a_{ij}(x,t)\xi_i\, \xi_j \geq a_0\, |\xi|^2, \quad x \in \overline{\Omega}, \quad \xi \in \mathbb{R}^n, \quad a_0 > 0. \tag{6.4}$$

$a_{ij}(x,\cdot)$, $a(x,\cdot)$ are continuously differentiable on $(0,\infty)$, $\partial_t a_{ij}(x,\cdot), \partial_t a(x,\cdot)$ are bounded on $[0,\infty)$ and

$$\partial_t a_{ij}(\cdot,t) \in C^1(\overline{\Omega}),\ \partial_t a(\cdot,t) \in C(\overline{\Omega}), \quad \forall t \in [0,\infty), \tag{6.5}$$

$a_{ij}(x,\cdot), a(x,\cdot)$ are twice continuously differentiable on $(0,\infty)$, $\partial_t^2 a_{ij}(x,\cdot), \partial_t^2 a(x,\cdot)$ are bounded on $[0,\infty)$, and

$$\partial_t^2 a_{ij}(\cdot,t) \in C^1(\overline{\Omega}), \partial_t^2 a(\cdot,t) \in C(\overline{\Omega}), \quad \forall t \in [0,\infty). \tag{6.6}$$

In conditions (6.2)–(6.3) the operators $A(t)$, $\forall t \in [0,\infty)$, are positive and selfadjoint. Let us now consider the unperturbed problem associated to the problem (6.1)

$$\begin{cases} \partial_t\, v(x,t) + A(x,t)v = f(x,t), \quad x \in \Omega, \ \ t > 0, \\ v(x,0) = u_0(x). \end{cases} \tag{6.7}$$

Using Theorem 5.1 we obtain the following theorem.

Theorem 6.1. *Let $\Omega \subset \mathbb{R}^n$ be an open bounded set with smooth $\partial\Omega$. Let $T > 0$. Suppose that conditions (6.2) – (6.5) are fulfilled. If $u_0, u_{0\,\varepsilon}, u_{1\,\varepsilon} \in H^2(\Omega) \cap H_0^1(\Omega)$, $f, f_\varepsilon \in W^{1,2}(0,T; L_2(\Omega))$, then there exist constants $\varepsilon_0 = \varepsilon_0(\gamma, a_0, \omega) \in (0,1)$ and $C = C(T, n, \gamma, a_0, \omega) > 0$ such that*

$$\begin{aligned} &||u_\varepsilon - v||_{C([0,T];L_2(\Omega))} \\ &\leq C\left(\widetilde{M}\,\varepsilon^{1/4} + \left|u_{0\,\varepsilon} - u_0\right| + \left|\left|f_\varepsilon - f\right|\right|_{L^2(0,T;L_2(\Omega))}\right), \quad \varepsilon \in (0,\varepsilon_0], \end{aligned} \tag{6.8}$$

where u_ε and v are the strong solutions to problems (6.1) and (6.7), respectively, and

$$\widetilde{M} = \left|A(0)u_{0\,\varepsilon}\right| + |A^{1/2}(0)u_{1\,\varepsilon}| + ||f_\varepsilon||_{W^{1,2}(0,\infty;L_2(\Omega))}.$$

Using Theorem 5.2 we obtain the following theorem.

Theorem 6.2. *Let $\Omega \subset \mathbb{R}^n$ be an open bounded set with smooth $\partial\Omega$. Let $T > 0$. Suppose that conditions (6.2) – (6.6) are fulfilled. If*

$$u_0, u_{0\varepsilon}, A(0)u_{0\varepsilon}, u_{1\varepsilon}, f(0), f_\varepsilon(0) \in H^2(\Omega) \cap H_0^1(\Omega), \quad f, f_\varepsilon \in W^{2,2}(0,T; L_2(\Omega)),$$

then there exist constants $\varepsilon_0 = \varepsilon_0(\omega_0, \omega_1) \in (0,1)$ and $C = C(T, n, \omega_0, \omega_1) > 0$ such that

$$\left|\left|u'_\varepsilon - v' + h_\varepsilon\, e^{-\frac{t}{\varepsilon}}\right|\right|_{C([0,\,T];\,L_2(\Omega))} \leq C\left(\widetilde{M}_1\,\varepsilon^{(1/4} + \widetilde{D}_\varepsilon\right), \tag{6.9}$$

where v and u_ε are the strong solutions to problems (6.1) and (6.7), respectively, $h_\varepsilon = f_\varepsilon(0) - u_{1\,\varepsilon} - A(0)u_{0\,\varepsilon}$,

$$\widetilde{D}_\varepsilon = \left|\left|f_\varepsilon - f\right|\right|_{W^{1,\,2}(0,\,T;\,H_0^1(\Omega))} + \left|A_0(u_{0\varepsilon} - u_0)\right|,$$

$$\widetilde{M}_1 = \left|A^{1/2}(0)f_\varepsilon(0)\right| + \left|A^{3/2}(0)u_{0\,\varepsilon}\right| + \left|A^{1/2}(0)u_{1\,\varepsilon}\right| + \left|A(t)h_\varepsilon\right| + \left|\left|f_\varepsilon\right|\right|_{W^{2,2}(0,\,\infty;\,H_0^1(\Omega))}.$$

References

[1] D'Acunto B. *Hyperbolic-parabolic singular perturbations.* Rend. Mat. Appl, 1993, No. 1, 229–254.

[2] Esham B. F., Weinacht R. J. *Hyperbolic-parabolic singular perturbations for scalar nonlinearities.* Appl. Anal., 1988, **29,** No. 1-2, 19–44.

[3] Evans L. C. *Partial Differential Equations.* American Mathematical Society, 1998.

[4] Gallay Th., Raugel G. *Scaling variables and asymptotic expansions in damped wave equations.* J. Differential Equations, 1998, **150,** No. 1, 42–97.

[5] Gobbino M. *Singular perturbation hyperbolic-parabolic for degenerate nonlinear equations of Kirchhoff type.* Nonlinear Anal., 2001, **44,** No. 3, 361–374.

[6] Hajouj B. *Perturbations singulières d'équations hyperboliques du second ordre non linéaires.* Ann. Math. Blaise Pascal, 2000, **7,** No. 1, 1–22.

[7] Horodnii M. F. *Stability of bounded solutions of differential equations with small parameter in a Banach space.* Ukrainian Math. J., 2003, **55,** No. 7, 1071–1085.

[8] Hsiao G., Weinacht R. *Singular perturbations for a semilinear hyperbolic equation.* SIAM J. Math. Anal., 1983, **14,** No. 6, 1168–1179.

[9] Jager E. M. *Singular perturbations of hyperbolic type.* Nieuw Arch. Wisk., 1975, **(3)23,** No. 2, 145-172.

[10] Kubesov N. A. *Asymptotic behavior of the solution of a mixed problem with large initial velocity for a singularly perturbed equation that degenerates into a parabolic equation.* Vestnik Nats. Akad. Respub. Kazakhstan, 1994, **1,** 71–74 (in Russian).

[11] Lions J. L. *Control optimal de systemes gouvernés par des équations aux dérivées partielles.* Dunod Gauthier-Villars, Paris, 1968.

[12] Milani A. *On singular perturbations for IBV problems.* Ann. Fac. Sci. Toulouse Math., 2000, **(6)9,** No. 3, 467–468.

[13] Moroşanu Gh. *Nonlinear Evolution Equations and Applications*, Ed. Acad. Române, Bucureşti, 1988, 340 p.

[14] Perjan A. *Linear singular perturbations of hyperbolic-parabolic type.* Bul. Acad. Stiinte Repub. Mold. Mat., 2003, No. 2(42), 95–112.

[15] Perjan A. *Limits of solutions to the semilinear wave equations with small parameter.* Bul. Acad. Stiinte Repub. Mold. Mat., 2006, No. 1(50), 65–84.

[16] Perjan A., Rusu G. *Convergence estimates for abstract second-order singularly perturbed Cauchy problems with Lipschitzian nonlinearities.* Asymptotic Analysis, 2011, **74**, No. 3-4, 135–165.

[17] Zlamal M. The mixed problem for hyperbolic equations with a small parameter. Czechoslovak Math. J., 1960, **10(85)**, 83–120 (in Rusian).

Andrei Perjan, Galina Rusu
Department of Mathematics and Informatics
Moldova State University
A. Mateevici str. 60, MD 2009, Chisinau
Moldova

E-mail: *perjan@usm.md; rusugalinamoldova@gmail.com*

Received August 3, 2014

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 65–79
ISSN 1024–7696

On LCA groups with locally compact rings of continuous endomorphisms. I

Valeriu Popa

Abstract. We determine the discrete abelian groups and the compact abelian groups with the property that their rings of continuous endomorphisms are locally compact in the compact-open topology.

Mathematics subject classification: 16W80.
Keywords and phrases: LCA groups, rings of continuous endomorphisms, compact-open topology.

1 Introduction

Let X be an LCA group, and let $A(X)$ denote the group of all topological automorphisms of X, taken with the Birkhoff topology. As is well known, $A(X)$ is a Hausdorff topological group [3, Ch. IV]. M. Levin in [9], O. Mel'nikov in [10], P. Plaumann in [12], and L. Robertson in [13] have investigated (among many other things) various types of LCA groups X with the property that their group $A(X)$ is locally compact.

By analogy, one may ask for a description of LCA groups X with the property that the ring $E(X)$ of continuous endomorphisms of X is locally compact in the compact-open topology. Here we answer this question for the case of discrete abelian groups and for the case of compact abelian groups.

2 Notation

Throughout the following, $\mathbb{N}$ is the set of natural numbers (including zero), $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$, and $\mathbb{P}$ is the set of prime numbers.

The groups of which we shall make constant use are the reals modulo one $\mathbb{T}$, the p-adic integers $\mathbb{Z}_p$ (all with their usual topologies), the rationals $\mathbb{Q}$, the quasi-cyclic groups $\mathbb{Z}(p^\infty)$ and the cyclic groups $\mathbb{Z}(n)$ of order n (all with the discrete topology), where $p \in \mathbb{P}$ and $n \in \mathbb{N}_0$.

We denote by $\mathcal{L}$ the class of all locally compact abelian groups. For $X \in \mathcal{L}$, we let $c(X)$, $d(X)$, $k(X)$, $m(X)$, $t(X)$, and X^* denote, respectively, the connected component of zero in X, the maximal divisible subgroup of X, the subgroup of compact elements of X, the smallest closed subgroup K of X such that the quotient group X/K is torsion-free, the torsion subgroup of X, and the character group

of X. Further, we denote by $E(X)$ the ring of continuous endomorphisms of X and by $H(X,Y)$, where $Y \in \mathcal{L}$, the group of continuous homomorphisms from X to Y, both endowed with the compact-open topology. It is well known that $H(X,Y)$ is a topological group and $E(X)$ is a topological ring. Recall that the compact-open topology on $H(X,Y)$ is generated by the sets

$$\Omega_{X,Y}(K,U) = \{h \in H(X,Y) \mid h(K) \subset U\},$$

where K is a compact subset of X and U is an open subset of Y. We write $\Omega_X(K,U)$ for $\Omega_{X,X}(K,U)$.

For $p \in \mathbb{P}$, $n \in \mathbb{N}$ and $X \in \mathcal{L}$, X_p is the topological p-primary component of X, $t_p(X)$ is the p-primary component of $t(X)$, $X[n] = \{x \in X \mid nx = 0\}$, $nX = \{nx \mid x \in X\}$, and $S(X) = \{q \in \mathbb{P} \mid \big(k(X)/c(X)\big)_q \neq 0\}$.

For $a \in X$ and $S \subset X$, $o(a)$ is the order of a, $\langle S\rangle$ is the subgroup of X generated by S, $\overline{S}$ is the closure of S in X, and $A(X^*,S) = \{\gamma \in X^* \mid \gamma(x) = 0 \text{ for all } x \in S\}$. If $(A_i)_{i\in I}$ is an indexed collection of subgroups of X, $\sum_{i\in I} A_i$ stands for $\langle \bigcup_{i\in I} A_i\rangle$.

Further, if A is a closed subgroup of X, then A_* denotes the smallest pure subgroup of X containing A, and X/A the quotient of X modulo A, taken with the quotient topology. Also, we write $X = A \oplus B$ in case X is a topological direct sum of its subgroups A and B.

Let $(X_i)_{i\in I}$ be an indexed collection of groups in $\mathcal{L}$. We write $\prod_{i\in I} X_i$ for the direct product of the groups X_i with the product topology. In case each X_i is discrete, $\bigoplus_{i\in I} X_i$ denotes the external direct sum of the groups X_i, taken with the discrete topology. If each $X_i = X$ for some fixed X, we write X^I for $\prod_{i\in I} X_i$ and $X^{(I)}$ for $\bigoplus_{i\in I} X_i$.

The symbol $\cong$ denotes topological group (ring) isomorphism.

We close this section by mentioning a few facts, which will be used frequently in the sequel. The first one is the famous theorem of Ascoli, whose proof can be found in [2, Ch. X, §2, Theorem 2, Corollary 3].

Theorem 1 (**Ascoli**). *Let X be a locally compact topological space, let Y be a uniform space, and let $C(X,Y)$ be the space of continuous mappings from X into Y, endowed with the compact-open topology. A subset Ω of $C(X,Y)$ is relatively compact in $C(X,Y)$ if ant only if the following conditions hold:*

(i) *Ω is equicontinuous.*

(ii) *For each $a \in X$, the orbit $\Omega a = \{f(a) \mid f \in \Omega\}$ is relatively compact in Y.*

Lemma 1. *For any $X \in \mathcal{L}$, the mapping $f \to f^*$, where the endomorphism $f^* \in E(X^*)$ is defined by $f^*(\gamma) = \gamma \circ f$ for all $\gamma \in X^*$, is a topological ring anti-isomorphism from $E(X)$ onto $E(X^*)$.*

Proof. The assertion follows from [11, Ch. IV, Theorem 4.2, Corollary 2]. □

Lemma 2. *Let X be a group in $\mathcal{L}$ admitting the decomposition $X = A \oplus B$ for some closed subgroups A and B of X. Then $E(X) \cong \begin{pmatrix} E(A) & H(B,A) \\ H(A,B) & E(B) \end{pmatrix}$, where the matrix ring $\begin{pmatrix} E(A) & H(B,A) \\ H(A,B) & E(B) \end{pmatrix}$ is taken with the usual addition and multiplication, and carries the product topology.*

Proof. Since the canonical projections $\pi_A : X \to A$, $\pi_B : X \to B$ and the canonical injections $\eta_A : A \to X$, $\eta_B : B \to X$ are continuous, the mapping

$$\xi : E(X) \to \begin{pmatrix} E(A) & H(B,A) \\ H(A,B) & E(B) \end{pmatrix},\ f \to \begin{pmatrix} \pi_A f \eta_A & \pi_A f \eta_B \\ \pi_B f \eta_A & \pi_B f \eta_B \end{pmatrix},$$

is an isomorphism of rings with the inverse ξ^{-1} given by

$$\xi^{-1}\Big(\begin{pmatrix} f_A & f_{B,A} \\ f_{A,B} & f_B \end{pmatrix}\Big) = \eta_A f_A \pi_A + \eta_A f_{B,A} \pi_B + \eta_B f_{A,B} \pi_A + \eta_B f_B \pi_B$$

[6, Proposition 106.1]. Now, if K_A (resp., K_B) is a compact subset of A (resp., B) and U_A (resp., U_B) is an open neighborhood of zero in A (resp., B), then $K_A + K_B$ is a a compact subset of X, $U_A + U_B$ is an open neighborhood of zero in X, and

$$\xi\big(\Omega_X(K_A + K_B, U_A + U_B)\big) \subset \begin{pmatrix} \Omega_A(K_A, U_A) & \Omega_{B,A}(K_B, U_A) \\ \Omega_{A,B}(K_A, U_B) & \Omega_B(K_B, U_B) \end{pmatrix}.$$

Since the sets $\begin{pmatrix} \Omega_A(K_A, U_A) & \Omega_{B,A}(K_B, U_A) \\ \Omega_{A,B}(K_A, U_B) & \Omega_B(K_B, U_B) \end{pmatrix}$ form a fundamental system of neighborhoods of zero in $\begin{pmatrix} E(A) & H(B,A) \\ H(A,B) & E(B) \end{pmatrix}$, it follows that ξ is continuous. To see that ξ is also open, pick any compact subset K of X and any open neighborhood U of zero in X. Further, choose an open neighborhood V of zero in X such that $V + V \subset U$. Since $X = A \oplus B$, we can consider that $V = \pi_A(V) + \pi_B(V)$. Then

$$\xi\big(\Omega_X(K, U)\big) \supset \begin{pmatrix} \Omega_A(\pi_A(K), \pi_A(V)) & \Omega_{B,A}(\pi_B(K), \pi_A(V)) \\ \Omega_{A,B}(\pi_A(K), \pi_B(V)) & \Omega_B(\pi_B(K), \pi_B(V)) \end{pmatrix},$$

proving that ξ is open. □

3 Discrete torsion groups

We begin our study on local compactness of the topological ring $E(X)$ with the case of discrete torsion groups $X \in \mathcal{L}$. The description of these groups, will permit also to answer our question for compact, totally disconnected groups in $\mathcal{L}$.

First we establish a preparatory fact.

Lemma 3. *Let $p \in \mathbb{P}$, and let X be a discrete p-group in $\mathcal{L}$. If $E(X)$ is locally compact, then X is isomorphic to a group of the form $\mathbb{Z}(p^\infty)^{n_0} \times \prod_{i=1}^{m} \mathbb{Z}(p^{n_i})$, where $m, n_0, \ldots, n_m \in \mathbb{N}$.*

Proof. Let $E(X)$ be locally compact. We can write $X = A \oplus B$, where $A = d(X)$ and B is a reduced subgroup of X. Since

$$E(X) \cong \begin{pmatrix} E(A) & H(B,A) \\ 0 & E(B) \end{pmatrix},$$

it follows that $E(A)$ and $E(B)$ are locally compact. To determine the structure of A, let Ω_A be a compact neighborhood of zero in $E(A)$. Since A is discrete, there is a finite subset K_A of A such that $\Omega_A(K_A, \{0\}) \subset \Omega_A$. Consequently, $\Omega_A(K_A, \{0\})$ is compact in $E(A)$. Let $F_A = \langle K_A \rangle$. Then F_A is finite because A is torsion [5, Theorem 15.5], and A/F_A is divisible because A is divisible [5, (D), p. 98]. It follows that if $A \neq \{0\}$, then $A/F_A \neq \{0\}$ too, and hence we can write $A/F_A = D \oplus D'$, where $D \cong \mathbb{Z}(p^\infty)$ [5, Theorem 23.1]. Let α be the canonical projection of A onto A/F_A and φ the canonical projection of A/F_A onto D with kernel D'. Fix a non-zero $a \in D[p]$ and any $a' \in A$ such that $(\varphi \circ \alpha)(a') = a$. Further, choose an arbitrary $y \in A[p]$, and denote by ξ_y the extension to D of the group homomorphism from $\langle a \rangle$ into A, which transports a to y [5, Theorem 21.1]. Then $(\xi_y \circ \varphi \circ \alpha) \in \Omega_A(K_A, \{0\})$ and $(\xi_y \circ \varphi \circ \alpha)(a') = y$. Since $y \in A[p]$ was chosen arbitrarily, it follows that

$$A[p] \subset \Omega_A(K_A, \{0\})a'.$$

But $\Omega_A(K_A, \{0\})a'$ is finite since $\Omega_A(K_A, \{0\})$ is compact and A is discrete. It follows that $A[p]$ is finite, and hence $A \cong \mathbb{Z}(p^\infty)^{n_0}$ for some $n_0 \in \mathbb{N}$ [5, Theorem 25.1].

Next we determine the structure of B. As in the case of A, there is a finite subset K_B of B such that $\Omega_B(K_B, \{0\})$ is compact in $E(B)$. Let $F_B = \langle K_B \rangle$. Then F_B is finite, and hence if $B = F_B$, there is nothing to prove. Assume $B \neq F_B$. First observe that B/F_B cannot be divisible. For, if it were, then it would follow that $B = pB + F_B$. Choosing $n \in \mathbb{N}$ such that $p^n F_B = \{0\}$, we would obtain $p^n B = p^{n+1} B$, which would imply that $p^n B$ is divisible. Since B is reduced, it would follow that $p^n B = \{0\}$, and hence B/F_B would be of bounded order as well. This is in contradiction with the fact that B/F_B is non-zero and divisible. Consequently, B/F_B is not divisible, and hence its socle contains elements of finite height [5, (C), p. 98]. It follows that B/F_B admits a non-zero cyclic direct summand [5, Corollary 27.2]. Write

$$B/F_B = \langle b \rangle \oplus C$$

for some non-zero $b \in B/F_B$, and let β be the canonical projection of B onto B/F_B, and ψ the canonical projection of B/F_B onto $\langle b \rangle$ with kernel C. Further, let $b' \in B$ be such that $(\psi \circ \beta)(b') = b$. Given any $z \in B[p]$, define $\eta_z \in H(\langle b \rangle, B)$ by setting $\eta_z(b) = z$. Then $\eta_z \circ \psi \circ \beta \in \Omega_B(K_B, \{0\})$ and $(\eta_z \circ \psi \circ \beta)(b') = z$. Since $z \in B[p]$ was chosen arbitrarily, it follows that

$$B[p] \subset \Omega_B(K_B, \{0\})b',$$

so $B[p]$ is finite, and hence $B \cong \prod_{i=1}^m \mathbb{Z}(p^{n_i})$ for some $m, n_1, \ldots, n_m \in \mathbb{N}$ [5, Theorem 25.1]. □

Now we can prove

Theorem 2. *For a discrete torsion group $X \in \mathcal{L}$, the following statements are equivalent:*

(i) *$E(X)$ is compact.*

(ii) *$E(X)$ is locally compact.*

(iii) *For each $p \in S(X)$, $t_p(X)$ is isomorphic with $\mathbb{Z}(p^\infty)^{n_0(p)} \times \prod_{i=1}^{m(p)} \mathbb{Z}(p^{n_i(p)})$, where $m(p), n_0(p), \ldots, n_{m(p)}(p) \in \mathbb{N}$.*

Proof. The fact that (i) and (iii) are equivalent is proved in [6, Proposition 107.4]. It is also clear that (i) implies (ii). Assume (ii), and pick an arbitrary $p \in S(X)$. We can write

$$X = t_p(X) \oplus t_p(X)^{\#},$$

where $t_p(X)^{\#} = \sum_{q \in S(X)\setminus\{p\}} t_q(X)$. It follows from Lemma 2 that $E\big(t_p(X)\big)$ is locally compact, so (ii) implies (iii) by Lemma 3. □

By utilizing duality, we obtain the solution to the considered problem in the case of compact, totally disconnected groups in $\mathcal{L}$.

Corollary 1. *For a compact, totally disconnected group $X \in \mathcal{L}$, the following statements are equivalent:*

(i) *$E(X)$ is compact.*

(ii) *$E(X)$ is locally compact.*

(iii) *For each $p \in S(X)$, X_p is topologically isomorphic with $\mathbb{Z}_p^{n_0(p)} \times \prod_{i=1}^{m(p)} \mathbb{Z}(p^{n_i(p)})$, where $m(p), n_0(p), \ldots, n_{m(p)}(p) \in \mathbb{N}$.*

4 Discrete torsion-free groups

In this section, we consider the case of discrete torsion-free groups in $\mathcal{L}$ and the case of their duals, the compact connected groups in $\mathcal{L}$. We have

Theorem 3. *For a discrete torsion-free group $X \in \mathcal{L}$, the following statements are equivalent:*

(i) *$E(X)$ is discrete.*

(ii) *$E(X)$ is locally compact.*

(iii) *There is a finitely generated subgroup F of X such that X contains no subgroup isomorphic to a group of the form X/L, where L is a proper, pure subgroup of X containing F.*

Proof. Clearly, (i) implies (ii). Assume (ii), and let Ω be a compact neighborhood of zero in $E(X)$. Since X is discrete, there exists a finite subset K of X such that $\Omega_X(K,\{0\}) \subset \Omega$, so $\Omega_X(K,\{0\})$ is compact in $E(X)$. We claim that $\Omega_X(K,\{0\}) = \{0\}$. For, if there existed a nonzero endomorphism $f \in \Omega_X(K,\{0\})$, we would have $f(x) \neq 0$ for some $x \in X\backslash F$. It would then follow that the orbit $\Omega_X(K,\{0\})x$ contains the infinite group $\langle f(x)\rangle$. This is a contradiction because $\Omega_X(K,\{0\})x$ must be finite by Ascoli's theorem. Thus $\Omega_X(K,\{0\}) = \{0\}$, and hence (ii) implies (i).

Next we show that (i) and (iii) are equivalent. Assume (i), and let K be a finite subset of X such that $\Omega_X(K,\{0\}) = \{0\}$. Set $F = \langle K\rangle$. Given any proper, pure subgroup L of X such that $F \subset L$, let λ be the canonical projection of X onto X/L. If there existed an isomorphism η from X/L into X, we would have $\eta\circ\lambda \in \Omega_X(K,\{0\})$. This is a contradiction, because $X/L \neq \{0\}$, and hence $\eta \circ \lambda \neq 0$. Consequently, (i) implies (iii). Now assume (iii), and let F be a finitely generated subgroup of X with the property that X contains no subgroup isomorphic to a group of the form X/L, where L is a proper, pure subgroup of X containing F. Fix a finite set K of generators of F. We claim that $\Omega_X(K,\{0\}) = \{0\}$. Indeed, if there existed a non-zero $f \in \Omega_X(K,\{0\})$, we would have $\ker(f) \neq X$, $F \subset \ker(f)$, and $X/\ker(f) \cong \mathrm{im}(f)$. Moreover, since $\mathrm{im}(f)$ is torsion-free, $\ker(f)$ would also be pure in X [5, (d), p. 114]. This contradiction shows that $\Omega_X(K,\{0\}) = \{0\}$, so (iii) implies (i). □

We mention for later use the following

Corollary 2. *Let $X \in \mathcal{L}$ be discrete, divisible, and torsion-free. The ring $E(X)$ is locally compact if and only if $X \cong \mathbb{Q}^r$ for some $r \in \mathbb{N}$.*

Proof. Let $E(X)$ be locally compact. It follows from Theorem 3 that there is a finitely generated subgroup F of X such that X contains no subgroup isomorphic to a group of the form X/L, where L is a proper, pure subgroup of X containing F. Since any pure subgroup of a divisible group is divisible, we can write $X = F_* \oplus G$ for some subgroup G of X [5, Theorem 21.2]. As $F \subset F_*$ and $G \cong X/F_*$, we must have $X = F_*$, so $X \cong \mathbb{Q}^r$ for some $r \in \mathbb{N}$.

The converse is clear. □

Dualizing Theorem 3 gives the following characterization of compact connected groups $X \in \mathcal{L}$ whose ring $E(X)$ is locally compact.

Corollary 3. *Let $X \in \mathcal{L}$ be compact and connected. The following statements are equivalent:*

(i) *$E(X)$ is discrete.*

(ii) *$E(X)$ is locally compact.*

(iii) *There is a closed subgroup G of X satisfying the conditions:*

  (1) *X/G has no small subgroups;*

(2) *No non-zero quotient of X by a closed subgroup is topologically isomorphic to a pure, closed subgroup of X contained in G.*

Proof. As is well known, X is compact and connected iff X^* is discrete and torsion-free [7, (23.17) and (24.25)]. Now, since $E(X)$ and $E(X^*)$ are topologically isomorphic, it is clear that $E(X)$ is discrete iff $E(X^*)$ is discrete, and $E(X)$ is locally compact iff $E(X^*)$ is locally compact. In particular, it follows from Theorem 3 that (i) and (ii) are equivalent. To finish, it remains to observe that a subgroup F of X^* is finitely generated iff the quotient $X/A(X,F)$ has no small subgroups [1, Proposition 7.9]. Further, a subgroup L of X^* is pure in X^* iff $A(X,L)$ is pure in X [1, Corrolary 7.6] and $F \subset L$ iff $A(X,L) \subset A(X,F)$. Finally, the existence of a monomorphism $f : X^*/L \to X^*$ is equivalent to the existence of a continuous epimorphism $f^* : X \to A(X,L)$ [7, (24.40)]. □

Corollary 4. *Let $X \in \mathcal{L}$ be compact, connected, and torsion-free. The ring $E(X)$ is locally compact if and only if $X \cong (\mathbb{Q}^*)^r$ for some $r \in \mathbb{N}$.*

Proof. Follows from Corollary 2 by duality. □

5 Discrete mixed and reduced groups

For discrete mixed groups in $\mathcal{L}$ the situation is more complicated. In this section we examine the case of reduced groups. We also examine the case of duals of such groups.

We begin by recalling the following

Definition 1. Let X be an abelian group. For $p \in \mathbb{P}$ and $a \in X$, the p-height of a in X is defined by:

$$h_p^X(a) = \begin{cases} n, & \text{if } a \in p^n X \text{ but } a \notin p^{n+1}X; \\ \infty, & \text{if } a \in \bigcap_{i\in\mathbb{N}} p^i X. \end{cases}$$

Theorem 4. *Let $X \in \mathcal{L}$ be discrete, mixed, and reduced. The ring $E(X)$ is locally compact if and only if X has a finitely generated subgroup F satisfying the following conditions:*

(i) *For each proper subgroup L of X such that $F \subset L$ and $X/L \neq t(X/L)$, X contains no subgroup isomorphic to X/L.*

(ii) *For each $p \in S(X)$, either X/F is p-divisible or $t_p(X)$ is finite.*

(iii) *For each non-zero $a \in X$, the set*

$$S_a = \left\{p \in S(X) \mid h_p^{X/F}(a+F) < \infty \ \text{ and } \ t_p(X) \neq X[p^{h_p^{X/F}(a+F)}]\right\}$$

is finite.

Proof. Let $E(X)$ be locally compact. Since X is discrete, there is a finite subset K of X such that $\Omega_X(K,\{0\})$ is compact in $E(X)$. Given $x \in X$, we deduce from the Ascoli's theorem that $\Omega_X(K,\{0\})x$ is finite. Consequently, for any $f \in \Omega_X(K,\{0\})$, $f(x)$ is a torsion element of X, and hence $\mathrm{im}(f) \subset t(X)$. Set $F = \langle K \rangle$.

To see that (i) holds, let L be a proper subgroup of X such that $F \subset L$ and $t(X/L) \neq X/L$, and let $\lambda : X \to X/L$ be the canonical projection. If there existed an isomorphism η from X/L into X, we would have $\eta \circ \lambda \in \Omega_X(K,\{0\})$, a contradiction because $\mathrm{im}(\eta \circ \lambda) \not\subset t(X)$. This proves (i).

To see that (ii) holds, pick any $p \in S(X)$ such that X/F is not p-divisible. Then $F + pX \neq X$, so we can write

$$X/(F+pX) = A \oplus B,$$

where $A \cong \mathbb{Z}(p)$. Let π be the canonical projection of X onto $X/(F+pX)$ and φ the canonical projection of $X/(F+pX)$ onto A with kernel B. Fix a generator g of A, and let $g' \in X$ be such that $(\varphi \circ \pi)(g') = g$. Further, pick any $y \in X[p]$, and define $\xi_y \in H(A,X)$ by setting $\xi_y(g) = y$. It is clear that $\xi_y \circ \varphi \circ \pi \in \Omega_X(K,\{0\})$, so

$$y = (\xi_y \circ \varphi \circ \pi)(g') \in \Omega_X(K,\{0\})g'.$$

Since $y \in X[p]$ was chosen arbitrarily, it follows that

$$X[p] \subset \Omega_X(K,\{0\})g',$$

so $X[p]$ is finite. Since X is reduced, this proves (ii) [5, Theorem 25.1].

To see that (iii) holds, pick any non-zero $a \in X$ and any $p \in S_a$, and set $n = h_p^{X/F}(a+F)$. Then $a \in F + p^n X$ and $a \notin F + p^{n+1}X$, so $X/(F+p^{n+1}X)$ is a non-zero p-group of bounded order and $a + (F + p^{n+1}X)$ has order p in $X/(F+p^{n+1}X)$. Let $g' \in X$ be such that $a - p^n g' \in F$. Then

$$a + (F + p^{n+1}X) = p^n g' + (F + p^{n+1}X).$$

By [6, Corollary 27.1], we can write

$$X/(F+p^{n+1}X) = A' \oplus B',$$

where $A' = \langle g' + (F + p^{n+1}X) \rangle$ and B' is a subgroup of $X/(F+p^{n+1}X)$. Clearly, $g' + (F+p^{n+1}X)$ has order p^{n+1} in $X/(F+p^{n+1}X)$. Let π' be the canonical projection of X onto $X/(F+p^{n+1}X)$ and φ' the canonical projection of $X/(F+p^{n+1}X)$ onto A' with kernel B'. Given any $y \in X[p^{n+1}]$, define $\xi'_y \in H(A,X)$ by setting

$$\xi'_y\big(g' + (F + p^{n+1}X)\big) = y.$$

Then $\xi'_y \circ \varphi' \circ \pi' \in \Omega_X(K,\{0\})$, so

$$p^n y = (\xi'_y \circ \varphi' \circ \pi')(a) \in \Omega_X(K,\{0\})a.$$

Since, by the definition of S_a, $t_p(X)$ contains elements y of order p^{n+1}, it follows that $\Omega_X(K,\{0\})a$ contains at least one non-zero p-element. Thus, if S_a were infinite, it would follow that $\Omega_X(K,\{0\})a$ is infinite as well, a contradiction. This proves (iii).

To show the converse, let F be a finitely generated subgroup of X satisfying the conditions (i), (ii) and (iii), and let K be a finite set of generators of F. We claim that $\Omega_X(K,\{0\})$ is compact in $E(X)$. Indeed, since X is discrete, $\Omega_X(K,\{0\})$ acts equicontinuously on X. Hence, by the Ascoli's theorem, we need only to show that $\Omega_X(K,\{0\})$ acts with finite orbits. Fix an arbitrary $a \in X$. We first show that

$$\Omega_X(K,\{0\})a \subset \sum_{p\in S_a} t_p(X).$$

Pick an arbitrary $f \in \Omega_X(K,\{0\})$. If $f(a) = 0$, there is nothing to prove. Assume $f(a) \neq 0$. Since $F \subset \ker(f)$ and $X/\ker(f) \cong \mathrm{im}(f)$, it follows from (i) that $X/\ker(f)$ is torsion, and hence $\mathrm{im}(f) \subset t(X)$. Consequently, we can write

$$f(a) = b_1 + \cdots + b_m \tag{1}$$

with nonzero $b_1 \in t_{p_1}(X), \ldots, b_m \in t_{p_m}(X)$ for some $m \in \mathbb{N}_0$ and some distinct $p_1, \ldots, p_m \in S(X)$. We must show that $p_1, \ldots, p_m \in S_a$. By way of contradiction, suppose there is $j = 1, \ldots, m$ such that $p_j \notin S_a$. First observe that X/F cannot be p_j-divisible. For, if it were, it would follow from [5, (D), p. 98] that $\mathrm{im}(f)$ is p_j-divisible, so the projection $\mathrm{im}(f)_{p_j}$ of $\mathrm{im}(f)$ into $t_{p_j}(X)$ would be p_j-divisible. As $\mathrm{im}(f)_{p_j}$ is a p_j-group, it would follow that $\mathrm{im}(f)_{p_j}$ is divisible [5, p. 98], which would imply $\mathrm{im}(f)_{p_j} = \{0\}$ because X is reduced. Hence we would have $b_j = 0$, a contradiction. This proves that X/F cannot be p_j-divisible, and hence $t_{p_j}(X)$ must be finite by (ii). Now, since by assumption $p_j \notin S_a$, we must have either $h_{p_j}^{X/F}(a+F) = \infty$, or else $n = h_{p_j}^{X/F}(a+F) < \infty$ and $t_{p_j}(X) = X[p_j^n]$. In the former case, we clearly have $h_{p_j}^{X}\big(f(a)\big) = \infty$ [5, (g), p. 98]. Hence, given any $i \in \mathbb{N}$, we can write $f(a) = p_j^i y_i$ with $y_i \in X$. Further, since the numbers $p_1, \ldots, p_m$ are distinct, we can write $b_k = p_j^i c_{i,k}$ for all $k \neq j$ [5, p. 98]. It follows from (1) that

$$b_j = p_j^i(y_i - c_{i,1} - \cdots - c_{i,j-1} - c_{i,j+1} - \ldots - c_{i,m}).$$

Since $t_{p_j}(X)$ is p_j-pure in X, we conclude that $b_j = p_j^i c_{i,j}$ for some $c_{i,j} \in t_{p_j}(X)$ [5, p. 98]. Thus $h_{p_j}^{t_{p_j}(X)}(b_j) = \infty$, whence $b_j = 0$ because $t_{p_j}(X)$ is finite. This contradicts the assumption that $b_j \neq 0$. In the second case, one can show in a similar way that $h_{p_j}^{t_{p_j}(X)}(b_j) \geq n$, which again gives $b_j = 0$ because, in this case, $t_{p_j}(X)$ cannot have non-zero elements b with $h_{p_j}^{t_{p_j}(X)}(b) \geq n$. This proves that $p_1, \ldots, p_m \in S_a$. Since $f \in \Omega_X(K,\{0\})$ was chosen arbitrarily, we conclude that $\Omega_X(K,\{0\})a \subset \sum_{p\in S_a} t_p(X)$. Finally, in order to show that $\Omega_X(K,\{0\})$ acts with finite orbits, it is enough to show by the finiteness of S_a that for each $p \in S_a$, $t_p(X)$ is finite. But, if $p \in S_a$, then $n = h_p^{X/F}(a+F) < \infty$, so $a \in F + p^n X$ and $a \notin F + p^{n+1}X$. It follows

that $X \neq F + p^{n+1}X$, so $X/(F + p^{n+1}X)$, being a non-zero p-group of bounded order, cannot be p-divisible [5, p. 98]. As

$$X/(F + p^{n+1}X) \cong \big(X/F\big)/\big((F + p^{n+1}X)/F\big),$$

X/F cannot be p-divisible too, so $t_p(X)$ is finite by (ii). The proof is complete. □

To state the dual analog of Theorem 4, several additional concepts must be introduced.

Definition 2. A group $X \in \mathcal{L}$ is said to be

(i) comixed if either $\bigcap_{n\in\mathbb{N}} \overline{nX}$ is a non-trivial subgroup of X, i.e. $\{0\} \subsetneq \bigcap_{n\in\mathbb{N}} \overline{nX} \subsetneq X$, or $\bigcap_{n\in\mathbb{N}} \overline{nX} = \{0\}$ and none of the subgroups $\overline{nX}$ with $n \in \mathbb{N}_0$ is compact.

(ii) coreduced if $m(X) = X$.

Definition 3. Let $X \in \mathcal{L}$. A closed subgroup C of X is said to be submaximal in X if X/C is topologically isomorphic to a closed subgroup of $\mathbb{T}$.

Definition 4. Let $X \in \mathcal{L}$, and let C and G be closed subgroups of X. For $p \in \mathbb{P}$, the p-coheight of C in G is defined by:

$$ch_p^G(C) = \begin{cases} n, & \text{if } G[p^n] \subset C \text{ but } G[p^{n+1}] \not\subset C; \\ \infty, & \text{if } t_p(G) \subset C. \end{cases}$$

We have

Corollary 5. *Let $X \in \mathcal{L}$ be compact, comixed, and coreduced. The ring $E(X)$ is locally compact if and only if X has a closed subgroup G satisfying the following conditions:*

(i) *X/G has no small subgroups.*

(ii) *No quotient of X by a closed subgroup is topologically isomorphic to a closed subgroup M of G with $c(M) \neq \{0\}$.*

(iii) *For each $p \in S(X)$, either $G[p] = \{0\}$ or $\bigcap_{n\in\mathbb{N}} p^n X$ is open in X.*

(iv) *For each submaximal subgroup C of X, the set*

$$S_C = \big\{p \in S(X) \mid ch_p^G(C) < \infty \text{ and } \bigcap_{n\in\mathbb{N}} p^n X \neq p^{ch_p^G(C)} X\big\}$$

is finite.

Proof. Clearly, X is compact, comixed, and coreduced iff X^* is discrete, mixed, and reduced. It follows from Lemma 1 that $E(X)$ is locally compact iff X^* satisfies the conditions of Theorem 4. It remains to translate these conditions in terms of X. We already mentioned in the proof of Corollary 3 that a subgroup F of X^* is finitely generated iff the quotient $X/A(X,F)$ has no small subgroups. Now, a subgroup L of X^* has the property that $X^*/L \neq t(X^*/L)$ iff its annihilator $A(X,L)$ has non-zero connected component. For,

$$c\big(A(X,L)\big) \cong c\big((X^*/L)^*\big) \cong A\big((X^*/L)^*, t(X^*/L)\big)$$

by [7, (23.25) and (24.20)]. It follows that X^* satisfies condition (i) of Theorem 4 iff X satisfies condition (ii) of this corollary. Further, given any $p \in S(X)$ and any subgroup F of X^*, we deduce from [7, (23.25) and (24.22)(i)] that

$$A(X,F)[p] \cong (X^*/F)^*[p] = A\big((X^*/L)^*, p(X^*/F)\big).$$

It follows that X^*/F is p-divisible iff $A(X,F)[p] = \{0\}$. It is also clear from [1, (e), p. 10] that $t_p(X^*)$ is finite in X^* iff $\cap_{n\in\mathbb{N}} p^n X$ is open in X. Consequently, X^* satisfies condition (ii) of Theorem 4 iff X satisfies condition (iii) of this corollary. Finally, we deduce from [7, (23.25)] that a closed subgroup C of X is submaximal in X iff $A(X^*,C)$ is cyclic in X^*. Letting $a \in X^*$ be a generator of $A(X^*,C)$, it is easy to see by use of duality that $ch_p^{A(X,F)}(C) = h_p^{X^*/F}(a+F)$, and $p^{ch_p^{A(X,F)}(C)} X \neq \cap_{n\in\mathbb{N}} p^n X$ iff $X^*[p^{h_p^{X^*/F}(a+F)}] \neq t_p(X^*)$. It follows that X^* satisfies condition (iii) of Theorem 4 iff X satisfies condition (iv) of our corollary. □

6 Discrete mixed and non-reduced groups

In this final section, we handle the remaining case of discrete, mixed, and non-reduced groups in $\mathcal{L}$. By duality, we obtain also the solution to our problem in the case of compact, comixid groups $X \in \mathcal{L}$ with $m(X) \neq X$.

Theorem 5. *Let X be a discrete, mixed, non-reduced group in $\mathcal{L}$, written in the form $X = d(X) \oplus Y$ for some reduced subgroup Y of X. The ring $E(X)$ is locally compact if and only if the following conditions hold:*

(i) $d(X) \cong \mathbb{Q}^r \times \big(\bigoplus_{p\in S(d(X))} \mathbb{Z}(p^\infty)^{n_p}\big)$, *where r and the n_p's are positive integers.*

(ii) *There is a finitely generated subgroup M of Y satisfying:*

(1) $Y/M = t(Y/M)$.

(2) *For each $p \in S(Y)$, either Y/M is p-divisible or $t_p(Y)$ is finite.*

(3) *For each non-zero $a \in Y$, the set*

$$S_a = \big\{p \in S(Y) \mid h_p^{Y/M}(a+M) < \infty \ \text{ and } \ t_p(Y) \neq Y[p^{h_p^{Y/M}(a+M)}]\big\}$$

is finite.

Proof. Let $E(X)$ be locally compact. Since $X = d(X) \oplus Y$, we have

$$E(X) \cong \begin{pmatrix} E(d(X)) & H(Y, d(X)) \\ 0 & E(Y) \end{pmatrix},$$

so $E(d(X))$, $E(Y)$, and $H(Y, d(X))$ are locally compact. Further, we can write $d(X) = A \oplus B$, where $A = t(d(X))$ and $t(B) = \{0\}$. Then

$$E(d(X)) \cong \begin{pmatrix} E(A) & H(B, A) \\ 0 & E(B) \end{pmatrix},$$

so $E(A)$, $E(B)$, and $H(B, A)$ are locally compact as well. Now, from the local compactness of $E(A)$ it follows by Theorem 2 that for each $p \in S(d(X))$, $t_p(A) \cong \mathbb{Z}(p^\infty)^{n_p}$ for some $n_p \in \mathbb{N}_0$. Further, from the local compactness of $E(B)$ it follows by Corollary 2 that $B \cong \mathbb{Q}^r$ for some $r \in \mathbb{N}$. Hence (i) holds.

Next, from the local compactness of $H(Y, d(X))$, we deduce that there exists a finite subset K of Y such that $\Omega_{Y,d(X)}(K, \{0\})$ is compact in $H(Y, d(X))$. In addition, from the local compactness of $E(Y)$, we conclude that there is a finitely generated subgroup F of Y satisfying the conditions (i)-(iii) of Theorem 4. Fix a finite set K' of generators of F, and set $M = \langle K \cup K' \rangle$. Let us establish (1). Suppose the contrary, and pick an element $a \in Y$ with $o(a + M) = \infty$. We can define, for each $z \in d(X)$, a group homomorphism $\xi_z : \langle a + M \rangle \to d(X)$ by setting $\xi_z(a + M) = z$. Since $d(X)$ is divisible, ξ_z extends to a group homomorphism $\widehat{\xi_z} : Y/M \to d(X)$. Letting $\pi : Y \to Y/M$ denote the canonical projection, we have $\widehat{\xi_z} \circ \pi \in \Omega_{Y,d(X)}(K \cup K', \{0\})$ and $z = (\widehat{\xi_z} \circ \pi)(a)$, so $z \in \Omega_{Y,d(X)}(K \cup K', \{0\})a$. Since $z \in d(X)$ was chosen arbitrarily, it follows that

$$d(X) \subset \Omega_{Y,d(X)}(K \cup K', \{0\})a.$$

This is a contradiction because $\Omega_{Y,d(X)}(K \cup K', \{0\})a$ is finite by Ascoli's theorem and $d(X)$ is infinite. Thus Y/M must be torsion. To see that (2) holds, pick any $p \in S(Y)$. By the choice of F, either Y/F is p-divisible, or $t_p(Y)$ is finite. Since $Y/M \cong \big(Y/F\big)/\big(M/F\big)$, it is clear that if Y/M is not p-divisible, then Y/F is not p-divisible as well. Therefore (2) must hold. Finally, to see that (3) holds, pick any non-zero $a \in Y$. By the choice of F, the set

$$S_a^F = \big\{p \in S(Y) \mid h_p^{Y/F}(a + F) < \infty \ \text{ and } \ t_p(Y) \neq Y[p^{h_p^{Y/F}(a+F)}]\big\}$$

is finite. But since Y/M is a homomorphic image of Y/F, we have

$$h_p^{Y/F}(a + F) \leq h_p^{Y/M}(a + M),$$

whence

$$Y[p^{h_p^{Y/F}(a+F)}] \subset Y[p^{h_p^{Y/M}(a+M)}]$$

for all $p \in S(Y)$. It follows that $S_a \subset S_a^F$, which proves (3).

For the converse, we first show that $E(d(X))$ is locally compact. Indeed, we can write $d(X) = A \oplus B$, where $A \cong \bigoplus_{p\in S\left(t\left(d(X)\right)\right)} \mathbb{Z}(p^\infty)^{n_p}$ and $B \cong \mathbb{Q}^r$. It is clear from Theorem 2 and Corollary 2 that $E(A)$ and $E(B)$ are locally compact. Since

$$E(d(X)) \cong \begin{pmatrix} E(A) & H(B,A) \\ 0 & E(B) \end{pmatrix},$$

it remains to show that $H(B,A)$ is locally compact. But $H(B,A) \cong H(\mathbb{Q},A)^r$ [7, (24.34)(c)], so it suffices to show that $H(\mathbb{Q},A)$ is locally compact. We claim that $\Omega_{\mathbb{Q},A}(\{1\},\{0\})$ is compact in $H(\mathbb{Q},A)$. Clearly, $\Omega_{\mathbb{Q},A}(\{1\},\{0\})$ is equicontinuous. Pick any $a \in \mathbb{Q}$, and let $\pi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ denote the canonical projection. Since $\mathbb{Q}/\mathbb{Z}$ is torsion, we can write $\pi(a) = \sum_{p\in P_a} b_p$, where P_a is a finite subset of $\mathbb{P}$ and $b_p \in t_p(\mathbb{Q}/\mathbb{Z})$ for each $p \in P_a$. It is clear that $\pi(a) \in \sum_{p\in P_a}(\mathbb{Q}/\mathbb{Z})[p^{n_p}]$, where, for each $p \in P_a$, n_p denotes the exponent of b_p. Given any $f \in \Omega_{\mathbb{Q},A}(\{1\},\{0\})$, we can write $f = \widehat{f} \circ \pi$ for some $\widehat{f} \in H(\mathbb{Q}/\mathbb{Z},A)$ [8, Theorem 5.6]. It follows that

$$f(a) = \widehat{f}(\pi(a)) \in \sum_{p\in P_a\cap S(A)} \widehat{f}\big((\mathbb{Q}/\mathbb{Z})[p^{n_p}]\big) \subset \sum_{p\in P_a\cap S(A)} A[p^{n_p}],$$

so

$$\Omega_{\mathbb{Q},A}(\{1\},\{0\})a \ \subset \sum_{p\in P_a\cap S(A)} A[p^{n_p}],$$

and hence $\Omega_{\mathbb{Q},A}(\{1\},\{0\})a$ is finite. This proves that $\Omega_{\mathbb{Q},A}(\{1\},\{0\})$ is compact, so $E(d(X))$ is locally compact. Next, since Y certainly satisfies the conditions of Theorem 4, we deduce that $E(Y)$ is locally compact as well. To finish, it is enough, in view of the isomorphism

$$E(X) \cong \begin{pmatrix} E(d(X)) & H(Y,d(X)) \\ 0 & E(Y) \end{pmatrix},$$

to show that $H(Y,d(X))$ is locally compact. Fix a finite set K of generators of M. We claim that $\Omega_{Y,d(X)}(K,\{0\})$ is compact in $H(Y,d(X))$. To see this, it suffices to show that $\Omega_{Y,d(X)}(K,\{0\})$ acts with finite orbits. Let $\pi' : Y \to Y/M$ be the canonical projection, and pick an arbitrary $a \in Y$. Since Y/M is torsion, we can write $\pi'(a) = \sum_{p\in P'_a} b'_p$, where P'_a is a finite subset of $\mathbb{P}$ and $b'_p \in t_p(Y/M)$ for each $p \in P'_a$. It is clear that $\pi'(a) \in \sum_{p\in P'_a}(Y/M)[p^{n_p}]$, where, for each $p \in P'_a$, n_p denotes the exponent of b'_p. As every $f \in \Omega_{Y,d(X)}(K,\{0\})$ can be written in the form $f = \widehat{f} \circ \pi'$ for some $\widehat{f} \in H(Y/M,d(X))$ [8, Theorem 5.6], we conclude that

$$\Omega_{Y,d(X)}(K,\{0\})a \ \subset \sum_{p\in P'_a\cap S(A)} A[p^{n_p}],$$

proving that $\Omega_{Y,d(X)}(K,\{0\})a$ is finite. Hence $H(Y,d(X))$ is locally compact. The proof is complete. □

We end by stating the dual analog of Theorem 5.

Corollary 6. *Let X be a compact, comixed group in $\mathcal{L}$ with $m(X) \neq X$. The ring $E(X)$ is locally compact if and only if the following conditions hold:*

(i) $X/m(X) \cong (\mathbb{Q}^*)^r \times \prod_{p\in S(Y)} \mathbb{Z}_p^{n_p}$, *where r and the n_p's are positive integers.*

(ii) *There exists a closed totally disconnected subgroup L of $m(X)$ satisfying:*

(1) *$m(X)/L$ has no small subgroups.*

(2) *For each $p \in S(m(X))$, either $L[p] = \{0\}$ or $\bigcap_{n\in\mathbb{N}} p^n\big(m(X)\big)$ is open in $m(X)$.*

(3) *For each submaximal subgroup C of $m(X)$, the set*

$$S_C = \Big\{p \in S(m(X)) \mid ch_p^L(C) < \infty \ \text{ and } \ \bigcap_{n\in\mathbb{N}} p^n\big(m(X)\big) \neq p^{ch_p^L(C)}\big(m(X)\big)\Big\}$$

is finite.

Proof. Clearly, a group $X \in \mathcal{L}$ is compact, comixed, and satisfies $m(X) \neq X$ iff X^* is discrete, mixed, and non-reduced. In particular, $X^* = d(X^*) \oplus Y$ for some reduced subgroup Y of X^*, whence

$$X = m(X) \oplus A(X, Y).$$

Now, in view of Lemma 1, $E(X)$ is locally compact iff X^* satisfies the conditions of Theorem 5. It remains to translate these conditions in terms of X. Since

$$d(X^*) \cong \big(X/m(X)\big)^*,$$

it is clear that X^* satisfies condition (i) of Theorem 5 iff X satisfies condition (i) of this corollary. We next show that X^* satisfies condition (ii) of Theorem 5 iff X satisfies condition (ii) of our corollary. Given a subgroup M of Y, we have $A(X, M) \supset A(X, Y)$, so

$$A(X, M) = \big(m(X) \cap A(X, M)\big) \oplus A(X, Y).$$

Since

$$M^* \cong X/A(X, M) \cong m(X)/\big(m(X) \cap A(X, M)\big),$$

we conclude that M is finitely generated iff $m(X)/\big(m(X) \cap A(X, M)\big)$ has no small subgroups [1, Proposition 7.9]. Further, by [4, Exercise 3.8.7(b)], we have

$$\big(Y/M\big)^* \cong A(X, M)/A(X, Y) \cong m(X) \cap A(X, M),$$

so Y/M is torsion iff $m(X) \cap A(X, M)$ is totally disconnected [7, (24.26)]. It follows that Y has a finitely generated subgroup M satisfying condition (1) of Theorem 5 iff $m(X)$ has a closed totally disconnected subgroup L satisfying condition (1) of our corollary. Next, since

$$Y \cong X^*/d(X^*) \cong m(X)^*,$$

it is clear that $S(m(X)) = S(Y)$. Given any $p \in S(Y)$, we have

$$\begin{aligned} A\big((Y/M)^*, p(Y/M)\big) &\cong (Y/M)^*[p] \\ &\cong \big(A(X,M)/A(X,Y)\big)[p] \\ &\cong \big(m(X) \cap A(X,M)\big)[p], \end{aligned}$$

so Y/M is p-divisible iff $\big(m(X) \cap A(X,M)\big)[p] = \{0\}$. Taking account of the isomorphism $Y^* \cong m(X)$, we also see that $t_p(Y)$ is finite iff $\bigcap_{n\in\mathbb{N}} p^n\big(m(X)\big)$ is open in $m(X)$. Consequently, X^* satisfies condition (2) of Theorem 5 iff X satisfies condition (2) of this corollary. Finally, it follows from [7, (23.25)] that a closed subgroup C of $m(X)$ is submaximal in $m(X)$ iff $A(m(X)^*, C)$ is cyclic in $m(X)^*$. Since $m(X)^* \cong Y$, it is easy to see by use of duality that X^* satisfies condition (3) of Theorem 4 iff X satisfies condition (3) of this corollary. □

References

[1] Armacost D. L. *The structure of locally compact abelian groups.* Pure and Applied Mathematics Series, Vol. 68 (Marcel Dekker, ed.), New York, 1981.

[2] Bourbaki N. *Topologie generale, Chapter IX-X, Éléments de mathematique.* Nauka, Moscow, 1975.

[3] Braconnier J. *Sur les groupes topologiques localement compact.* J. Math. Pures Apl., 1948, **27**, No. 9, 1–85.

[4] Dikranjan D., Prodanov I., Stoyanov L. *Topological groups.* Pure and Applied Mathematics Series, Vol. 130 (Marcel Dekker, ed.), New York and Basel, 1990.

[5] Fuchs L. *Infinite abelian groups, Vol. 1.* Academic Press, New York and London, 1970.

[6] Fuchs L. *Infinite abelian groups, Vol. 2.* Academic Press, New York and London, 1973.

[7] Hewitt E., Ross K. *Abstract Harmonic Analysis, Vol. 1.* Academic Press, New York, 1963.

[8] Hungerford Th. W. *Algebra.* Springer-Verlag, New York, 1974.

[9] Levin M. *The automorphism group of a locally compact abelian group.* Acta Math., 1971, **127**, 259–278.

[10] Mel'nikov O. *Compactness conditions for groups of automorphisms of topological groups.* Mat. Zametki, 1976, **19**(5), 735–743.

[11] Moskowitz M. *Homological algebra in locally compact abelian groups.* Trans. Amer. Math. Soc., 1967, **127**, 361–404.

[12] Plaumann P. *Automorphism groups of locally compact abelian groups.* Lecture Notes Math., 1981, **874**, 272–282.

[13] Robertson L. *Connectivity, divisibility, and torsion.* Trans. Amer. Math. Soc., 1967, **128**, 482–505.

Valeriu Popa
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD-2028, Chişinău
Moldova
E-mail: *vpopa@math.md*

Received August 25, 2014

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 80–88
ISSN 1024–7696

Algorithms for solving stochastic discrete optimal control problems on networks

Dmitrii Lozovanu, Maria Capcelea

Abstract. In this paper we consider the stationary stochastic discrete optimal control problem with average cost criterion. We formulate this problem on networks and propose polynomial time algorithms for determining the optimal control by using a linear programming approach.

Mathematics subject classification: 93E20, 90C05.
Keywords and phrases: Time-discrete system, optimal control, stochastic network, Markov process, optimal strategy, linear programming.

1 Problem Formulation

Let a discrete dynamical system $\mathbb{L}$ with finite set of states X be given, where $|X| = n$. At every discrete moment of time $t = 0, 1, 2, \dots$ the state of $\mathbb{L}$ is $x(t) \in X$. The dynamics of the system is described by a directed graph of states' transitions $G = (X, E)$ where the set of vertices X corresponds to the set of states of the dynamical system and an arbitrary directed edge $e = (x, y) \in E$ expresses the possibility of the system $\mathbb{L}$ to pass from the state $x = x(t)$ to the state $y = x(t + 1)$ at every discrete moment of time t. So, a directed edge $e = (x, y)$ in G corresponds to a stationary control of the system in the state $x \in X$ which provides a transition from $x = x(t)$ to $y = x(t + 1)$ for every discrete moment of time t. We assume that graph G does not contain deadlock vertices, i.e., for each vertex x there exists at least one leaving directed edge $e = (x, y) \in E$. In addition, we assume that with each edge $e = (x, y) \in E$ a quantity $c_e \in \mathbb{R}$ is associated, which expresses the cost of the system $\mathbb{L}$ to pass from the state $x = x(t)$ to the state $y = x(t)$ for every $t = 0, 1, 2, \dots$.

A sequence of directed edges $E' = \{e_0, e_1, e_2, \dots, e_t, \dots\}$, where $e_t = (x(t), x(t + 1))$, $t = 0, 1, 2, \dots$, determines in G a control of the dynamical system with a fixed starting state $x_0 = x(0)$. An arbitrary control in G generates a trajectory $x_0 = x(0), x(1), x(2), \dots$ for which the average cost per transition can be defined in the following way

$$f(E') = \lim_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} c_{e_\tau}.$$

In [1] it is shown that this value exists and $|f_{x_0}(E')| \leq \max_{e\in E'} |c_e|$. Moreover, in [1] it is shown that if G is strongly connected, then for an arbitrary fixed starting

state $x_0 = x(0)$ there exists the optimal control $E^* = \{e_0^*, e_1^*, e_2^* \dots\}$ for which

$$f(E^*) = \min_{E'} \lim_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} c_{e_\tau}$$

and this optimal control does not depend either on the starting state or on time. Therefore, the optimal control for this problem can be found in the set of stationary strategies $\mathbb{S}$.

We assume that the set of states X of the dynamical system may admit states in which the system $\mathbb{L}$ makes transitions to the next state in a random way according to a given distribution function of probabilities on the set of possible transitions from these states [2]. So, the set of states X is divided into two subsets X_C and X_N $(X = X_C \cup X_N,\ X_C \cap X_N = \emptyset)$, where X_C represents the set of states $x \in X$ in which the transitions of the system to the next state y can be controlled by the decision maker at every discrete moment of time t and X_N represents the set of states $x \in X$ in which the decision maker is not able to control the transition because the system passes to the next state y randomly. Thus, for each $x \in X_N$ a probability distribution function $p_{x,y}$ on the set of possible transitions (x, y) from x to $y \in X(x)$ is given, i. e.,

$$\sum_{y\in X(x)} p_{x,y} = 1, \quad \forall x \in X_N; \quad p_{x,y} \geq 0, \quad \forall y \in X(x). \tag{1}$$

Here $p_{x,y}$ expresses the probability of the system's transition from the state x to the state y for every discrete moment of time t.

We call the graph G, with the properties mentioned above, decision network and denote it by (G, X_C, X_N, c, p, x_0). So, this network is determined by the directed graph G with a fixed starting state x_0, the subsets X_C, X_N, the cost function $c : E \to \mathbb{R}$ and the probability function $p : E_N \to [0, 1]$ on the subset of the edges $E_N = \{e = (x, y) \in E \,|\, x \in X_N,\ y \in X\}$, where p satisfies the condition (1). If the control problem is considered for an arbitrary starting state, then we denote the network by (G, X_C, X_N, c, p).

We define a stationary strategy for the control problem on networks as a map:

$$s : x \to y \in X(x) \quad \text{for} \quad x \in X_C,$$

where $X(x) = \{y \in X | e = (x, y) \in E\}$.

Let s be an arbitrary stationary strategy. Then we can determine the graph $G_s = (X,\ E_s \cup E_N)$, where $E_s = \{e = (x, y) \in E \,|\, x \in X_C,\ y = s(x)\}$. This graph corresponds to a Markov process with the probability matrix $P^s = (p^s_{x,y})$, where

$$p^s_{x,y} = \begin{cases} p_{x,y} & \text{if} \quad x \in X_N \quad \text{and} \quad y = X; \\ 1 & \text{if} \quad x \in X_C \quad \text{and} \quad y = s(x); \\ 0 & \text{if} \quad x \in X_C \quad \text{and} \quad y \neq s(x). \end{cases}$$

In the considered Markov process, for an arbitrary state $x \in X_C$, the transition $(x, s(x))$ from the states $x \in X_C$ to the states $y = s(x) \in X$ is made with the probability $p_{x,s(x)} = 1$ if the strategy s is applied. For this Markov process we can determine the average cost per transition for an arbitrary fixed starting state $x_i \in X$. Thus, we can determine the vector of average costs ω^s, which corresponds to the strategy s, according to the formula $\omega^s = Q^s \mu^s$, where Q^s is the limit matrix of the Markov process, generated by the stationary strategy s, and μ^s is the corresponding vector of the immediate costs, i.e., $\mu_x^s = \sum_{y \in X(x)} p_{x,y}^s c_{x,y}$ [3]. A component ω_x^s of the vector ω^s represents the average cost per transition in our problem with a given starting state x and a fixed strategy s, i.e., $f_x(s) = \omega_x^s$.

In such a way we can define the value of the objective function $f_{x_0}(s)$ for the control problem on a network with a given starting state x_0, when the stationary strategy s is applied.

The control problem on the network (G, X_C, X_N, c, p, x_0) consists of finding a stationary strategy s^* for which

$$f_{x_0}(s^*) = \min_s f_{x_0}(s).$$

2 A Linear Programming Approach for Determining Optimal Stationary Strategies on Perfect Networks

We consider the stochastic control problem on the network (G, X_C, X_N, c, p, x_0) with $X_C \neq \emptyset$, $X_N \neq \emptyset$ and assume that G is a strongly connected directed graph. Additionally, we assume that in G for an arbitrary stationary strategy $s \in \mathbb{S}$ the subgraph $G_s = (X, E_s \cup E_N)$ is strongly connected. This means that the Markov chain induced by the probability transition matrix P^s is irreducible for an arbitrary strategy s. We call the decision network with such a condition a *perfect network*. At first we describe an algorithm for determining the optimal stationary strategies for the control problem on perfect networks.

So, in this section we consider the control problem that the average cost per transition is the same for an arbitrary starting state, i. e., $f_x(s) = \omega^s, \quad \forall x \in X$.

Let $s \in \mathbb{S}$ be an arbitrary strategy. Taking into account that for every fixed $x \in X_C$ we have a unique $y = s(x) \in X(x)$, we can identify the map s with the set of boolean values $s_{x,y}$ for $x \in X_C$ and $y \in X(x)$, where

$$s_{x,y} = \begin{cases} 1 & \text{if} \quad y = s(x); \\ 0 & \text{if} \quad y \neq s(x). \end{cases}$$

For the optimal stationary strategy s^* we denote the corresponding boolean values by $s_{x,y}^*$.

Assume that the network (G, X_C, X_N, c, p, x_0) is perfect. Then the following lemma holds.

Lemma 1. *A stationary strategy s^* is optimal if and only if it corresponds to an optimal solution q^*, s^* of the following mixed integer bilinear programming problem:*

Minimize

$$\psi(s,q) = \sum_{x\in X_C}\sum_{y\in X(x)} c_{x,y}s_{x,y}q_x + \sum_{z\in X_N}\mu_z q_z \tag{2}$$

subject to

$$\begin{cases} \sum\limits_{x\in X_C} s_{x,y}q_x + \sum\limits_{z\in X_N} p_{z,y}q_z = q_y, \quad \forall y\in X; \\ \sum\limits_{x\in X_C} q_x + \sum\limits_{z\in X_N} q_z = 1; \\ \sum\limits_{y\in X(x)} s_{x,y} = 1, \quad \forall x\in X_C; \\ \qquad s_{x,y}\in\{0,1\}, \quad \forall x\in X_C,\ y\in X; \quad q_x\geq 0, \quad \forall x\in X, \end{cases} \tag{3}$$

where

$$\mu_z = \sum_{y\in X(z)} p_{z,y}c_{z,y}, \quad \forall z\in X_N.$$

Proof. Denote $\mu_x = \sum_{y\in X(x)} c_{x,y}s_{x,y}$ for $x\in X_C$. Then μ_x for $x\in X_C$ and μ_z for $z\in X_N$ represent, respectively, the immediate cost of the system in the states $x\in X_C$ and $z\in X_N$ when the strategy $s\in S$ is applied. Indeed, we can consider the values $s_{x,y}$ for $x\in X_C$ and $y\in X(x)$ as probability transitions from the state $x\in X_C$ to the state $y\in X(x)$.

Therefore, for fixed s the solution $q^s = (q^s_{x_{i_1}}, q^s_{x_{i_2}}, \ldots, q^s_{x_{i_n}})$ of the system of linear equations

$$\begin{cases} \sum\limits_{x\in X_C} s_{x,y}q_x + \sum\limits_{z\in X_N} p_{z,y}q_z = q_y, \quad \forall y\in X; \\ \sum\limits_{x\in X_C} q_x + \sum\limits_{z\in X_N} q_z = 1; \end{cases} \tag{4}$$

corresponds to the vector of limit probabilities in the ergodic Markov chain determined by the graph $G_s = (X, E_s\cup E_N)$ with the probabilities $p_{x,y}$ for $(x,y)\in E_N$ and $p_{x,y} = s_{x,y}$ for $(x,y)\in E_C$ $(E_C = E\setminus E_N)$. Therefore, for given s the value

$$\psi(s,q^s) = \sum_{x\in X_C}\mu_x q_x + \sum_{z\in X_N}\mu_z q_z,$$

expresses the average cost per transition for the dynamical system if the strategy s is applied, i. e.,

$$f_x(s) = \psi(s,q^s), \quad \forall x\in X.$$

So, if we solve the optimization problem (2), (3) on a perfect network then we find the optimal strategy s^*. □

In the following for an arbitrary vertex $y\in X$ we will denote by $X_C^-(y)$ the set of vertices from X_C which contain directed leaving edges $e = (x,y)\in E$ that end in y, i. e., $X_C^-(y) = \{x\in X_C \,|\, (x,y)\in E\}$; in an analogues way we define the set $X^-(y) = \{x\in X \,|\, (x,y)\in E\}$.

Based on the lemma above we can prove the following result.

Theorem 1. *Let $\alpha^*_{x,y}$ $(x \in X_C,\, y \in X)$, q^*_x $(x \in X)$ be a basic optimal solution of the following linear programming problem:*
Minimize

$$\overline{\psi}(\alpha, q) = \sum_{x \in X_C} \sum_{y \in X(x)} c_{x,y}\alpha_{x,y} + \sum_{z \in X_N} \mu_z q_z \tag{5}$$

subject to

$$\begin{cases} \sum\limits_{x \in X_C^-(y)} \alpha_{x,y} + \sum\limits_{z \in X_N} p_{z,y} q_z = q_y, \quad \forall y \in X; \\ \sum\limits_{x \in X_C} q_x + \sum\limits_{z \in X_N} q_z = 1; \\ \sum\limits_{y \in X(x)} \alpha_{x,y} = q_x, \quad \forall x \in X_C; \\ \alpha_{x,y} \geq 0, \quad \forall x \in X_C,\ y \in X; \quad q_x \geq 0, \quad \forall x \in X. \end{cases} \tag{6}$$

Then the optimal stationary strategy s^* on a perfect network can be found as follows:

$$s^*_{x,y} = \begin{cases} 1 & if \quad \alpha^*_{x,y} > 0; \\ 0 & if \quad \alpha^*_{x,y} = 0, \end{cases}$$

where $x \in X_C$, $y \in X(x)$. Moreover, for every starting state $x \in X$ the optimal average cost per transition is equal to $\overline{\psi}(\alpha^*, q^*)$, i. e.,

$$f_x(s^*) = \sum_{x \in X_C} \sum_{y \in X(x)} c_{x,y}\alpha^*_{x,y} + \sum_{z \in X_N} \mu_z q^*_z$$

for every $x \in X$.

Proof. To prove the theorem it is sufficient to apply Lemma 1 and to show that the bilinear programming problem (2), (3) with boolean variables $s_{x,y}$ for $x \in X_C$, $y \in X$ can be reduced to the linear programming problem (5), (6). Indeed, we observe that the restrictions $s_{x,y} \in \{0, 1\}$ in the problem (2), (3) can be replaced by $s_{x,y} \geq 0$ because the optimal solutions after such a transformation of the problem are not changed. In addition, the restrictions

$$\sum_{y \in X(x)} s_{x,y} = 1, \quad \forall x \in X_C$$

can be changed by the restrictions

$$\sum_{y \in X(x)} s_{x,y} q_x = q_x, \quad \forall x \in X_C,$$

because for the perfect network it holds $q_x > 0, \ \forall x \in X_C$.

Based on the properties mentioned above in the problem (2), (3) we may replace the system (3) by the following system

$$\begin{cases} \sum\limits_{x\in X_C^-(y)} s_{x,y}q_x + \sum\limits_{z\in X_N} p_{z,y}q_z = q_y, \quad \forall y \in X; \\ \sum\limits_{x\in X_C} q_x + \sum\limits_{z\in X_N} q_z = 1; \\ \sum\limits_{y\in X(x)} s_{x,y}q_x = q_x, \quad \forall x \in X_C; \\ s_{x,y} \geq 0, \ \ \forall x \in X_C, \ y \in X; \quad q_x \geq 0, \ \ \forall x \in X. \end{cases} \tag{7}$$

Thus, we may conclude that problem (2), (3) and problem (2), (7) have the same optimal solutions. Taking into account that for the perfect network $q_x > 0, \ \ \forall x \in X$ we can introduce in problem (2), (7) the notations $\alpha_{x,y} = s_{x,y}q_x$ for $x \in X_C$, $y \in X(x)$. This leads to the problem (5), (6). It is evident that $\alpha_{x,y} \neq 0$ if and only if $s_{x,y} = 1$. Therefore, the optimal stationary strategy s^* can be found according to the rule given in the theorem. □

So, if the network (G, X_C, X_N, c, p, x_0) is perfect then we can find the optimal stationary strategy s^* by using the following algorithm.

Algorithm 1. Determining the Optimal Stationary Strategy on Perfect Networks

1) Formulate the linear programming problem (5), (6) and find a basic optimal solution $\alpha^*_{x,y}$ $(x \in X_C, \ y \in X)$, q^*_x $(x \in X)$.

2) Fix a stationary strategy s^* where $s^*_{x,y} = 1$ for $x \in X_C$, $y \in X(x)$ if $\alpha^*_{x,y} > 0$; otherwise put $s^*_{x,y} = 0$.

3 Extension of the Algorithm 1 for Solving the Unichain Control Problem

We show that the algorithm 1 can be extended for the problem in which an arbitrary strategy s generates a Markov unichain. For a unichain control problem the graph G_s induced by a stationary strategy may not be strongly connected, but it contains a unique deadlock strongly connected component that is reachable from every $x \in X$. A basic optimal solution α^*, q^* of the linear programming problem (5), (6) determines the strategy

$$s^*_{x,y} = \begin{cases} 1 & \text{if} \ \ \alpha^*_{x,y} > 0; \\ 0 & \text{if} \ \ \alpha^*_{x,y} = 0, \end{cases}$$

and a subset $X^* = \{x \in X \,|\, q^*_x > 0\}$, where s^* provides the optimal average cost per transition for the dynamical system $\mathbb{L}$ when it starts transitions in the states

$x_0 \in X^*$. This means that for an arbitrary network algorithm 1 determines the optimal stationary strategy of the problem only in the case if the system starts transitions in the states $x \in X^*$.

For a unichain control problem algorithm 1 determines the strategy s^* and the recurrent class X^*. The remaining states $x \in X \setminus X^*$ in X correspond to transient states and the optimal stationary strategies in these states can be chosen in order to reach X^*.

We show how to use the linear programming model (5), (6) for determining the optimal stationary strategies of the control problem on the nonperfect network in which for an arbitrary stationary strategy s the matrix P^s corresponds to a recurrent Markov chain.

An arbitrary strategy s in G generates a graph $G_s = (X, E_s \cup E_N)$ with unique deadlock strongly connected components $G'_s = (X'_s, E'_s)$ that can be reached from any vertex $x \in X$. The optimal stationary strategy s^* in G can be found from a basic optimal solution by fixing $s^*_{x,y} = 1$ for the basic variables. This means that in G we can find the optimal stationary strategy as follows:

We solve the linear programming problem (5), (6) and find a basic optimal solution α^*, q^*. Then we find the subset of vertices $X^* = \{x \in X \,|\, q^*_x > 0\}$ which in G corresponds to a strongly connected subgraph $G^* = (X^*, E^*)$. On this subgraph we determine the optimal solution of the problem using the algorithm 1. It is evident that if $x_0 \in X^*$ then we obtain the solution of the problem with fixed starting state x_0. To determine the solution of the problem for an arbitrary starting state we may select successively vertices $x \in X \setminus X^*$ which contain outgoing directed edges that end in X^* and will add them at each time to X^* using the following rule:

- if $x \in X_C \cap (X \setminus X^*)$ then we fix an directed edge $e = (x, y)$, put $s^*_{x,y} = 1$ and change X^* by $X^* \cup \{x\}$;
- if $x \in X_N \cap (X \setminus X^*)$ then change X^* by $X^* \cup \{x\}$.

4 An Approach for Solving the Multichain Control Problem Using a Reduction Procedure to a Unichain Problem

We consider the multichain control problem on the network (G, X_C, X_N, c, p, x_0), i. e., the case that for different starting states the average cost per transition may be different. We describe an approach for determining the optimal solution which is based on a reduction procedure of the multichain problem to the unichain case.

The graph G satisfies the condition that for an arbitrary vertex $x \in X_C$ each outgoing directed edge $e = (x, y)$ ends in X_N, i. e., we assume that

$$E_C = \{e = (x, y) \in E \,|\, x \in X_C,\ y \in X_N\}.$$

If the graph G does not satisfy this condition then the considered control problem can be reduced to a similar control problem on an auxiliary network $(G', X'_C, X'_N, c', p', x_0)$, where the graph G' satisfies the condition mentioned above. Graph $G' = (X', E')$ is

obtained from $G = (X, E)$, where each directed edge $e = (x, y) \in E_C$ is changed by the following two directed edges $e^1 = (x, x_e)$ and $e^2 = (x_e, y)$.

We include each vertex x_e in X'_N and with each edge $e' = (x_e, y)$ we associate the cost $c'_{x_e,y} = 0$ and the transition probability $p'_{x_e,y} = 1$. With the edges $e' = (x, x_e)$ we associate the cost $c'_{x,x_e} = c_{(x,y)}$, where $e = (x, y)$. For the edges $e \in E_N$ in the new network we preserve the same costs and transition probabilities as in the initial network, i. e., the cost function c' on E_N and on the set of edges (x, x_e) for $x \in X_C,\ e \in E_C$ is induced by the cost function c. Thus, in the auxiliary network the graph G' is determined by the set of vertices $X' = X'_C \cup X'_N$ and the set of edges $E' = E'_C \cup E'_N$, where $X'_C = X_C;\ X'_N = X_N \cup \{x_e,\ e \in E_C\};\ E'_C = \{e' = (x, x_e) \mid x \in X_C,\ e = (x, y) \in E_C\};\ E'_N = E_N \cup \{e' = (x_e, y) \mid\ e = (x, y) \in E_C, y \in X\}$. There exists a bijective mapping between the set of strategies in the states $x \in X_C$ of the network (G, X_C, X_N, c, p, x_0) and the set of strategies in the states $x \in X_C$ of the network $(G', X'_C, X'_N, c', p', x_0)$ that preserves the average costs of the problems on the corresponding networks.

Thus, without loss of generality we may consider that G possesses the property that for an arbitrary vertex $x \in X_C$, each outgoing directed edge $e = (x, y)$ ends in X_N. Additionally, let us assume that the vertex x_0 in G is reachable from every vertex $x \in X_N$. Then an arbitrary strategy s in the considered problem induces a transition probability matrix $P^s = (p^s_{x,y})$ that corresponds to a Markov unichain with a positive recurrent class X^+ that contains the vertex x_0.

Therefore, if we solve the control problem on the network then we obtain the solution of the problem with fixed starting state x_0. So, we obtain such a solution if the network satisfies the condition that for an arbitrary strategy s the vertex x_0 in G_s is attainable for every $x \in X_N$. Now let us assume that this property does not take place. In this case we can reduce our problem to a similar problem on a new auxiliary network $(G'', X''_C, X''_N, p'', c'', x_0)$ for which the property mentioned above holds. This network is obtained from the initial one by the following way: we construct the graph $G'' = (X, E'')$ which is obtained from $G = (X, E)$ by adding new directed edges $e''_{x_0} = (x, x_0)$ from $x \in X_N \setminus \{x_0\}$ to x_0, if for some vertices $x \in X_N \setminus \{x_0\}$ in G there are no directed edges $e = (x, x_0)$ from x to x_0. We define the costs of directed edges $(x, y) \in E''$ in G'' as follows: if $e'' = (x, y) \in E$ then the cost $c''_{e''}$ of this edge in G'' is the same as in G, i. e., $c''_{e''} = c_{e''}$ for $e'' \in E$; if $e'' = (x, x_0) \in E'' \setminus E$ then we put $c''_{e''} = 0$. The probabilities $p''_{x,y}$ for $(x, y) \in E''$ where $x \in X_N$ we define by using the following rule: we fix a small positive value ε and put $p''_{x,y} = p_{x,y} - \varepsilon p_{x,y}$ if $(x, y) \in E'' \setminus E,\quad y \neq x_0$ and in G there is no directed edge $e = (x, x_0)$ from x to x_0; if in G for a vertex $x \in X \setminus \{x_0\}$ there exists a leaving directed edge $e = (x, x_0)$ then for an arbitrary outgoing directed edge $e = (x, y),\ y \in X(x)$ we put $p''_{x,y} = p_{x,y}$; for the directed edges $(x, x_0) \in E' \setminus E$ we put $p''_{x,x_0} = \varepsilon$.

Let us assume that the probabilities $p_{x,y}$ for $(x, y) \in E$ are given in the form of irreducible decimal fractions $p_{x,y} = a_{x,y}/b_{x,y}$.

Additionally, assume that the values ε satisfy the condition

$$\varepsilon \leq 2^{-2L-2},$$

where

$$L = \sum_{(x,y)\in E} \log(a_{x,y}+1) + \sum_{(x,y)\in E} \log(b_{x,y}+1) + \sum_{e\in E}(|c_e|+1) + 2\log(n) + 1.$$

Then, based on the results from [4] for our auxiliary optimization problem (with approximated data) we can conclude that the solution of this problem will correspond to the solution of our initial problem.

So, to find the optimal solution of the problem on the network (G, X_C, X_N, c, p, x_0) it is necessary to construct the auxiliary network $(G', X'_C, X'_N, c', p', x_0)$, where for each vertex $x \in X'_N$ an arbitrary directed edge $e' = (x, y)$ ends in X_N. Then we construct the network $(G'', X''_C, X''_N, c'', p'', x_0)$ and the auxiliary stochastic optimal control problem on this network. If the optimal stationary strategy s'^* in the auxiliary problem is found, then we fix $s^* = s'^*$ on X_C.

References

[1] Bellman R. *Functional equations in the theory of dynamic programming, XI-Limit theorems.* Rand. Circolo Math. Palermo, 1959, **8(3)**, 343–345.

[2] Lozovanu D., Pickl S. *Algorithmic solution of discrete control problems on stochastic networks.* Procceedings of CTW09 Workshop on Graphs and Combinatorial Optimization, Paris, 2009, 221–224.

[3] Puterman M. *Markov Decision Processes: Stochastic Dynamic Programming.* John Wiley, New Jersey, 2005.

[4] Khachian L. G. *Polynomial time algorithm in linear programming.* USSR Computational Mathematics and Mathematical Phisics, 1980, **20**, 51–58.

Dmitrii Lozovanu
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5, Academiei str., Chisinau, MD-2028
Moldova
E-mail: *lozovanu@math.md*

Maria Capcelea
Moldova State University
60, Mateevici str., Chisinau, MD-2009
Moldova
E-mail: *mariacapcelea@yahoo.com*

Received September 10, 2014

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 89–96
ISSN 1024–7696

Near-totally conjugate orthogonal quasigroups

G. B. Belyavskaya, T. V. Popovich

Abstract. The near-totally conjugate orthogonal quasigroups (near-*totCO*-quasigroups), i. e., quasigroups for which there exist five (but there are no six) pairwise orthogonal conjugates, are studied. We consider six types of such quasigroups, connection between them and prove that for any integer $n \geq 7$ which is relatively prime to 2, 3 and 5 there exist near-*totCO*-quasigroups of order n of any type. Three types of conjugate orthogonality graphs, associated with these quasigroups are characterized.

Mathematics subject classification: 20N05, 05B15.
Keywords and phrases: Quasigroup, T-quasigroup, conjugate, parastrophe, conjugate orthogonal quasigroup, Latin square, graph of conjugate orthogonality.

1 Introduction

A quasigroup is an ordered pair (Q, A), where Q is a set and A is a binary operation, defined on Q, such that each of the equations $A(a, y) = b$ and $A(x, a) = b$ is uniquely solvable for any pair of elements a, b in Q. It is known that the multiplication table of a finite quasigroup defines a Latin square and six (not necessarily distinct) conjugates (or parastrophes) are associated with each quasigroup (Q, A) (Latin square): $A = {}^1A$, ${}^rA$, ${}^lA$, ${}^{rl}A$, ${}^{lr}A$, ${}^sA$, which are quasigroups, where ${}^{rl}A = {}^r({}^lA)$ and

$${}^rA(x, y) = z \Leftrightarrow A(x, z) = y, \quad {}^lA(x, y) = z \Leftrightarrow A(z, y) = x, \quad {}^sA(x, y) = A(y, x).$$

Two quasigroups (Q, A) and (Q, B) are orthogonal ($A \perp B$) if the system of equations $\{A(x, y) = a,\ B(x, y) = b\}$ is uniquely solvable for all $a, b \in Q$.

A set $\Sigma = \{A_1, A_2, ..., A_n\}$ of quasigroups, defined on the same set, is orthogonal if any two quasigroups of this set are orthogonal.

The notion of orthogonality plays an important role in the theory of Latin squares, also in quasigroup theory and in distinct applications, in particular, in coding theory and cryptography. In addition, quasigroups that are orthogonal to some of their conjugates or two conjugates of which are orthogonal (known as conjugate orthogonal or parastrophic-orthogonal quasigroups) have a significant interest.

Many articles were devoted to the investigation of various aspects of conjugate orthogonal quasigroups. Recall some of them.

In [4–7, 9, 13], the spectrum of conjugate orthogonal quasigroups (Latin squares) was studied. Different identities associated with such orthogonality and related combinatorial designs were considered in [1, 4, 10].

F. E. Bennett and Hantao Zhang [8] considered a problem related to the spectrum of Latin squares if each conjugate is required to be orthogonal to its transpose (to precisely its transpose among the other five conjugates) Latin square. In the paper [5], in particular, it is shown that for all $n > 5594$, with the possible exception of $n = 6810$, a Latin square with all distinct and pairwise orthogonal conjugates exists. The proof rests on several constructions of pairwise balanced designs of index one. In [6], F. E. Bennett improved this result, proving that such idempotent Latin squares exist for any order $n > 5074$.

In [7, 8, 12], connection between conjugate orthogonal Latin squares and graphs is considered. An orthogonal Latin square graph is one in which the vertices are Latin squares of the same order and on the same symbols, and two vertices are adjacent if and only if the Latin squares are orthogonal. In the article [7], *a graph of conjugate orthogonality* of a Latin square (a finite quasigroup) was considered, i. e., the graph the vertices of which are six conjugates of a Latin square and two vertices are connected if and only if the corresponding pair of conjugates is orthogonal.

The article [2] is devoted to the study of conjugate sets of a quasigroup and of quasigroups all conjugates of which are distinct (DC-quasigroups). In [3], the quasigroups all six conjugates of which form an orthogonal set were investigated.

In this paper we study quasigroups for which there exist five (but there are no six) pairwise orthogonal conjugates. We call such quasigroups near-totally conjugate orthogonal quasigroups (shortly, near-*totCO*-quasigroups), give some information about the spectrum of these quasigroups and characterize graphs, associated with them.

2 Totally and near-totally conjugate-orthogonal quasigroups

It is known that the number of distinct conjugates of a quasigroup can be 1, 2, 3 or 6 (see, for example, [11]).

A quasigroup (Q, A) is called *a totally conjugate-orthogonal quasigroup or a totCO-quasigroup* if all six its conjugates are pairwise orthogonal [3]. In this case the system of six conjugates of a quasigroup is an orthogonal set. Any conjugate of a *totCO*-quasigroup is also a *totCO*-quasigroup.

A quasigroup (Q, A) is called *a T-quasigroup* if there exist an abelian group $(Q, +)$, its automorphisms φ, ψ and an element $a \in Q$ such that $A(x, y) = \varphi x + \psi y + a$.

Let $\sigma \perp \tau$ mean that ${}^{\sigma}A \perp {}^{\tau}A$. It is evident that if $\sigma \perp \tau$, then $s\sigma \perp s\tau$.

The following theorem of [3] gives conditions for the orthogonality of pairs of conjugates for a T-quasigroup.

Theorem 1 [3]. *Let (Q, A) be a finite or infinite T-quasigroup of the form $A(x, y) = \varphi x + \psi y$. Then two its conjugates are orthogonal if and only if the following mappings corresponding to these conjugates:*

$(1 \perp l$ or $s \perp lr) \to \varphi + \varepsilon$, $(r \perp rl) \to \varphi + \varepsilon$ and $\varphi - \varepsilon$,

$(1 \perp r$ or $s \perp rl) \to \psi + \varepsilon$, $(l \perp lr) \to \psi + \varepsilon$ and $\psi - \varepsilon$,

$(1 \perp lr \text{ or } s \perp l) \to \varphi + \psi^2$, $\quad (1 \perp rl \text{ or } s \perp r) \to \varphi^2 + \psi$,
$(r \perp lr \text{ or } rl \perp l) \to \varphi - \psi$, $\quad (1 \perp s) \to \varphi - \psi$ *and* $\varphi + \psi$,
$(l \perp r \text{ or } lr \perp rl) \to \psi\varphi - \varepsilon$ *are permutations.*

In this theorem $(\varphi+\psi) : (\varphi+\psi)x = \varphi x + \psi x$ is an endomorphism of the abelian group of a T-quasigroup, ε is the identity permutation on Q.

Note that conditions of the theorem are valid also for T-quasigroups of the form $A(x, y) = \varphi x + \psi y + a$.

In [1], the following criterion for a *totCO*-T-quasigroup was established.

Theorem 2 [3]. *A T-quasigroup (Q, A): $A(x, y) = \varphi x + \psi y + a$ is a totCO-quasigroup if and only if all the following mappings*

$$\varphi + \varepsilon,\ \varphi - \varepsilon,\ \psi + \varepsilon,\ \psi - \varepsilon,\ \varphi^2 + \psi,\ \psi^2 + \varphi,\ \varphi - \psi,\ \varphi + \psi,\ \psi\varphi - \varepsilon$$

are permutations.

Corollary 1 [3]. *A T-quasigroup (Q, A): $A(x, y) = ax + by \pmod n$ is a totCO-quasigroup if and only if all elements*

$$a + 1,\ a - 1,\ b + 1,\ b - 1,\ a^2 + b,\ b^2 + a,\ a - b,\ a + b,\ ab - 1$$

modulo n are relatively prime to n.

In [1], it was proved that there exist infinite *totCO*-quasigroups. For finite quasigroups it is valid the following

Theorem 3 [3]. *For any $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$, where p_i, $i = 1, 2, ..., s$, are prime numbers not equal to 2, 3, 5 and 7, $k_i \geq 1$, there exists a totCO-quasigroup of order n.*

Consider quasigroups that are not *totCO*-quasigroups and five conjugates of which form an orthogonal set.

Definition 1. *A quasigroup (Q, A) is called near-totally conjugate orthogonal (a near-totCO-quasigroup) if it is not a totCO-quasigroup and there exist five its pairwise orthogonal conjugates.*

In [2], a quasigroup is called a distinct conjugate quasigroup or, shortly, a *DC*-quasigroup, if all its conjugates are distinct. It is evident that *totCO*-quasigroups and near-*totCO*-quasigroups are *DC*-quasigroups.

Let (Q, A) be a *DC*-quasigroup, then there are exactly six different subsets with five conjugates:

$$\Sigma_1 = \{l,\ r,\ rl,\ lr,\ s\},\ \ \Sigma_s = \{1,\ l,\ r,\ lr,\ rl\},\ \ \Sigma_l = \{1,\ r,\ rl,\ lr,\ s\},$$

$$\Sigma_{lr} = \{1,\ l,\ r,\ rl,\ s\},\ \ \Sigma_r = \{1,\ l,\ rl,\ lr,\ s\},\ \ \Sigma_{rl} = \{1,\ l,\ r,\ lr,\ s\}.$$

The index σ of Σ_σ indicates the missing conjugate in a set.

Say that a near-*totCO*-quasigroup (Q, A) has *the conjugate orthogonality type or the CO-type* $\Sigma_1\,(\Sigma_s, \Sigma_l, \Sigma_{lr}, \Sigma_r$ or $\Sigma_{rl})$ if the respective set of conjugates is orthogonal.

The following statement shows that there exist connections between CO-types of a quasigroup.

Proposition 1. *A near-totCO-quasigroup has the CO-type Σ_1 if and only if it has the CO-type Σ_s.*

A near-totCO-quasigroup has the CO-type Σ_l if and only if it has the CO-type Σ_{lr}.

A near-totCO-quasigroup has the CO-type Σ_r if and only if it has the CO-type Σ_{rl}.

Proof. Let the set Σ_1 be orthogonal, then it is easy to see that the set ${}^s\Sigma_1 = \{sl, sr, srl, slr, ss\} = \{lr, rl, l, r, 1\} = \Sigma_s$ is also orthogonal since the commutation of orthogonal operations retains their orthogonality. Analogously we obtain that ${}^s\Sigma_l = \Sigma_{lr}$ and ${}^s\Sigma_r = \Sigma_{rl}$. Note that $s = rlr = lrl$ and $\sigma\sigma = 1$ for any conjugate.

The converse statement is obvious. □

Corollary 2. *If a quasigroup is a near-totCO-quasigroup, then there exists an orthogonal set of five conjugates, containing this quasigroup.*

Indeed, in all cases at least one of two conjugate sets of Proposition 1 contains the initial quasigroup.

Proposition 2. *Any conjugate of a near-totCO-quasigroup is also a near-totCO-quasigroup.*

Proof. Let a near-*totCO*-quasigroup (Q, A) have the CO-type $\Sigma_1(A) = \{l, r, rl, lr, s\}$. Then any conjugate of this set is a near-*totCO*-quasigroup since it is contained in this orthogonal set, and the rest four conjugates can be considered as conjugates of this conjugate. For example, for the conjugate ${}^lA$ we have

$$\Sigma_1({}^lA) = \{l, r = (rl)l, (r)l, lr = (s)l, s = (lr)l\}.$$

Thus ${}^lA$ is included in an orthogonal set of its five conjugates.

Let a near-*totCO*-quasigroup (Q, A) have the CO-type $\Sigma_l = \{1, r, rl, lr, s\}$. As above, prove that the conjugates r, rl, lr, s are near-*totCO*-quasigroups. For the conjugate ${}^lA$ use the CO-type Σ_{lr} which by Proposition 1 is also a CO-type of (Q, A).

Analogously consider the conjugates of the sets Σ_r and Σ_{rl}. □

Theorem 4. *If a quasigroup (Q, A) is not a totCO-quasigroup, then*

– the set Σ_1 (Σ_s) of its conjugates is orthogonal if and only if all pairs of conjugates, except the pair $(1, s)$, are orthogonal;

– the set Σ_l (Σ_{lr}) is orthogonal if and only if all pairs of conjugates, except the pair (l, lr), are orthogonal;

– the set Σ_r (Σ_{rl}) is orthogonal if and only if all pairs of conjugates, except the pair (r, rl), are orthogonal.

Proof. Using Proposition 1 and taking into account the orthogonal pairs of conjugates of Σ_1 and Σ_s (of Σ_l and Σ_{lr}; of Σ_r and Σ_{rl}), we will establish that there are

exactly 14 orthogonal pairs of 15 possible pairs of conjugates and only the pair $(1,\ s)$ (the pair $(l,\ lr)$, the pair $(r,\ rl)$ respectively) is missing.

It is easy to check the converse statement. □

Note that from this theorem it follows that a near-*totCO*-quasigroup can not have CO-types simultaneously from two different pairs of connected CO-types. Otherwise it is a *totCO*-quasigroup.

Corollary 3. *A $T-$quasigroup $(Q,\ A)$: $A(x,\ y) = \varphi x + \psi y + a$ that is not a totCO-quasigroup is a near-totCO-quasigroup*

– of the type Σ_1 (Σ_s) if and only if all mappings of Theorem 2, except the unique mapping $\varphi + \psi$, are permutations;

– of the type Σ_l (Σ_{lr}) if and only if all mappings of Theorem 2, except the unique mapping $\psi - \varepsilon$, are permutations;

– of the type Σ_r (Σ_{rl}) if and only if all mappings of Theorem 2, except the unique mapping $\varphi - \varepsilon$, are permutations.

Proof. Show that the corresponding conditions of Theorem 4 and the corollary for T-quasigroups are equivalent. By Theorem 1, two permutations $\varphi+\varepsilon$, $\varphi-\varepsilon$ correspond to orthogonality of the pair $(1, s)$. But the mapping $\varphi - \varepsilon$ is a permutation since $r \perp lr$. Hence, only the mapping $\varphi + \varepsilon$ is not a permutation. It is easy to see that the converse statement is valid by Theorem 1.

Analogously, using Theorem 1, we obtain the pointed out conditions for the pairs $(l,\ lr)$ and $(r,\ rl)$. □

Corollary 4. *An abelian group is not a near-totCO-quasigroup (a totCO-quasigroup).*

Indeed, an abelian group $(Q, +)$ is a T-quasigroup $A(x, y) = \varphi x + \psi y + a$ with $\varphi = \psi = \varepsilon$, $a = 0$, so for it $\varphi - \varepsilon = \psi - \varepsilon = \varphi - \psi = \varphi\psi - \varepsilon = 0$, where 0 is the zero of the endomorphism ring of the group $(Q, +)$. By Corollary 3 (by Theorem 2) the T-quasigroup is not a near-*totCO*-quasigroup (a *totCO*-quasigroup). □

Corollary 5. *Among T-quasigroups there are not idempotent near-totCO-quasigroups of the CO-type Σ_1 (Σ_s).*

Indeed, if a T-quasigroup $A(x, y) = \varphi x + \psi y + a$ is idempotent, then $A(x, x) = x = \varphi x + \psi x + a = R_a^+(\varphi + \psi)x$, where $R_a^+ x = x + a$, whence the mapping $\varphi + \psi$ is a permutation. □

Proposition 3. *A $T-$quasigroup $(Q,\ A)$: $A(x,\ y) = ax + by \pmod n$ that is not a totCO$-$quasigroup, is a near-totCO-quasigroup*

– of the type Σ_1 (Σ_s) if and only if all mappings of Theorem 2, except the unique mapping $x \to (a + b)x \pmod n$, are permutations;

– of the type Σ_l (Σ_{lr}) if and only if all mappings of Theorem 2, except the unique mapping $x \to (b - 1)x \pmod n$ are permutations;

– of the type Σ_r (Σ_{rl}) if and only if all mappings of Theorem 2, except the unique mapping $x \to (a - 1)x \pmod n$ are permutations.

Indeed, for a quasigroup of such form $(\varphi-\varepsilon)x = (L_a-\varepsilon)x = (a-1)x$; $(\psi-\varepsilon)x = (L_b-\varepsilon)x = (b-1)x$ and $(\varphi+\psi)x = (L_a+L_b)x = (a+b)x$, where $L_a x = ax$. □

Corollary 6. *A $T-$ quasigroup (Q, A) : $A(x, y) = ax + by \pmod n$ is a near-totCO-quasigroup if and only if all numbers of Corollary 1 are relatively prime to n, except the single number of $a-1$, $b-1$ or $a+b$.*

Theorem 5. *For any integer $n \geq 7$ that is prime to 2, 3 and 5 there exists a near-totCO-quasigroup of every of six CO-types.*

Proof. Let $\overline{a}$ be an element a modulo n, (m, n) be the greatest common divisor of m and n. Consider the quasigroup (Q, A): $A(x, y) = x + 3y \pmod n$ (here $(3, n) = 1$). Check the conditions of Proposition 3 for this quasigroup: $(a+1)x = 2x$, $(a-1)x = 0x$, $(b+1)x = 4x$, $(b-1)x = 2x$, $(a^2+b)x = 4x$, $(b^2+a)x = 10x$, $(a-b)x = -2x$, $(a+b)x = 4x$, $(ab-1)x = 2x$ modulo n. Since $n \geq 7$ the mappings $2x$, $4x$, $10x$, $-2x$ are permutations if n is relatively prime to 2, 3 and 5. Note that if $(2, n) = 1$, then $(-2, n) = (n-2, n) = 1$.

Let n be relatively prime to 2, 3 and 5, then $n \neq 10$ and $n < 10$ only for $n = 7$. In this case $\overline{10} = 3$ and $(3, 7) = 1$. If $n > 10$, then $\overline{10} = 10$ and $(10, n) = 1$ as n is relatively prime to 2 and 5. Hence, only the mapping $(a-1)x$ is not a permutation and by Proposition 3, the quasigroup $A(x, y) = x + 3y \pmod n$ is a near-*totCO*-quasigroup of the CO-type Σ_r (Σ_{rl}) for any n, relatively prime to 2, 3 and 5.

Analogously, the quasigroup (Q, B): $B(x, y) = 3x+y \pmod n$, where $(3, n) = 1$ is a quasigroup of the CO-type Σ_l (Σ_{lr}) as only the mapping $(b-1)x = 0x$ is not a permutation.

The quasigroup (Q, C): $C(x, y) = 3x - 3y \pmod n$, where $(3, n) = 1$, is a quasigroup of the CO-type Σ_1 (Σ_s) since $(a+1)x = 4x$, $(a-1)x = 2x$, $(b+1)x = -2x$, $(b-1)x = -4x$, $(a^2+b)x = 6x$, $(b^2+a)x = 12x$, $(a-b)x = 6x$, $(a+b)x = 0x$, $(ab-1)x = -10x$.

Let n be relatively prime to 2, 3 and 5, then $n \neq 12$ and $n < 12$ only for $n = 7, 11$. These numbers are prime, so $(\overline{12}, n) = 1$.

If $n > 12$, then $\overline{12} = 12$ and $(12, n) = 1$ as n is relatively prime to 2 and 3. Thus only the mapping $x \to (a+b)x = 0x$ is not a permutation. By Proposition 3, (Q, C) is a quasigroup of the CO-type Σ_1 (Σ_s). □

Corollary 7. *For any $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$, where p_i is a prime number, $p_i \neq 2, 3, 5$, $k_i \geq 1$, $i = 1, 2, ..., s$, $s \geq 1$, and for any of six CO-types there exists a near-totCO-quasigroup of order n.*

The computer research showed that near-*totCO*-quasigroups of order $n \leq 5$ do not exist among T-quasigroups of the form $A(x, y) = ax + by \pmod n$.

Besides the quasigroup which was used for the proof of Theorem 5, there exist other T-quasigroups with analogous properties.

Proposition 4. *The quasigroups (Q, A), (Q, B), (Q, C) : $A(x, y) = x + cy \pmod n$, $B(x, y) = cx + y \pmod n$, $C(x, y) = cx - cy \pmod n$, $c > 1$, of odd*

order n are near-totCO-quasigroups if and only if the numbers $c-1$, $c+1$, c^2+1 modulo n are relatively prime to n.

Proof. At first note that the element c is relatively prime to n since A, B, C are quasigroups, so $(2c, n) = 1$ and the mapping $2x$ is a permutation in a group of odd order. After that it is easy to check that under these conditions all mappings of Corollary 1, except the mapping $(a-1)x = (1-1)x$ for the quasigroup A (except the mapping $(b-1)x = (1-1)x$ for the quasigroup B and except the mapping $(a+b)x = (c-c)x$ for the quasigroup C), are permutations. So by Corollary 6, these quasigroups are near-*totCO*-quasigroups. Moreover, by Proposition 3, the quasigroups A, B, C have the CO-types Σ_r and Σ_{rl}; Σ_l and Σ_{lr}; Σ_1 and Σ_s respectively.

Conversely, if the quasigroup A (B, C) is a near-*totCO*-quasigroup, then by Proposition 3, for each quasigroup all numbers, pointed out in Proposition 4 are relatively prime to n. □

Example. Consider the quasigroup (Q, A) : $A(x, y) = x + 2y \pmod 7$. For this quasigroup the numbers $c - 1 = 1$, $c + 1 = 3$, $c^2 + 1 = 5$ modulo 7 are relatively prime to 7. By Proposition 4, it is a near-*totCO*-quasigroup of the CO-types Σ_r and Σ_{rl}. Its conjugates (modulo 7) are:

$$A(x, y) = x + 2y,\ {}^{r}A(x, y) = -4x + 4y,\ {}^{l}A(x, y) = x - 2y,$$

$${}^{lr}A(x, y) = -2x + y,\ {}^{rl}A(x, y) = 4x - 4y,\ A^*(x, y) = 2x + y.$$

It is easy to check directly that all pairs of different conjugates, except the pair $({}^{r}A, {}^{rl}A)$, are orthogonal.

In the article [7], *the graph of conjugate orthogonality* of a Latin square (a finite quasigroup) was considered, i. e., the graph the vertices of which are six conjugates of a Latin square and two vertices are connected if and only if the corresponding pair of conjugates is orthogonal. It is evident that the complete graph K_6 of conjugate orthogonality corresponds to a *totCO*-quasigroup.

We call the graph of conjugate orthogonality of a quasigroup *near-complete* if its complement (with respect to the complete graph K_6) contains a single edge. Such graph contains exactly 14 edges.

From Theorem 4 and Corollary 7 the following statements immediately follow for graphs of conjugate orthogonality.

Theorem 6. *A near-totCO-quasigroup of the CO-type Σ_1 (Σ_s) corresponds to the near-complete graph of conjugate orthogonality without the edge $(1, s)$.*

A near-totCO-quasigroup of the CO-type Σ_l (Σ_{lr}) corresponds to the near-complete graph of conjugate orthogonality without the edge (l, lr).

A near-totCO-quasigroup of the CO-type Σ_r (Σ_{rl}) corresponds to the near-complete graph of conjugate orthogonality without the edge (r, rl).

Proposition 5. *For every $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$, where p_i is a prime number, $p_i \neq 2, 3, 5$, $k_i \geq 1$, $i = 1, 2, ..., s$, $s \geq 1$, there exists a Latin square (a quasigroup) of order n, corresponding to a near-complete graph of conjugate orthogonality.*

Recall that two graphs are isomorphic if the vertices of every graph can be numbered such that the vertices in one graph are connected if and only if in the second graph the vertices with the same numbers are neighboring. Isomorphic graphs have the same structure.

It is easy to see that three near-complete graphs corresponding to different CO-types of near-*totCO*-quasigroups are isomorphic.

References

[1] Belousov V. D. *Parastrophic-orthogonal quasigroups*. Quasigroups and Related Systems, 2005, **13**, No. 1, 25–73.

[2] Belyavskaya G. B., Popovich T. V. *Conjugate sets of loops and quasigroups. DC-quasigroups*. Bul. Acad. Ştiinţe Repub. Moldova. Mat., 2012, No. 1(59), 21–32

[3] Belyavskaya G. B., Popovich T. V. *Totally conjugate orthogonal quasigroups and complete graphs*. Journal of Mathematical Sciences, 2012, **185**, No. 2, 184–191.

[4] Bennett F. E. *The spectra of a variety of quasigroups and related combinatorial designs*. Discrete mathematics, 1989, **77**, 29–50.

[5] Bennett F. E. *Latin squares with pairwise orthogonal conjugates*. Discrete mathematics, 1981, **36**, 117–137.

[6] Bennett F. E. *On conjugate orthogonal idempotent Latin squares*. Ars. combinatorica, 1985, **19**, 37–50.

[7] Bennett F. E., Mendelsohn N. S. *Conjugate orthogonal Latin square graphs*. Congressus Numerantium, 1979, **23**, 179–192.

[8] Bennett F. E., Zhang Hantao. *Latin squares with self-orthogonal conjugates*. Discrete mathematics, 2004, **284**, 45–55.

[9] Chaffer R. A., Lieberman D. J., Smith D. D. *The number of orthogonal conjugates of a quasigroup*. Congressus Numerantium, 1982, **35**, 169–180.

[10] Evans T. *Algebraic structures associated with Latin squares and orthogonal arrays*. Proc. Conf. Algebraic Aspects of Combinatorics, Congressus Numerantium, 1975, **13**, 31–52.

[11] Lindner C. C., Steedly D. *On the number of conjugates of a quasigroup*. Algebra Univ., 1975, **5**, 191–196.

[12] Lindner C. C., Mendelsohn E., Mendelsohn N. S., Wolk B. *Orthogonal Latin square graphs*. J. Graph Theory, 1979, **3**, 325–328.

[13] Phelps K. T. *Conjugate orthogonal quasigroups*. J. Combin. Theory (A), 1978, **25**, 117–127.

Received September 11, 2014

G. B. Belyavskaya
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD-2028, Chişinău
Moldova
E-mail: *gbel1@rambler.ru*

T. V. Popovich
A. Russo State University
Balti, Moldova
E-mail: *tanea-popovici@mail.ru*