

ASYMPTOTIC IDENTITY OF μ -PROJECTIONS AND I -PROJECTIONS

MARIÁN GRENDÁR
Dedicated to Mar

ABSTRACT. Concept of μ -projection, closely related to that of constrained mode of multinomial distribution, is introduced. Sets of μ -projections and I -projections are shown to be asymptotically identical.

INTRODUCTION

At [1], a convergence of constrained mode of a multinomial distribution for sample size $n \rightarrow \infty$ to I -projection of q on the constraining set \mathcal{H} , was investigated and illustrated by a numeric examples. There the point-wise convergence was also proven, for \mathcal{H} defined by a differentiable constraint (cf. [1], Thm 1).

Here, a concept of μ -projection, closely related to that of the constrained mode of the multinomial distribution, is introduced. For a general feasible set it is shown here that μ -projections are asymptotically indistinguishable from I -projections.

TERMINOLOGY AND NOTATION

Let $\{X\}_{l=1}^n$ be a sequence of independently and identically distributed random variables with a common law (measure) on a measurable space. Let the measure be concentrated on m atoms from a set $\mathcal{X} \triangleq \{x_1, x_2, \dots, x_m\}$ called support or alphabet. Let q_i denote the probability (measure) of i -th element of \mathcal{X} . Let $\mathcal{P}(\mathcal{X})$ be a set of all probability mass functions (pmf's) on \mathcal{X} .

A type (also called n -type, empirical measure, frequency distribution or occurrence vector) induced by a sequence $\{X\}_{l=1}^n$ is the pmf $\nu^n \in \mathcal{P}(\mathcal{X})$ whose i -th element ν_i^n is defined as: $\nu_i^n \triangleq n_i/n$ where $n_i \triangleq \sum_{l=1}^n I(X_l = x_i)$; there $I(\cdot)$ is the characteristic function. Multiplicity $\Gamma(\nu^n)$ of type ν^n is: $\Gamma(\nu^n) \triangleq n! / \prod_{i=1}^m n_i!$.

Let $\Pi \subseteq \mathcal{P}(\mathcal{X})$. Let \mathcal{P}_n denote a subset of $\mathcal{P}(\mathcal{X})$ which consists of all n -types. Let $\Pi_n \triangleq \Pi \cap \mathcal{P}_n$.

2000 Mathematics Subject Classification. Primary 62B15; Secondary 94A15, 65J20.

Key words and phrases. Information projection, μ -projection, J -projection, Maximum Probability method, Maximum Entropy method, Jeffreys Entropy Maximization method.

Supported by VEGA 1/7295/20 grant. Valuable discussions with Ondrej Šuch are gratefully acknowledged. Anonymous referee is thanked for careful reading and inspiring comments. Lapses are mine.

Received 11. 5. 2004; Accepted 21. 9. 2004

μ -projection $\hat{\nu}^n$ of q on Π_n is defined as: $\hat{\nu}^n \triangleq \arg \sup_{\nu^n \in \Pi_n} \pi(\nu^n; q)$, where $\pi(\nu^n; q) \triangleq \Gamma(\nu^n) \prod (q_i)^{n\nu_i^n}$. Equivalently, for $\Pi_n \neq \emptyset$ μ -projection $\hat{\nu}^n$ of q on Π_n can be defined in terms of supremum of a conditional probability: $\hat{\nu}^n \triangleq \arg \sup_{\nu^n \in \Pi_n} \pi(\nu^n | \nu^n \in \Pi_n; q \mapsto \nu^n)$ where $\pi(\nu^n | \nu^n \in \Pi_n; q \mapsto \nu^n)$ denotes the conditional probability that if q generated an n -type from Π_n then it is just the type ν^n .

I -projection \hat{p} of q on Π is $\hat{p} \triangleq \arg \inf_{p \in \Pi} I(p||q)$, where $I(p||q) \triangleq \sum_{\mathcal{X}} p_i \log \frac{p_i}{q_i}$ where $I(\cdot||\cdot)$ is Kullback-Leibler distance, information divergence or (minus) relative entropy.

ASYMPTOTIC IDENTITY OF μ -PROJECTIONS AND I -PROJECTIONS

Theorem 1. Let \mathcal{X} be a finite set. Let \mathcal{M}_n be set of all μ -projections of q on Π_n . Let \mathcal{I} be set of all I -projections of q on Π . For $n \rightarrow \infty$, $\mathcal{M}_n = \mathcal{I}$.

Proof. Necessary and sufficient conditions for $\hat{\nu}^n$ to be a μ -projection of q on Π_n are: a) $\pi(\hat{\nu}^n; q) \geq \pi(\nu^n; q)$, $\forall \nu^n \in \Pi_n$; b) whenever $\tilde{\nu}^n$ has the property a) then $\pi(\hat{\nu}^n; q) \leq \pi(\tilde{\nu}^n; q)$. The requirement a) can be equivalently stated as:

$$(1) \quad \left(\prod \frac{n_i!}{\hat{n}_i!} \right)^{1/n} \geq \left(\prod q_i^{n_i - \hat{n}_i} \right)^{1/n}$$

and b) similarly. Standard inequality $(n/e)^n < n! < n(n/e)^n$ (valid for $n > 6$) allows to bind the LHS of (1):

$$(2) \quad \frac{\prod (\nu_i^n)^{\nu_i^n}}{n^{m/n} \prod (\hat{\nu}_i^n)^{\hat{\nu}_i^n} (\prod \hat{\nu}_i^n)^{1/n}} < \text{LHS} < \frac{n^{m/n} \prod (\nu_i^n)^{\nu_i^n} (\prod \nu_i^n)^{1/n}}{\prod (\hat{\nu}_i^n)^{\hat{\nu}_i^n}}$$

and similar bounds can be stated in the case of the requirement b)¹. Since m is by assumption finite, as $n \rightarrow \infty$ the upper and lower bounds at (2) collapse into $\prod (\nu_i^n)^{\nu_i^n} / \prod (\hat{\nu}_i^n)^{\hat{\nu}_i^n}$. Consequently, the necessary and sufficient conditions a), b) for μ -projection turn as $n \rightarrow \infty$ into (expressed in an equivalent log-form): i) $\sum (\nu_i^n \log \nu_i^n - \hat{\nu}_i^n \log \hat{\nu}_i^n) \geq \sum (\nu_i^n - \hat{\nu}_i^n) \log q_i$ for all $\nu^n \in \Pi_n$; and ii) whenever $\tilde{\nu}^n$ has the property i) then $\sum \hat{\nu}_i^n \log \hat{\nu}_i^n - \tilde{\nu}_i^n \log \tilde{\nu}_i^n \geq \sum (\hat{\nu}_i^n - \tilde{\nu}_i^n) \log q_i$.

Necessary and sufficient conditions for \hat{p} to be an I -projection of q on Π are: I) $\sum (p_i \log p_i - \hat{p}_i \log \hat{p}_i) \geq \sum (p_i - \hat{p}_i) \log q_i$ for all $p \in \Pi$; and II) whenever \tilde{p} has the property I) then $\sum (\hat{p}_i \log \hat{p}_i - \tilde{p}_i \log \tilde{p}_i) \geq \sum (\hat{p}_i - \tilde{p}_i) \log q_i$.

A comparison of i), ii) and I), II) then completes the proof. \square

Note. Since $\pi(\nu^n; q)$ is defined for $\nu^n \in \mathcal{Q}^m$, μ -projection can be defined for Π_n , when n is finite, only. Theorem 1 makes possible to extend the definition by defining a μ -projection of q on Π as follows: $\hat{\nu} \triangleq \arg \sup_{r \in \Pi} \pi(r; q) = \sum_{\mathcal{X}} r_i \log \frac{r_i}{q_i}$.

Asymptotic identity of γ -projections and J -projections.

γ projection $\hat{\nu}^n$ of $q \in \mathcal{Q}^m$ on Π_n is $\hat{\nu}^n \triangleq \arg \sup_{\nu^n \in \Pi_n} \pi(\nu^n; q) \pi(nq; \nu^n)$.

J -projection (or Jeffreys' projection) \tilde{p} of $q \in \mathcal{Q}^m$ on Π is defined as: $\tilde{p} \triangleq \arg \inf_{p \in \Pi} \sum_{\mathcal{X}} p_i \log \frac{p_i}{q_i} + q_i \log \frac{q_i}{p_i}$.

¹Note that if an i -th component of a type is zero then it does not change value of $\pi(\nu^n; q)$. Thus it is assumed that product operations at (1), (2) are performed on non-zero components only.

Theorem 2. Let $q \in \mathcal{Q}^m$. Let \mathcal{X} be a finite set. Let \mathcal{G}_n be set of all γ -projections of q on Π_n . Let \mathcal{J} be set of all J -projections of q on Π . Let n_0 be denominator of the smallest common divisor of q_1, q_2, \dots, q_m . Let $n = un_0$, $u \in \mathcal{N}$. Let $u \rightarrow \infty$. Then $\mathcal{G}_n = \mathcal{J}$.

Proof. Along the same lines as proof of the Theorem 1.

COMMENTS

1) Theorem 1 which is intended to replace Thm 1 of [1] (a.k.a. MaxProb/MaxEnt Thm) shows that μ -projections are asymptotically indistinguishable from I -projections. In other words, Maximum Probability (MaxProb, cf. [1]) and Relative Entropy Maximization method (REM/MaxEnt) methods, when applied to the Boltzmann-Jaynes inverse problem (cf. [2]), make asymptotically the same choice. However, for finite n , I - and μ -projections on Π_n are in general different. In light of this, the asymptotic identity of I - and μ -projections can be viewed in two ways: either as saying that 1) I -projection is asymptotic form of μ -projection (the view presented at [1]) or that 2) I - and μ -projections asymptotically coincide. If one adopts the second view then for a finite n it is necessary to face a challenge of choosing between I - and μ -projections.

2) μ -projection is related to the probability $\pi(\nu^n; q)$, hence it can be viewed as a 'UNI'-projection. γ -projection is related to $\pi(\nu^n; q) \pi(nq; \nu^n)$, thus it can be viewed as an 'AND'-projection (cf. [5]). It is then natural to consider also an 'OR'-projection defined as $\nu^n \triangleq \arg \sup_{\nu^n \in \Pi_n} \pi(\nu^n; q) + \pi(nq; \nu^n)$. However there seems to be no analytic way how to define its asymptotic form.

3) In the same manner it can be proven that infimum (minimum) probability type(s) $\arg \inf_{\nu^n \in \Pi_n} \pi(\nu^n; q)$ is asymptotically identical with infimum (minimum) relative entropy distribution(s) $\arg \inf_{p \in \Pi} - \sum p_i \log(p_i/q_i)$.

4) Conditioned Weak Law of Large Numbers (CWLLN, [3]) and Gibbs Conditioning Principle (GCP, [4]) which provide for a convex, closed set Π a probabilistic justification of REM thus thanks to the Theorem 1 justify under that conditions MaxProb, as well.

5) CWLLN and GCP hold when (among other things) the I -projection is unique. An extension of CWLLN to the case of multiple I -projections was explored at [6]. A proof of Conditional Equi-concentration of Types on I -projections (ICET) - which sharpens the Asymptotic Equiprobability of I -projections (cf. [6]) - will be given elsewhere [7]. Theorem 1 of the present paper makes possible to state directly also a Conditional Equi-concentration of Types on μ -projections.

REFERENCES

1. Grendár, M., Jr. and Grendár, M., *What is the question that MaxEnt answers? A probabilistic interpretation*, Bayesian inference and Maximum Entropy methods in Science and Engineering (A. Mohammad-Djafari, ed.), AIP, Melville, NY, 2001, pp. 83-94.
2. ———, *Maximum Entropy method with non-linear moment constraints: challenges*, Bayesian inference and Maximum Entropy methods in Science and Engineering (G. Erickson and Y. Zhai, eds.), AIP, Melville, NY, 2004, pp. 97-109.
3. Cover, T. and Thomas, J., *Elements of Information Theory*, Wiley, NY, 1991.
4. Dembo, A. and Zeitouni, O., *Large Deviations Techniques and Applications*, Springer, NY, 1998.
5. Grendár, M., Jr. and Grendár, M., *On the probabilistic rationale of I -divergence and J -divergence minimization*, arxiv/math.PR/0008037, 2000.

6. ———, *Asymptotic Equiprobability of I-projections*, Acta Univ. M. Belii **10** (2003), 3-8.
7. Grendár, M., *Conditional Equi-concentration of Types*, Focus on Probability Theory, NSP, NY, 2004 in print.

INSTITUTE OF MATHEMATICS AND CS (OF SLOVAK ACADEMY OF SCIENCES (SAS) AND OF MATEJ BEL UNIVERSITY); SEVERNÁ 5; SK-974 01 BANSKÁ BYSTRICA; SLOVAKIA

INSTITUTE OF MEASUREMENT SCIENCE OF SAS; DÚBRAVSKÁ CESTA 9; SK-841 04 BRATISLAVA; SLOVAKIA

E-mail: marian.grendar@savba.sk

ECCENTRIC SEQUENCES AND CYCLES IN GRAPHS

ALFONZ HAVIAR, PAVEL HRNČIAR AND GABRIELA MONOSZOVÁ

ABSTRACT. An eccentric sequence is called minimal if it has no proper eccentric subsequence with the same number of distinct eccentricities. A graph is said to be a minimal graph if it realizes a minimal eccentric sequence. Some minimal graphs and some minimal eccentric sequences are described. It is shown that a graph with radius r , diameter $d \leq 2r - 2$ and with at most $3r - 2$ vertices contains a cycle of length $2r$ or $2r + 1$.

1. INTRODUCTION

The eccentricity of a vertex v of a connected graph is the distance between v and a vertex furthest from v . To any finite connected graph G one can assign the sequence of the eccentricities of its vertices, called the eccentric sequence of G . To decide whether a sequence of positive integers is the eccentric sequence of some graph is a difficult task. Only very few results are known in this direction (see [1] and the recent survey [2]). L. Lesniak showed that a sequence S of positive integers is the eccentric sequence of some graph if and only if some subsequence S' of S with the same number of distinct values is eccentric. This result naturally leads to the concept of minimal eccentric sequences. Throughout the paper, any graph which realizes a minimal eccentric sequence is said to be a minimal graph.

In the paper we describe large classes of minimal unicyclic graphs with an even cycle (see Theorem 3.1) and with an odd cycle (see Theorem 3.2). From this we obtain an explicit description of minimal eccentric sequences with two distinct values and with length at most $\lfloor \frac{8r+5}{3} \rfloor$ (see Theorem 3.4). The key result of the present paper is our Theorem 2.6, which asserts that a graph with radius r , diameter $d \leq 2r - 2$ and with at most $3r - 2$ vertices contains a cycle of length $2r$ or $2r + 1$. In fact, it significantly reduces the number of possibilities which one needs to consider to prove Theorems 3.1 and 3.2.

We are going to recall terminology and fix notations. We consider undirected connected finite graphs without loops and multiple edges. We will use standard notations of the graph theory (see for example [4]). We recall some of them. We

2000 *Mathematics Subject Classification.* 05C12.

Key words and phrases. radius, cycle, circumference, eccentricity, eccentric sequence, minimal graph.

The authors were supported by the Slovak grant agency, grant number 2/2060/22 and by grant APVT-51-012502

Received 4. 5. 2004; Accepted 21. 9. 2004

denote by $V(G)$ the vertex set and by $E(G)$ the set of edges of a graph G . The symbol $|V(G)|$ is used for cardinality of $V(G)$. Let $u, v \in V(G)$, by a $u - v$ path we mean the finite alternating sequence $u = u_0, e_1, u_1, e_2, \dots, u_{k-1}, e_k, u_k = v$ of vertices and edges beginning with vertex u and ending with vertex v such that $e_i = u_{i-1}u_i$ for $i = 1, 2, \dots, k$, in which no vertex is repeated. It is also denoted by $P_k = (u_0, u_1, u_2, \dots, u_k)$; the number k is its *length*. If $P_{n-1} = (u_1, u_2, \dots, u_n)$ is a path and $u_n u_1 \in E(G)$ then $C_n = (u_1, u_2, \dots, u_n, u_1)$ is a cycle of length n (throughout the paper, C_n will always denote a cycle of length n). The subgraph of a graph G induced by the edges of a path or a cycle is also referred to as a path or a cycle of G . The *distance* $d(u, v)$ between two vertices u and v is the minimum of the lengths of the $u - v$ paths of G . A shortest $u - v$ path is called a $u - v$ *geodesic path*. We denote by $d_{G'}(u, v)$ the distance between vertices $u, v \in V(G')$ in the subgraph G' of the graph G . The distance between a vertex $u \in V(G)$ and a subgraph G' of a graph G will be denoted by $d_G(u, G')$, i.e. $d_G(u, G') = \min\{d_G(u, x); x \in V(G')\}$.

Denote the degree of a vertex $u \in V(G)$ by $\deg_G(u)$ and the eccentricity of a vertex $u \in V(G)$ by $e_G(u)$. Recall that

$$e_G(u) = \max\{d_G(u, v); v \in V(G)\}.$$

We denote it briefly by $e(u)$ when no confusion can arise. We will use the symbol $\text{rad } G$ to denote the radius of the graph G (i.e. the minimum of eccentricities of vertices of the graph G). The symbol $\text{diam } G$ is used for the diameter of the graph G (i.e. the maximum of eccentricities of its vertices). We write simply r and d when there is no confusion.

The eccentric sequence of a graph G is a list of the eccentricities of its vertices in nondecreasing order. Since often there are some vertices having the same eccentricity we will denote it simply

$$e(G) = (e_1^{m_1}, e_2^{m_2}, \dots, e_k^{m_k}) = (e_i^{m_i})_{i=1}^k$$

where e_i are eccentricities for which $e_i < e_{i+1}$ and m_i is the multiplicity of e_i . A sequence of positive integers is called eccentric if there is a graph which realizes the considered sequence. By Lesniak [5] the following statement holds.

Theorem 1.1. *A nondecreasing sequence $(e_1^{m_1}, e_2^{m_2}, \dots, e_k^{m_k})$ is eccentric if and only if some of its subsequences with k distinct values is eccentric.*

An eccentric sequence is called minimal (by R. Nandakumar, see [1]) if it has no proper eccentric subsequence with the same number of distinct eccentricities. A graph is said to be a minimal graph if it realizes a minimal eccentric sequence.

Let $e(G_1) = (e_1^{m_1}, e_2^{m_2}, \dots, e_k^{m_k})$ and $e(G_2) = (e_1^{n_1}, e_2^{n_2}, \dots, e_k^{n_k})$ be eccentric sequences of graphs G_1 and G_2 . We write $e(G_1) \leq e(G_2)$ if $1 \leq m_i \leq n_i$ for each $i \in \{1, \dots, k\}$. We write $e(G_1) < e(G_2)$ if $e(G_1) \leq e(G_2)$ and moreover there is $i \in \{1, \dots, k\}$ for which $m_i < n_i$. If $e(G_1) < e(G_2)$ then it is obvious that $|V(G_1)| < |V(G_2)|$.

Definition 1.2. A graph G is said to be a *sun-graph* if it is unicyclic (i.e. it has exactly one cycle C), $\deg_G(u) \leq 3$ for $u \in V(C)$ and $\deg_G(u) \leq 2$ for $u \in V(G) - V(C)$. The mentioned cycle C is called the *kernel* of the sun-graph G .

Definition 1.3. Let G be a sun-graph with the kernel C . A $u - v$ path in the graph G is said to be a *ray* of the graph G if $\deg_G(u) = 1$ and v is the only vertex of the path belonging to $V(C)$. If G is a sun-graph with n rays we briefly say that G is an n -rays sun-graph.

In Figure 1.1 it is depicted a 4-rays sun-graph.

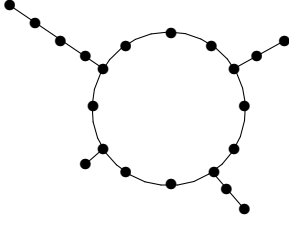


Fig. 1.1

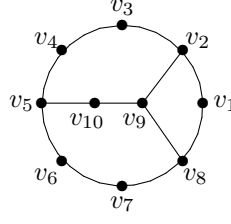


Fig. 1.2

Definition 1.4. A cycle C in a graph G is called a *geodesic cycle* if for each two vertices x, y of the cycle C it holds $d_C(x, y) = d_G(x, y)$.

In Figure 1.2 the cycle $(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_1)$ is a geodesic cycle and $(v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_2)$ is not a geodesic cycle.

Definition 1.5. Let C be a cycle of a graph G and let its length be $2k$ or $2k + 1$. A vertex of the cycle C is said to be *C -excited* (in the graph G) if its eccentricity is larger than k . The number of the C -excited vertices of G will be denoted by $\text{exc}_G(C)$.

Lemma 1.6. Let C be a cycle of a graph G and $|V(G)| - |V(C)| = m$. Then

- a) $\text{exc}_G(C) \leq 2m - 1$ if length of the cycle C is even and $m \geq 1$,
- b) $\text{exc}_G(C) \leq 2m$ if length of the cycle C is odd,
- c) $\text{exc}_G(C) \leq 2m - n$ if C is an even cycle and there are at least n vertices from $V(G) - V(C)$ such that each of them is adjacent to at least one vertex of the cycle C .

Proof. a) Consider a sequence $G_0 = C, G_1, \dots, G_m$ of subgraphs of the graph G such that the subgraph G_{i+1} is obtained from the subgraph G_i (for $i < m$) by adding some vertex $u \in V(G) - V(G_i)$ and some edge $uv \in E(G)$ where $v \in V(G_i)$ (see Figure 1.3). Obviously, $\text{exc}_{G_1}(C) = 1$ and $\text{exc}_{G_{i+1}}(C) \leq \text{exc}_{G_i}(C) + 2$. Therefore the graph G_m contains at most $2m - 1$ C -excited vertices. Since $V(G) = V(G_m)$ and $E(G_m) \subset E(G)$ we get $\text{exc}_G(C) \leq \text{exc}_{G_m}(C)$.

b) In this case $\text{exc}_{G_1}(C) = 2$ and we can prove the statement analogously as in the case a).

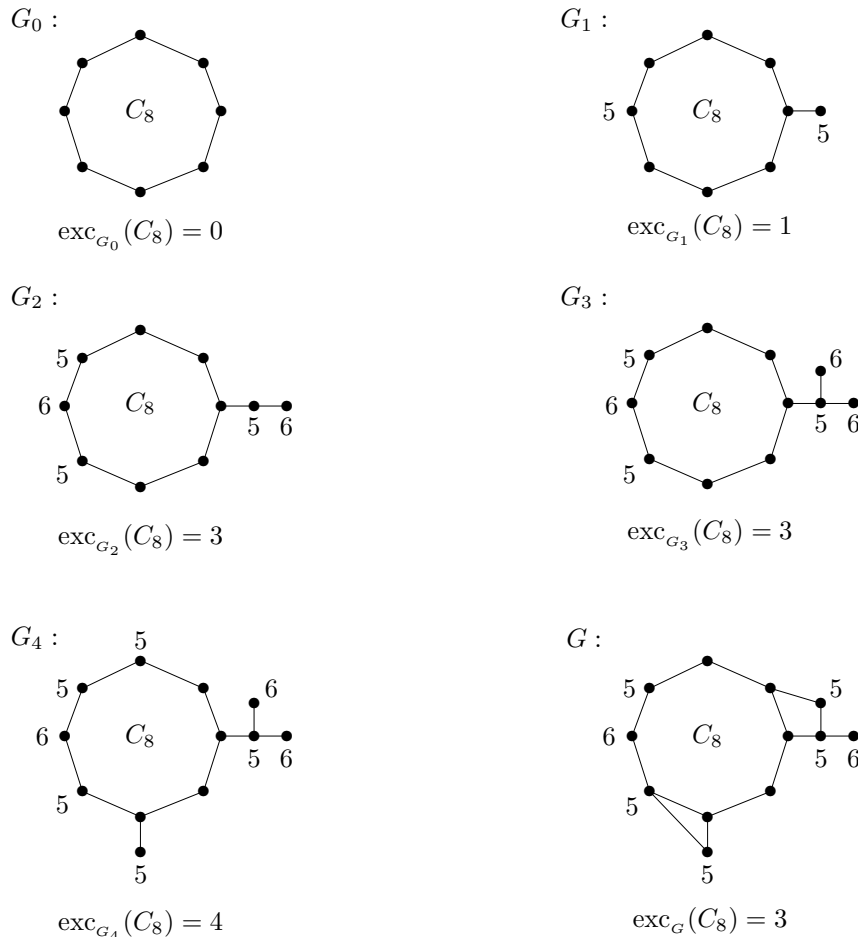


Fig. 1.3

c) The required sequence can be chosen in such a way that each vertex from $V(G_n) - V(C)$ is adjacent to a vertex of the cycle C . In this case $\text{exc}_{G_n}(C) \leq n$ and then obviously $\text{exc}_G(C) \leq 2m - n$. \square

The following statement can be proved analogously to Lemma 1.6.

Lemma 1.7. *Let G_1 be a unicyclic subgraph of G with the cycle C . If $A = \{v \in V(C); e_{G_1}(v) < \text{rad } G\}$ then $|V(G)| - |V(G_1)| \geq \left\lceil \frac{|A|}{2} \right\rceil$ ($\lceil x \rceil$ is the least integer $i \geq x$).*

2. ON CYCLES IN GRAPHS.

In this section we show that a graph G with radius r and diameter d , for which $d \leq 2r - 2$ and $|V(G)| \leq 3r - 2$, contains a cycle C_{2r} or C_{2r+1} . The statement is a consequence of the following three lemmas.

Lemma 2.1. *Let G be a graph with radius r and let G contain the subgraph G_1 depicted in Fig. 2.1. If $m + n + 2 \geq 2r$, $m + k + 2 < 2r$ and $n + k + 2 < 2r$ ($k = 0$ is possible and $uv \in E(G_1)$ in this case) then*

$$|V(G)| > 2r - 1 + \frac{m + n}{2}.$$

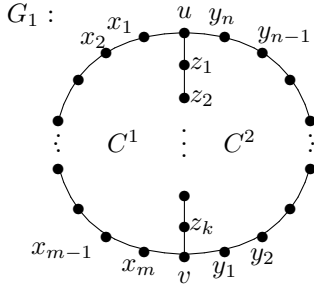


Fig. 2.1

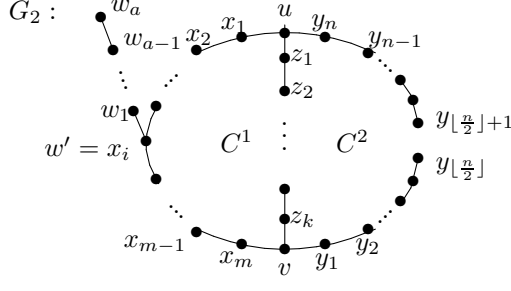


Fig. 2.2

Proof. Since $e_G(u) \geq r$ there is a vertex $w \in V(G)$ such that $d_G(u, w) \geq r$ and it is clear that $w \notin V(G_1)$. Let P be a $u - w$ geodesic path. Let w' be the last vertex of P such that $w' \in V(G_1)$. Without loss of generality we can assume that $w' \in \{u, v, x_1, \dots, x_m, z_1, \dots, z_k\}$. Let $P = (u, \dots, w', w_1, w_2, \dots, w_j)$ where $w_j = w$.

Let $r_1 = \lfloor \frac{m+k+2}{2} \rfloor$. By the assumption $m+k+2 < 2r$ and therefore the number $a = r - 1 - r_1$ is nonnegative and obviously $a \leq j$.

Consider a subgraph G_2 of the graph G (see Figure 2.2) for which

$$V(G_2) = V(G_1) \cup \{w_1, w_2, \dots, w_a\}$$

$$E(G_2) = E(G_1) \cup \{w'w_1, w_1w_2, \dots, w_{a-1}w_a\} - \{y_{\lfloor \frac{n}{2} \rfloor} y_{\lfloor \frac{n}{2} \rfloor + 1}\} \text{ if } a > 0.$$

If $a = 0$ then $V(G_2) = V(G_1)$ and $E(G_2) = E(G_1) - \{y_{\lfloor \frac{n}{2} \rfloor} y_{\lfloor \frac{n}{2} \rfloor + 1}\}$ (we put $y_0 = v$ if $n = 1$). Now consider the cycle $C^1 = (u, x_1, \dots, x_m, v, z_k, \dots, z_1, u)$. If $x \in V(C^1)$ then $d_{G_2}(w_i, x) \leq a + r_1 = r - 1$ for $i = 1, 2, \dots, a$. Therefore $e_{G_2}(x) \geq r$ for $x \in V(C^1)$ if and only if $d_{G_2}(x, y_{\lfloor \frac{n}{2} \rfloor}) \geq r$ or $d_{G_2}(x, y_{\lfloor \frac{n}{2} \rfloor + 1}) \geq r$.

Let $A = \{x \in V(C^1); e_{G_2}(x) < r\}$. We show that $|A| = 2r - n - k - 2$. Consider two cases.

a) $\lfloor \frac{n}{2} \rfloor + k + 1 \geq r$

In this case $k > 0$ and since $m + n + 1 \geq 2r - 1$ we get $A \subseteq \{z_1, \dots, z_k\}$. Let $A_1 = \{x \in A; d_{G_2}(x, y_{\lfloor \frac{n}{2} \rfloor + 1}) < r\}$ and $A_2 = \{x \in A; d_{G_2}(x, y_{\lfloor \frac{n}{2} \rfloor}) < r\}$. Then $|A| = |A_1 \cap A_2| = |A_1| + |A_2| - |A_1 \cup A_2| = (r - (n + 1 - \lfloor \frac{n}{2} \rfloor)) + (r - (\lfloor \frac{n}{2} \rfloor + 1)) - k$ and so we have $|A| = 2r - n - k - 2$.

b) $\lfloor \frac{n}{2} \rfloor + k + 1 < r$

In this case $\{z_1, z_2, \dots, z_k\} \subseteq A$ and we get

$$|A| = k + (r - (k + n + 1 - \lfloor \frac{n}{2} \rfloor)) + (r - (k + 1 + \lfloor \frac{n}{2} \rfloor)) = 2r - n - k - 2.$$

Since the eccentricity of each vertex of G is at least r , by Lemma 1.7 we have $|V(G)| - |V(G_2)| \geq \lceil \frac{|A|}{2} \rceil$. It follows that

$$\begin{aligned} |V(G)| &\geq m + n + k + 2 + a + \left\lceil \frac{|A|}{2} \right\rceil \\ &= m + n + k + 2 + r - 1 - \left\lfloor \frac{m + k + 2}{2} \right\rfloor + \left\lceil \frac{2r - n - k - 2}{2} \right\rceil \\ &\geq m + n + k + 2 + r - 1 - \frac{m + k + 2}{2} + \frac{2r - n - k - 2}{2} \\ &= 2r - 1 + \frac{m + n}{2}. \end{aligned}$$

It is clear that the equality does not hold if at least one from the integers $m + k$ and $n + k$ is odd. In the opposite case the lengths of the cycles C^1 and C^2 (see Figure 2.1) are even and $|A|$ is also an even integer. It is easy to see that in this case $|V(G)| - |V(G_2)| > \frac{|A|}{2} = \left\lceil \frac{|A|}{2} \right\rceil$. It implies $|V(G)| > 2r - 1 + \frac{m+n}{2}$ and the proof is complete. \square

Corollary 2.2. *Let a graph G contain a subgraph isomorphic to the graph in Fig. 2.1 and $\text{rad } G = r$. If $m + n + 2 \geq 2r$, $m + k + 2 < 2r$ and $n + k + 2 < 2r$ then $|V(G)| \geq 3r - 1$.*

Proof. Since $m + n \geq 2r - 2$, by Lemma 2.1 we get $|V(G)| > 2r - 1 + \frac{m+n}{2} \geq 2r - 1 + \frac{2r-2}{2} = 3r - 2$. \square

Remark. The graph G in Figure 2.3 satisfies the assumption of Corollary 2.2 ($m = n = 2$, $k = 0$, $r = 3$) and $|V(G)| = 3r - 1$.

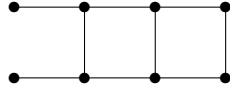


Fig. 2.3

Lemma 2.3. *Let G be a graph with radius r which contains a geodesic cycle C_m . If $m \geq 2r + 2$ then $|V(G)| \geq \frac{3m-4}{2}$.*

Proof. Let $u \in V(G)$ be a vertex with eccentricity $e(u) = r$. Since the eccentricity of each vertex of C_m is at least $r + 1$ it follows that $u \notin V(C_m)$. Denote by G' the component of the graph $G - C_m$ containing the vertex u .

We distinguish two cases.

- a) Each path of the cycle C_m having the length $\lceil \frac{m}{2} \rceil - 2$ contains a vertex adjacent to a vertex of G' .

In this case there exist vertices $w_1, w_2, w_3 \in V(C_m)$ and (not necessarily distinct) vertices $w'_1, w'_2, w'_3 \in V(G')$ satisfying

- (i) $w_1 w'_1, w_2 w'_2, w_3 w'_3 \in E(G)$,
- (ii) $d_{C_m}(w_1, w_2) + d_{C_m}(w_2, w_3) + d_{C_m}(w_3, w_1) = m$.

Let P^1 be a $w'_1 - w'_2$ geodesic path in G' . Let v be a vertex of the path P^1 such that $d_{G'}(w'_3, v) = d_{G'}(w'_3, P^1)$.

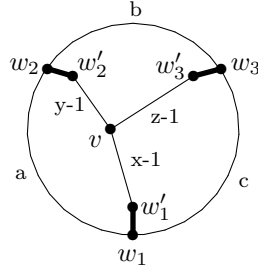


Fig. 2.4

Denote $a = d_G(w_1, w_2) = d_{C_m}(w_1, w_2)$, $b = d_G(w_2, w_3) = d_{C_m}(w_2, w_3)$,
 $c = d_G(w_1, w_3) = d_{C_m}(w_1, w_3)$, $x = d_{G'}(v, w'_1) + 1$,
 $y = d_{G'}(v, w'_2) + 1$, $z = d_{G'}(v, w'_3) + 1$ (see schematic Figure 2.4).

Since C_m is a geodesic cycle we get

$$a \leq x + y, \quad b \leq y + z, \quad c \leq x + z.$$

Hence,

$$x + y + z \geq \frac{a+b+c}{2} = \frac{m}{2}. \text{ It implies}$$

$$|V(G)| \geq a + b + c + x + y + z - 2 \geq m + \frac{m}{2} - 2 = \frac{3m-4}{2}.$$

b) There exists a path A of C_m satisfying the following two conditions

- (j) the length of A is at least $\lceil \frac{m}{2} \rceil - 2$,
- (jj) no vertex of A is adjacent to a vertex of G' .

We are going to show that this assumption yields a contradiction. In this case there exists a path of C_m of length at most $m - (\lceil \frac{m}{2} \rceil - 2) - 2 = \lfloor \frac{m}{2} \rfloor$ containing every vertex $v \in V(C_m)$ adjacent to at least one vertex of G' . Therefore there is a path (v_1, v_2, \dots, v_k) of C_m satisfying the following three conditions

- (k) $0 \leq k - 1 \leq \lfloor \frac{m}{2} \rfloor$,
- (kk) the vertex v_1 is adjacent to a vertex from $V(G')$ and the vertex v_k is also adjacent to a vertex from $V(G')$,
- (kkk) no vertex $v \in V(C_m) - \{v_1, v_2, \dots, v_k\}$ is adjacent to a vertex from $V(G')$.

Denote by P^1 a $u - v_1$ geodesic path and by P^2 a $u - v_k$ geodesic path in the subgraph of G induced by the set $V(C_m) \cup V(G')$. Note that P^1 and P^2 are also geodesic paths in G . Let v_i be the first vertex of P^1 belonging to C_m and v_j be the first vertex of P^2 belonging to C_m . Since C_m is a geodesic cycle it is easy to see that $i \leq j$ and we can assume that $P^1 = (u, \dots, v_i, v_{i-1}, v_{i-2}, \dots, v_1)$ and $P^2 = (u, \dots, v_j, v_{j+1}, v_{j+2}, \dots, v_k)$. Let u_1 be the last vertex of P^1 belonging to P^2 . Since C_m is a geodesic cycle there exists (if $d_G(v_i, v_j) < \lfloor \frac{m}{2} \rfloor$; the case $d_G(v_i, v_j) = \lfloor \frac{m}{2} \rfloor = d_G(v_1, v_k)$ is obvious) a vertex $v_p \in V(C_m)$ such that the following three conditions are satisfied (see schematic Figure 2.5)

$$i \leq p \leq j, \quad d_G(v_i, v_p) \leq d_G(v_i, u_1), \quad d_G(v_j, v_p) \leq d_G(v_j, u_1).$$

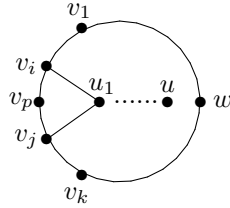


Fig. 2.5

Further, there exists a vertex $w \in C_m$, $w \notin \{v_1, v_2, \dots, v_k\}$ such that $d_G(w, v_p) > r$. Obviously, every $u - w$ path contains at least one vertex from the set $\{v_1, v_2, \dots, v_k\}$. Since C_m is a geodesic cycle, due to symmetry we may without loss of generality assume that some $u - w$ geodesic path in G contains the vertex v_1 . Thus we get

$$\begin{aligned} d(u, w) &= d(u, u_1) + d(u_1, v_i) + d(v_i, w) \geq d(u, u_1) + d(v_p, v_i) + d(v_i, w) \\ &\geq d(u, u_1) + d(v_p, w) \geq d(v_p, w) > r. \end{aligned}$$

A contradiction with the assumption $e(u) = r$.

□

Corollary 2.4. *Let G be a graph with radius r which contains a geodesic cycle C_m . If $m \geq 2r + 2$ then $|V(G)| \geq 3r + 1$.*

Proof. Since $m \geq 2r + 2$, by Lemma 2.3 we get $|V(G)| \geq \frac{3m-4}{4} \geq \frac{3(2r+2)-4}{2} = 3r + 1$. \square

Remark. The graph in Fig. 1.2 contains a geodesic cycle of length $2r + 2$ and $|V(G)| = 3r + 1$ ($r = 3$).

Lemma 2.5. *If a graph G satisfies the following conditions*

- (i) $\text{rad } G = r$,
- (ii) $\text{diam } G \leq 2r - 2$,
- (iii) $|V(G)| \leq 3r - 2$

then the circumference of G (i.e. the length of any longest cycle of G) is at least $2r$.

Proof. Suppose on the contrary that the length of a longest cycle C_m of the graph G is $m < 2r$.

Let G^+ be the block (i.e. maximal 2-connected subgraph) of G containing the cycle C_m . Consider a vertex v_1 such that $d(v_1, G^+) = \max\{d(v, G^+); v \in V(G)\}$. Since $\text{rad } G = r$, $m < 2r$ and G^+ is a 2-connected graph we get $d_G(v_1, G^+) > 0$, i.e. $v_1 \notin V(G^+)$. Let $v'_1 \in V(G^+)$ be a vertex for which $d(v_1, v'_1) = d(v_1, G^+)$. Since G^+ is the block of G , the vertex v'_1 is a cut-vertex of the graph G . Denote by G'_1 the component of the graph $G - v'_1$ containing the vertex v_1 and let $G_1 = \langle V(G'_1) \cup \{v'_1\} \rangle$, i.e. G_1 is the subgraph of G induced by the set $V(G'_1) \cup \{v'_1\}$. Consider a vertex v_2 such that $d(v_2, G^+) = \max\{d(v, G^+); v \in V(G) - V(G_1)\}$. If $d(v_1, v'_1) \leq r - 1$ then $d(v_2, G^+) > 0$ (otherwise $e_G(v'_1) < r$). Denote by v'_2 a vertex of G^+ for which $d(v_2, v'_2) = d(v_2, G^+)$. The vertex v'_2 is a cut-vertex of G . Let P^1 be a $v_1 - v'_1$ geodesic path and P^2 be a $v_2 - v'_2$ geodesic path. Now we distinguish two cases.

- a) $d(v_1, v'_1) \leq r - 1$

Since $d(v_1, v_2) \leq 2r - 2$ and $d(v_1, G^+) \geq d(v_2, G^+)$ there is a vertex $u \in V(G^+)$ such that $d(v_1, u) \leq r - 1$ and $d(v_2, u) \leq r - 1$. We are going to show that $e_G(u) \leq r - 1$ and this contradicts our assumption.

We show that $d(u, w) \leq r - 1$ for every vertex $w \in V(G)$. Clearly, if $w \in V(G^+)$ then $d(w, u) < r$. So, let $w \in V(G) - V(G^+)$ and P be a $w - u$ geodesic path. If $v'_1 \in V(P)$ or $v'_2 \in V(P)$ then $d(w, u) \leq \max\{d(u, v_1), d(u, v_2)\} \leq r - 1$. Assume that P contains neither the vertex v'_1 nor the vertex v'_2 . Denote by w' the first vertex of the path P belonging to the graph G^+ . Denote $a = d(w, w')$. Since $m < 2r$ there exists a positive integer k such that $m = 2r - 2k$ (if m is even) or $m = 2r - 2k + 1$ (if m is odd). The vertices u and w' belong to the block G^+ which contains the longest cycle C_m , hence $d(u, w') \leq r - k$. If $a \leq k - 1$ then $d(u, w) \leq (r - k) + (k - 1) = r - 1$. We will show that $a \geq k$ is impossible since it contradicts our assumption (iii). If $a \geq k$ then obviously there is a unicycle subgraph H of G containing the cycle C_m and k vertices from each of the paths P^1, P^2, P such that either at most 3 vertices of C_m have eccentricities at least r (if $m = 2r - 2k$) or at most 6 vertices of C_m have eccentricities at least r (if $m = 2r - 2k + 1$). Then by Lemma 1.7 we get $|V(G)| \geq 3r - 1$. Really, if $m = 2r - 2k$ then

$|V(G)| \geq (2r - 2k) + 3k + \lceil \frac{2r-2k-3}{2} \rceil = 2r + k + r - k - 1 = 3r - 1$, and
if $m = 2r - 2k + 1$ then

$|V(G)| \geq (2r - 2k + 1) + 3k + \lceil \frac{(2r-2k+1)-6}{2} \rceil = 2r + k + 1 + r - k - 2 = 3r - 1$.

b) $d(v_1, v'_1) \geq r$

Let u be the vertex of the path P^1 such that $d(u, v_1) = r - 1$. If $w \in V(G) - V(G_1)$ then $d(u, w) \leq r - 1$ ($\text{diam } G \leq 2r - 2$ and v'_1 is a cut-vertex of the graph G). If for each vertex $w \in V(G_1)$ it holds $d(u, w) \leq r - 1$ then $e_G(u) \leq r - 1$, a contradiction. Let $w \in V(G_1)$ be such that $d(u, w) \geq r$. Since $d(w, v_1) \leq 2r - 2$ and $d(w, v'_1) \leq d(v_1, v'_1)$ then there is a cycle C' of G such that $u \in V(C')$. Let G' be the block of the graph G containing the cycle C' . Let v_0 be a vertex of the graph G such that $d(v_0, G') = \max\{d(x, G'); x \in V(G)\}$. Let $v'_0 \in V(G')$ be a vertex such that $d(v_0, v'_0) = d(v_0, G')$. Then v'_0 is a cut-vertex of the graph G . If $d(v_0, v'_0) \leq r - 1$ then similarly as in the case a) (take the block G' instead of the block G^+) one can find a vertex with eccentricity less than r in the graph G , which is impossible. Consider now the case $d(v_0, v'_0) \geq r$. Let P' be a $v_0 - v'_0$ geodesic path and u' be the vertex of the path P' such that $d(v_0, u') = r - 1$. For every vertex z from any component of the graph $G - v'_0$ such that the vertex v_0 does not belong to this component we have $d(z, u') \leq r - 1$ (otherwise $d(z, v_0) > \text{diam } G$, which is impossible). Let K be the component of $G - v'_0$ which contains the vertex v_0 . Since $e_G(u') \geq r$, K contains a vertex s with $d(s, u') \geq r$. We show that this contradicts the assumption (iii). First realize that K has at least $2r$ vertices. Further, $d(v_1, G') < r$ and so v_0 and v_1 belong to different components of $G - v'_0$ (otherwise we would have $d(v_0, G^+) > d(v_1, G^+)$). It follows that the path P^1 contains at least r vertices different from the above mentioned $2r$ vertices. Therefore $|V(G)| \geq 2r + r = 3r$, a contradiction.

□

Remark. The graph in Figure 2.6 has $3r - 1$ vertices and the circumference of the graph is less than $2r$. So, the inequality (iii) in Lemma 2.5 is tight, it cannot be improved.

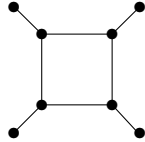


Fig. 2.6

The following important statement is an immediate consequence of Corollaries 2.2, 2.4 and Lemma 2.5.

Theorem 2.6. *If a graph G satisfies the conditions*

- (i) $\text{rad } G = r$,
- (ii) $\text{diam } G \leq 2r - 2$,
- (iii) $|V(G)| \leq 3r - 2$,

then G contains a geodesic cycle of length $2r$ or $2r+1$.

Corollary 2.7. (P.A. Ostrand, see [6])

For all positive integers r and d satisfying $r \leq d \leq 2r - 2$ there exist graphs of radius r and diameter d . The minimum order of such a graph is $d + r$. There are exactly $\lfloor \frac{d-r}{2} \rfloor + 1$ non-isomorphic graphs of order $d + r$, radius r and diameter d . They are characterized as being the sun-graphs with the kernel C_{2r} and with one or two rays (see Fig. 2.7). All isomorphic classes are obtained as s ranges from 0 to $\lfloor \frac{d-r}{2} \rfloor$.

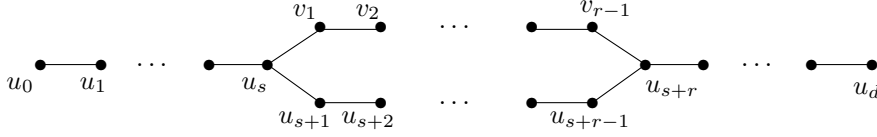


Fig. 2.7

Proof. By Theorem 2.6 a graph G such that $\text{rad } G = r$, $\text{diam } G = d \leq 2r - 2$ and $|V(G)| \leq 3r - 2$ contains a geodesic cycle C_{2r} or C_{2r+1} . Since $\text{diam } G = d$ the graph G has to contain at least $d - r$ vertices except vertices of the cycle. The corollary follows. \square

3. MINIMAL GRAPHS AND MINIMAL ECCENTRIC SEQUENCES.

Theorem 3.1. Let G be a sun-graph with at most 2 rays and with the kernel C_{2r} . If $|V(G)| = 2r + k$, $1 \leq k \leq r - 1$, $\text{diam } G \leq 2r - 2$ and $\text{exc}_G(C_{2r}) \geq 2k - 2$ then the graph G is minimal.

Proof. We will show that there is no graph H such that $e(H) < e(G)$ and $|V(H)| = 2r + k - 1$. Suppose, contrary to our claim, that such a graph H exists. Since $\text{rad } H = r$ and $|V(H)| \leq 3r - 2$, by Theorem 2.6 the graph H contains a cycle C of length $2r$ or $2r + 1$. By the assumption there are at most $2r - (2k - 2) = 2r - 2k + 2$ vertices with eccentricity r in G . We distinguish two cases.

a) $|V(C)| = 2r + 1$

Since $|V(H)| - |V(C)| = k - 2$, by Lemma 1.6b we get $\text{exc}_H(C) \leq 2(k - 2)$. Therefore there are at least $2r + 1 - 2(k - 2) = 2r - 2k + 5$ vertices with eccentricity r in H , contrary to $e(H) < e(G)$.

b) $|V(C)| = 2r$

In this case $|V(H)| - |V(C)| = k - 1$, whence by Lemma 1.6a we get $\text{exc}_H(C) \leq 2(k - 1) - 1 = 2k - 3$ for $k \geq 2$ (the case $k = 1$ is trivial). Therefore there are at least $2r - (2k - 3) = 2r - 2k + 3$ vertices with eccentricity r in the graph H , contrary to $e(H) < e(G)$. \square

Remark. Let G be a sun-graph with at least 3 rays and with the kernel C_{2r} . If $|V(G)| - |V(C)| = k$ then $\text{exc}_G(C) \leq 2k - 3$ by Lemma 1.6c. The eccentricity sequence of G need not be minimal even in the case of the equality $\text{exc}_G(C) = 2k - 3$ (see Figure 3.1).

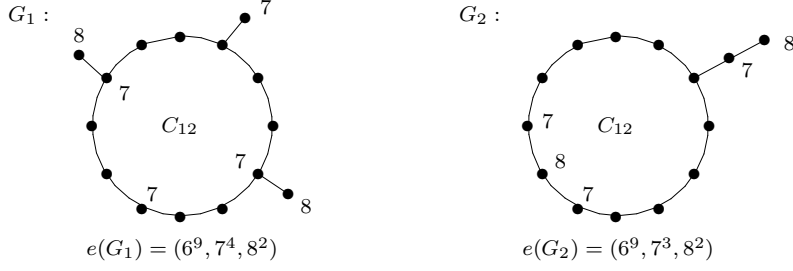


Fig. 3.1

Theorem 3.2. *Let G be a sun-graph with at least 5 rays and with the kernel C_{2r+1} . If $|V(G)| = 2r + 1 + k$, $k \leq r - 2$ and $\text{exc}_G(C_{2r+1}) \geq 2k - 1$ then the graph G is minimal.*

Proof. Since $\text{exc}_G(C_{2r+1}) \geq 2k - 1$ we get that $\text{exc}_G(C_{2r+1})$ is equal to either $2k - 1$ or $2k$ (by Lemma 1.6b). It is sufficient to show that there is no graph H such that $e(H) < e(G)$ and $|V(H)| = 2r + k$. Suppose, contrary to our claim, that such a graph H exists. By Theorem 2.6 H contains a cycle C of length $2r$ or $2r + 1$. By the assumption there are at most $2r + 1 - (2k - 1) = 2r - 2k + 2$ vertices with eccentricity r in G . We distinguish several cases.

a) $|V(C)| = 2r + 1$

In this case $\text{exc}_H(C_{2r+1}) \leq 2(k - 1) = 2k - 2$ (by Lemma 1.6b), hence there are at least $2r + 1 - (2k - 2) = 2r - 2k + 3$ vertices of the graph H with eccentricity r , a contradiction.

b) $|V(C)| = 2r$

Denote by m the number of vertices from $V(H) - V(C)$ which are adjacent to at least one vertex of the cycle C .

$b_1)$ Let $m \geq 3$. In this case, by Lemma 1.6.c we get $\text{exc}_H(C) \leq 2k - 3$ whence there are at least $2r - (2k - 3) = 2r - 2k + 3$ vertices with eccentricity r in H , a contradiction.

$b_2)$ Let $m = 2$. Since $e(H) < e(G)$ we have $\text{exc}_H(C) \geq 2k - 2$. By Lemma 1.6.c $\text{exc}_H(C) \leq 2k - 2$ and so we get $\text{exc}_H(C) = 2k - 2$. It is easy to verify that H is a 2-rays sun-graph with the kernel C_{2r} . Hence there are at most 6 vertices of the graph H with eccentricity $r + 1$. Since $e(H) < e(G)$ and $|V(G)| = |V(H)| + 1$, there are at most 7 vertices with eccentricity $r + 1$ in the graph G . Since $\text{exc}_G(C_{2r+1}) \geq 2k - 1$ and $\text{exc}_G(C_{2r+1}) \leq 2k$ (by Lemma 1.6b) we have two possibilities $\text{exc}_G(C_{2r+1}) = 2k$ or $\text{exc}_G(C_{2r+1}) = 2k - 1$. G is an n -rays sun-graph for $n \geq 5$ and we get that the number of vertices of C_{2r+1} with eccentricity $r + 1$ is $2n$ or $2n - 1$. So, G has at least 9 vertices with eccentricity $r + 1$, a contradiction.

$b_3)$ Let $m = 1$. The vertex from $V(H) - V(C)$ adjacent with at least one vertex of the cycle C is a cut-vertex of the graph H . Since $e(H) < e(G)$ we get $\text{exc}_H(C) \geq 2k - 2$. Therefore it is easy to verify that there are at most 3 vertices of the graph H with eccentricity $r + 1$. But we know that there are at least 9 vertices with eccentricity $r + 1$ in the graph G , a contradiction.

□

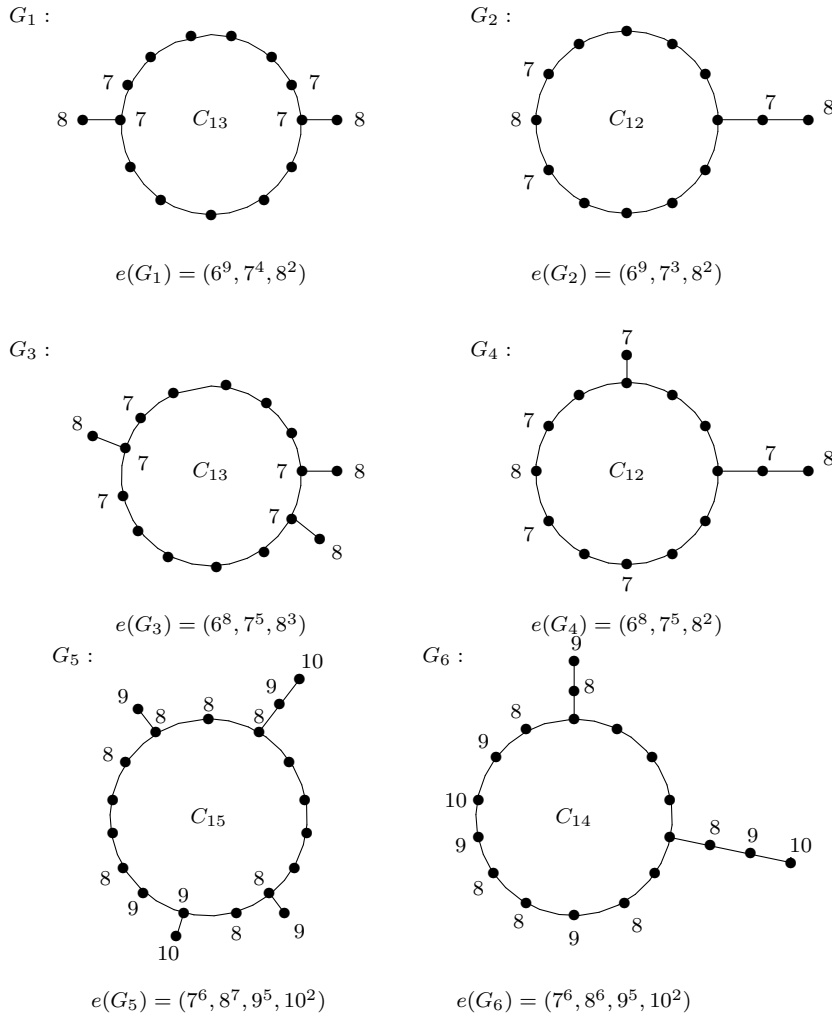


Fig. 3.2

Remarks.

1. If G is a sun-graph with one ray and with the kernel C_{2r+1} then obviously the graph G is not minimal.
2. If G is an n -ray sun-graph, $n \in \{2, 3, 4\}$ and G satisfies the remaining assumptions of Theorem 3.2 then G may or may not be minimal (see Lemma 3.3 and Fig. 3.2).

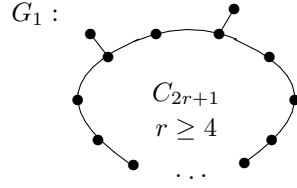
Lemma 3.3. *The following sequences*

- a) $(r^{2r-3}, (r+1)^6), \quad r \geq 4,$
- b) $(r^{2r-4}, (r+1)^8), \quad r \geq 5,$
 $(r^{2r-5}, (r+1)^9), \quad r \geq 5,$
- c) $(r^{2r-6}, (r+1)^{11}), \quad r \geq 6,$
 $(r^{2r-7}, (r+1)^{12}), \quad r \geq 6,$

are minimal eccentric sequences.

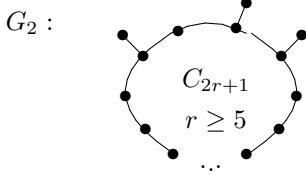
Proof. The sequences from the lemma are the eccentric sequences of the graphs in Figure 3.3.

a)



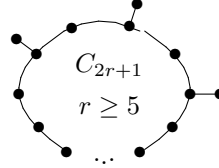
$$e(G_1) = (r^{2r-3}, (r+1)^6)$$

b)



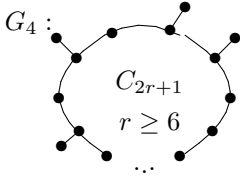
$$e(G_2) = (r^{2r-4}, (r+1)^8)$$

G_3 :

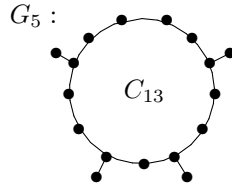


$$e(G_3) = (r^{2r-5}, (r+1)^9)$$

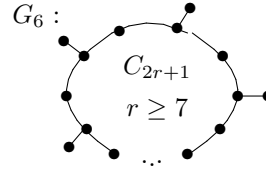
c)



$$e(G_4) = (r^{2r-6}, (r+1)^{11})$$



$$e(G_5) = (6^5, 7^{12})$$



$$e(G_6) = (r^{2r-7}, (r+1)^{12})$$

Fig. 3.3

We will show that these sequences are minimal. It is sufficient to show that if a considered sequence is the eccentric sequence of a graph G then there is no graph H such that $|V(H)| = |V(G)| - 1$ and $e(H) < e(G)$. Suppose, contrary to our claim, that such a graph H exists. The eccentricity of each vertex of H is either r or $r+1$. By Theorem 2.6 the graph H contains a cycle C_{2r} or C_{2r+1} . We distinguish three cases (see Figure 3.3).

a) In this case $|V(G_1)| = 2r+3$ and $|V(H)| = 2r+2$.

a_1) If H contains C_{2r+1} then $\text{exc}(C_{2r+1}) \leq 2$ by Lemma 1.6b. Hence there are at least $2r-1$ vertices with eccentricity r in H , contrary to $e(H) < e(G_1)$.

a_2) Let H contain a cycle C_{2r} . Since $\text{exc}_H(C_{2r}) \leq 3$ (by Lemma 1.6a) and $e(H) < e(G)$, the eccentricity of each of two vertices in $V(H) - V(C_{2r})$ is $r+1$. It yields that each of these vertices has to be adjacent with some vertex of the cycle C_{2r} . Hence $\text{exc}_H(C_{2r}) \leq 2$ (Lemma 1.6c), contrary to $e(H) < e(G_1)$.

b) In this case $|V(G_2)| = |V(G_3)| = 2r+4$ and therefore $|V(H)| = 2r+3$.

b_1) If H contains a cycle C_{2r+1} then $\text{exc}_H(C_{2r+1}) \leq 4$ (by Lemma 1.6b), a contradiction.

b_2) Let H contain a cycle C_{2r} .

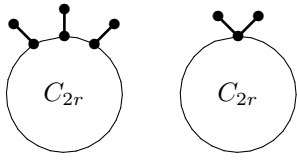


Fig. 3.4

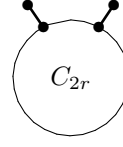
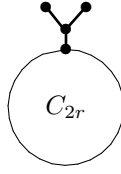


Fig. 3.5

If some of the graphs (for simplicity, the vertices of C_{2r} with degree two are not marked; their position on C_{2r} will not be important) represented by Figure 3.4 is a subgraph of the graph H then it is easy to see that there are at least $2r - 3$ vertices with eccentricity r in H , a contradiction. So we can assume that no graph represented by Figure 3.4 is a subgraph of H . If a graph represented by Figure 3.5 is a subgraph of the graph H then $\text{exc}_H(C_{2r}) \leq 4$. Therefore we have a contradiction with $e(H) < e(G_3)$ and the inequality $e(H) < e(G_2)$ is possible only under the assumption that the eccentricity of each vertex from $V(H) - V(C_{2r})$ is $r + 1$. Hence none of these three vertices is a cut-vertex of H (otherwise we would have a vertex with eccentricity $r+2$). Now it is easy to check that some of the graphs represented by Figure 3.6 has to be a subgraph of H , contrary to $e(H) < e(G_2)$.

The last possibility is that a graph represented by Figure 3.7 is a subgraph of H and the vertices v_1, v_2 are cut-vertices of H . Hence $e_H(v_3) \geq r + 2$, a contradiction.

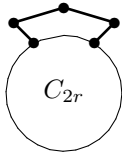


Fig. 3.6

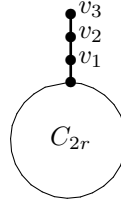


Fig. 3.7

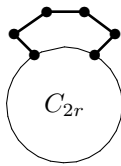


Fig. 3.8

c) In this case $|V(G_4)| = |V(G_6)| = 2r + 5$, $|V(G_5)| = 2 \cdot \text{rad } G_5 + 5$ and therefore $|V(H)| = 2r + 4$.

c_1) If H contains C_{2r+1} then $\text{exc}_H(C_{2r+1}) \leq 6$ (Lemma 1.6b). Therefore there

are at least $2r - 5$ vertices with eccentricity r in H , a contradiction.

c₂) Let H contain a cycle C_{2r} .

If some of the graphs represented by Figure 3.4 is a subgraph of the graph H then $\text{exc}_H(C_{2r}) \leq 5$, a contradiction. So we can suppose that none of the graphs represented by Figure 3.4 is a subgraph of H . If some of the graphs represented by Figure 3.5 is a subgraph of H then $\text{exc}_H(C_{2r}) \leq 6$. Therefore the eccentricity of each vertex from $V(H) - V(C_{2r})$ is $r + 1$. It follows that none of these four vertices can be a cut-vertex of H . Hence it is obvious that some of the graphs represented by Figure 3.8 is a subgraph of H and it is easy to check that the condition $e(H) < e(G)$ does not hold. The last possibility is that a graph represented by Figure 3.7 is a subgraph of H and the vertices v_1, v_2 are cut-vertices of H . Hence $e_H(v_3) \geq r + 2$, a contradiction.

□

Theorem 3.4.

a) *The sequences*

$$\begin{aligned} & (3^5, 4^2), \quad (3^4, 4^4), \\ & (4^7, 5^2), \quad (4^6, 5^4), \quad (4^5, 5^6), \\ & (5^9, 6^2), \quad (5^8, 6^4), \quad (5^7, 6^6), \quad (5^6, 6^8), \quad (5^5, 6^9) \end{aligned}$$

are minimal eccentric sequences.

b) *The sequences*

$$\begin{aligned} & (r^{2r-1}, (r+1)^2), \\ & (r^{2r-2}, (r+1)^4), \\ & (r^{2r-2i+1}, (r+1)^{3i}), i = 2, 3, \dots, \left\lfloor \frac{2r+1}{3} \right\rfloor, \\ & (r^{2r-2i}, (r+1)^{3i+2}), i = 2, 3, \dots, \left\lfloor \frac{2r-1}{3} \right\rfloor \end{aligned}$$

are minimal eccentric sequences of type $(r^\alpha, (r+1)^\beta)$ for $r \geq 6$ and $\alpha + \beta \leq \frac{8r+5}{3}$.

Proof. The sequences $(r^{2r-1}, (r+1)^2)$ and $(r^{2r-2}, (r+1)^4)$ are the eccentric sequences of the graphs in Figures 3.9 and 3.10, respectively, and by Theorem 3.1 they are minimal (for $r \geq 3$).

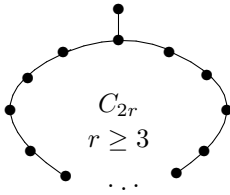


Fig. 3.9

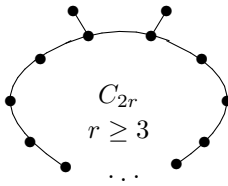
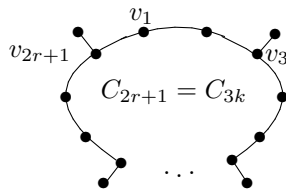


Fig. 3.10

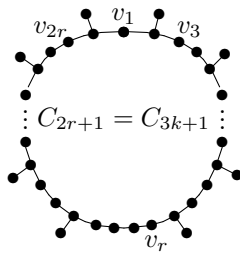
The sequences $(4^5, 5^6)$, $(5^7, 6^6)$, $(5^6, 6^8)$ and $(5^5, 6^9)$ are minimal by Lemma 3.3. We are going to show that also the sequences of the type $(r^{2r-2i+1}, (r+1)^{3i})$, $r \geq 6$ are minimal. For $i \in \{2, 3, 4\}$ it holds by Lemma 3.3. For $i \geq 5$ according to Theorem 3.2 it is sufficient to consider a subgraph of one of the graphs in Figures 3.11, 3.12 or 3.13 (depending on whether $2r + 1 = 3k$, $2r + 1 = 3k + 1$ or $2r + 1 = 3k + 2$, respectively). The subgraph has to be a sun-graph with the required number of vertices. For instance the eccentricity sequence $(12^{15}, 13^{15})$ is realized by a graph with 30 vertices and with radius $r = 12$. So we have to consider the graph in Figure 3.12 ($2 \cdot 12 + 1 = 3 \cdot 8 + 1$) which has 33 vertices for $r = 12$. Then the graph which realizes the sequence $(12^{15}, 13^{15})$ can be obtained from the previous graph with 33 vertices by deleting any three end-vertices. Two of the possibilities are depicted in Figure 3.14.



$$\deg(v_{3i}) = 3$$

$$i = 1, 2, \dots, \frac{2r+1}{3}$$

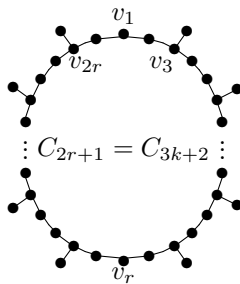
Fig. 3.11



$$\deg(v_{3i-1}) = \deg(v_{2r+4-3i}) = 3,$$

$$i = 1, 2, \dots, \frac{r}{3}$$

Fig. 3.12

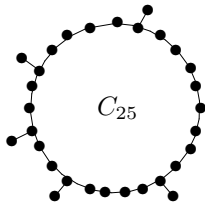


$$\deg(v_{3i}) = \deg(v_{2r-3i}) = \deg(v_{2r}) = 3,$$

$$i = 1, 2, \dots, \frac{r-2}{3}$$

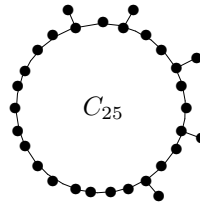
Fig. 3.13

$H_1 :$



$$e(H_1) = (12^{15}, 13^{15})$$

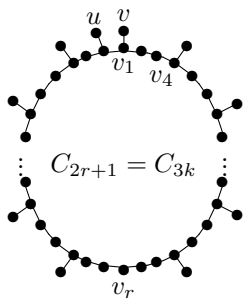
$H_2 :$



$$e(H_2) = (12^{15}, 13^{15})$$

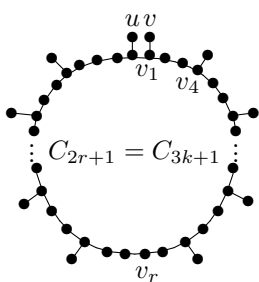
Fig. 3.14

It remains to show that the sequences of type $(r^{2r-2i}, (r+1)^{3i+2})$, $r \geq 6$ are minimal. For $i \in \{2, 3\}$ it holds by Lemma 3.3. For $i \geq 4$ (according to Theorem 3.2) it is sufficient to consider a subgraph of one of the graphs in Figures 3.15, 3.16 or 3.17 (depending on whether $2r+1 = 3k$, $2r+1 = 3k+1$ or $2r+1 = 3k+2$, respectively). The subgraph has to be a sun-graph with the required number of vertices and containing the vertices u, v . \square



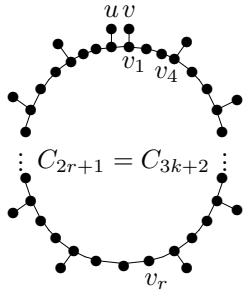
$$\deg(v_{2r+1}) = \deg(v_{3i-2}) = \deg(v_{2r+2-3i}) = 3, \\ i = 1, 2, \dots, \frac{r-1}{3}$$

Fig. 3.15



$$\deg(v_{2r+1}) = \deg(v_{r-2}) = \deg(v_{3i-2}) = \deg(v_{2r-3i}) = 3, \\ i = 1, 2, \dots, \frac{r}{3} - 1$$

Fig. 3.16



$$\deg(v_{3i+1}) = \deg(v_{2r+1-3i}) = 3,$$

$$i = 0, 1, 2, \dots, \frac{r-2}{3}$$

Fig. 3.17

Remark. All minimal eccentric sequences for $r = 3$ and with only two values are known (see [3]):

$$(3^5, 4^2), (3^4, 4^4), (3^3, 4^6), (3^2, 4^8), (3, 4^{10}).$$

The sequence $(3^3, 4^6)$ is realizable by a sun-graph but the last two sequences are not. In Figure 3.18 two realizations of the sequence $(3^3, 4^6)$ are depicted. Note that the minimality of this sequence does not follow from previous considerations ($3 + 6 = 3r$).



Fig. 3.18

In the Figure 3.19 a few realizations of the sequence $(3^4, 4^4)$ are depicted.

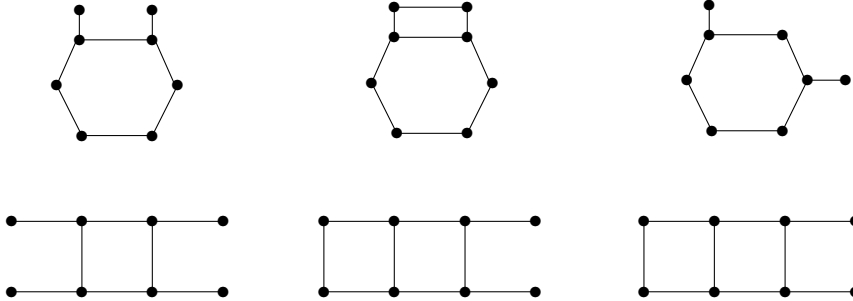


Fig. 3.19

REFERENCES

- [1] Buckley, F. and Harary F., *Distance in Graphs*, Addison-Wesley, Redwood City, California, 1990.
- [2] Buckley, F., *Eccentric sequences, eccentric sets, and graph centrality. Dedicated to the memory of Robert E. Sacks (Purchase, NY, 2000)*, Graph Theory Notes N.Y. 40, 2001, pp. 18-22.
- [3] Haviar, A., Hrnčiar, P. and Monoszová, G., *Minimal eccentric sequences with least eccentricity three*, Acta Univ. M. Belii, Math. no 5, 1997, pp. 27-50.
- [4] Chartrand, G. and Lesniak, L., *Graphs and Digraphs*, Chapman & Hall, London, 1996.
- [5] Lesniak, L., *Eccentric sequences in graphs*, Period. Math. Hungar. 6, 1975, pp. 287-293.
- [6] Ostrand, P.A., *Graphs with specified radius and diameter*, Discrete Math. 4, 1973, pp. 71-75.

DEPARTMENT OF MATHEMATICS; FACULTY OF NATURAL SCIENCES; MATEJ BEL
UNIVERSITY; TAJOVSKÉHO 40; SK-974 01 BANSKÁ BYSTRICA; SLOVAKIA

E-mail: haviar@fpv.umb.sk
hrcnciar@fpv.umb.sk
monosz@fpv.umb.sk

USING A COMPUTER IN MATROID THEORY RESEARCH

PETR HLINĚNÝ

ABSTRACT. In this paper we introduce our computer program MACEK for structural computations with matroids representable over finite (partial) fields.

See <http://www.mcs.vuw.ac.nz/research/macek>. Using this program, we then find all 56 ternary excluded minors for the class of matroids of branch-width three. That research continues on the binary case [P. Hliněný, *On the Excluded Minors for Matroids of Branch-Width Three*, Electronic Journal of Combinatorics 9 (2002), #R32].

1 INTRODUCTION

Matroids represented over a finite (partial) field play an important role in structural matroid theory, similar to the role that graphs embedded on a surface play in structural graph theory. However, unlike for embedded graphs, it is difficult to visualize a matroid in rank bigger than 3, even when it is given as a matrix or a vector configuration. It is even more difficult to examine basic structural properties of given matroids like isomorphism, minors, connectivity, branch-width, or matroid extensions.

It is often the case that proving a theorem in structural matroid theory requires one to check all the small cases (on about, say, 10 elements) by hand, or to verify specific properties of selected small matroids, which are often represented by matrices over finite fields. In graph theory, such tasks are easily solved with a pen and a paper, but, unfortunately, it is not like that with matroids. As matroid researchers know very well themselves, checking the “small cases” can be quite long and painful, and prone to errors. Such is the situation with the problem of finding the excluded minors for matroids of branch-width three we focus on here – it is known that the excluded minors have at most 14 elements.

That is why we have developed a computer program MACEK [6] for practical structural computations with matroids represented over finite partial fields. This program supports an easy manipulation and computations with matrices representing matroids over finite partial fields. For example, one can test for matroid minors, equivalence, representability, isomorphism, branch-width three, connectivity, and other structural properties. An important function is an exhaustive generation of all 3-connected extensions of matroids. The program is free, distributed under

2000 Mathematics Subject Classification. Primary 05B35; Secondary 68R05.

Key words and phrases. matroid, matroid extension, exhaustive generation, branch-width.

Partial support by Slovak grant VEGA #1/1002/04.

Received 13. 5. 2004; Accepted 21. 9. 2004

the terms of the GNU General Public License as published by the Free Software Foundation. See [6] for information about how to obtain and install the MACEK program.

2 BASICS OF MATROIDS

We refer to Oxley [10] for matroid terminology. A *matroid* is a pair $M = (E, \mathcal{B})$ where $E = E(M)$ is the ground set of M (elements of M), and $\mathcal{B} \subseteq 2^E$ is a nonempty collection of *bases* of M . Moreover, matroid bases satisfy the “exchange axiom”; if $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, then there is $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}$. We consider only finite matroids. Subsets of bases are called *independent sets*, and the remaining sets are *dependent*. Minimal dependent sets are called *circuits*. All bases have the same cardinality called the *rank* $r(M)$ of the matroid. The *rank function* $r_M(X)$ in M is the maximal cardinality of an independent subset of a set $X \subseteq E(M)$.

If G is a (multi)graph, then its *cycle matroid* on the ground set $E(G)$ is denoted by $M(G)$. The independent sets of $M(G)$ are acyclic subsets (forests) in G , and the circuits of $M(G)$ are the cycles in G . Another example of a matroid is a finite set of vectors with usual linear dependency. If \mathbf{A} is a matrix, then the matroid formed by the column vectors of \mathbf{A} is called the *vector matroid* of \mathbf{A} .

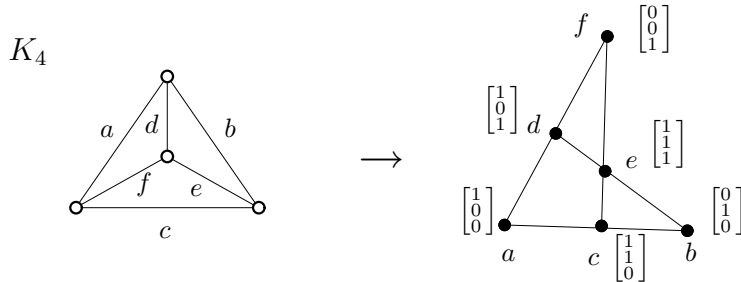


Fig. 1. An example of a vector representation of the cycle matroid $M(K_4)$. The matroid elements are depicted by dots, and their (linear) dependency is shown using lines.

The *dual* matroid M^* of M is defined on the same ground set E , and the bases of M^* are the set-complements of the bases of M . A set X is *coindependent* in M if it is independent in M^* . An element e of M is called a *loop* (a *coloop*), if $\{e\}$ is dependent in M (in M^*). The matroid $M \setminus e$ obtained by *deleting* a non-coloop element e is defined as $(E - \{e\}, \mathcal{B}^-)$ where $\mathcal{B}^- = \{B : B \in \mathcal{B}, e \notin B\}$. The matroid M/e obtained by *contracting* a non-loop element e is defined using duality $M/e = (M^* \setminus e)^*$. (This corresponds to contracting an edge in a graph.) Conversely, a matroid M' is a one-element *extension* (*coextension*) of M if $M = M' \setminus e$ ($M = M'/e$) for some element e . A *minor* of a matroid is obtained by a sequence of deletions and contractions of elements. Since these operations naturally commute, a minor M' of a matroid M can be uniquely expressed as $M' = M \setminus D/C$ where D are the coindependent deleted elements and C are the independent contracted elements.

Matroid Connectivity

An important concept in structural matroid theory is *connectivity*, which is close, but somehow different, to traditional graph connectivity. The *connectivity function* λ_M of a matroid M is defined for all subsets $A \subseteq E$ by

$$\lambda_M(A) = r_M(A) + r_M(E - A) - r(M) + 1.$$

Here $r(M) = r_M(E)$. A subset $A \subseteq E$ is *k-separating* if $\lambda_M(A) \leq k$. A partition $(A, E - A)$ is called a *k-separation* if A is *k-separating* and both $|A|, |E - A| \geq k$. Geometrically, the spans of the two sides of a *k-separation* intersect in a subspace of rank less than k . See in Fig. 2. In a corresponding graph view, the connectivity function $\lambda_G(F)$ of an edge subset $F \subseteq E(G)$ equals the number of vertices of G incident both with F and with $E(G) - F$. (Then $\lambda_G(F) = \lambda_{M(G)}(F)$ provided both sides of the separation are connected in G .) For $n > 1$, a matroid M is *n-connected* if it has no *k-separation* for $k = 1, 2, \dots, n - 1$, and $|E(M)| \geq 2n - 2$.

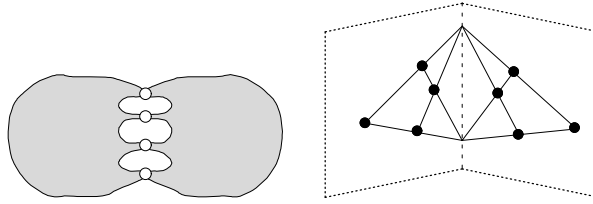


Fig. 2. An illustration to a 4-separation in a graph, and to a 3-separation in a matroid.

Of particular interest to us are 3-connected matroids, which capture the core of most structural properties and problems on matroids. 3-connected matroids can be reasonably easily handled using so called Seymour's Splitter Theorem [14]. Let the *k-wheel* be the matroid $M(W_k)$ where W_k is the graph obtained from a *k-cycle* by adding one vertex adjacent to all other vertices. The *k-whirl* is obtained from the *k-wheel* by relaxing (making independent) the rim circuit.

Theorem 1. (Seymour) Let M, N be 3-connected matroids such that N is a minor of M . Suppose that if N is a wheel (a whirl), then M has no larger wheel (no larger whirl) as a minor. Then there is a 3-connected matroid N_1 such that $|E(N_1)| = |E(N)| + 1$, and that M has an N_1 -minor.

This important theorem allows a step-by-step construction of large 3-connected matroids from smaller ones; adding only one element at each step while maintaining 3-connectivity. (In other words, doing 3-connected one-element extensions and coextensions.)

Matroid Representations

An \mathbb{F} -*representation* of a matroid M is a matrix \mathbf{A} over a field \mathbb{F} whose columns correspond to the elements of M , and linearly independent subsets of columns form the independent sets of M . Alternatively, one may view the matrix \mathbf{A} as a point configuration in a projective space over \mathbb{F} . A matrix \mathbf{A} is in the *standard form* if the number of rows in \mathbf{A} equals the rank of M , and if some basis of M is displayed

in \mathbf{A} as a unit submatrix. A matrix \mathbf{A}' is a *reduced representation* of the matroid $M = M(\mathbf{A}')$ if $[\mathbf{I} | \mathbf{A}']$ is the standard form matrix representing M .

Moreover, we consider matroids represented over partial fields. A *partial field* is a generalization of a field, in which the addition is a partial operation. We refer to [13] for a formal definition and properties of partial fields. A typical and well-known example is the *regular* partial field consisting of the integers $-1, 0, 1$ with usual addition and multiplication. A matrix \mathbf{A} over a partial field \mathbb{P} is *proper* if all subdeterminants of \mathbf{A} are defined in \mathbb{P} . For example, proper regular matrices are traditionally known as totally-unimodular. A matroid N is representable over \mathbb{P} iff there is a proper matrix \mathbf{A} over \mathbb{P} such that $N \simeq M(\mathbf{A})$.

A partial field is called *finite* if the equation $x - 1 = y$ has finitely many solutions in \mathbb{P} . All finite fields are clearly finite in this sense. However, a finite partial field may have infinitely many elements. (The reason for our terminology is that a fixed-rank simple matroid representable over a finite partial field may have only finite number of elements.)

We say that two matrices are *strongly equivalent* if one can be obtained from the other by a sequence of row or column permutations, non-zero scalings, and pivots. Considering reduced \mathbb{P} -representations of matroids, we call the \mathbb{P} -*represented matroid* an equivalence class of unlabeled matrices with respect to the strong equivalence. Clearly, represented matroids refine the isomorphism classes of matroids. On the other hand, one matroid may have several non-equivalent representations over \mathbb{P} . An obvious example of this phenomenon is presented in Fig. figdifrep.

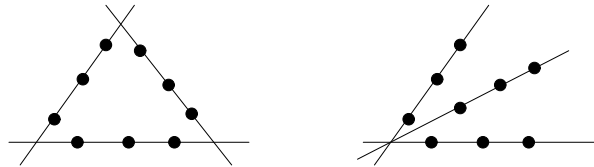


Fig. 3. Two inequivalent representations of a 9-element rank-3 matroid.

A matroid M is *regular* if M is representable over the regular partial field. A regular matroid is then representable over all fields. A matroid M is *binary*, *ternary*, if M is representable over the fields $GF(2)$, $GF(3)$, respectively. We remark that cycle matroids of graphs are regular.

Small matroid enumeration

To introduce and demonstrate capabilities of the MACEK program in practice, we first present a table summarizing enumeration of small 3-connected regular, binary, ternary, and quaternary matroids. Let $U_{2,k}$ denote the rank-2 matroid formed by k distinct points in one line.

representable \ elements	4	5	6	7	8	9	10	11	12	13	14	15
regular	0	0	1	0	1	4	7	10	33	84	260	908
$GF(2)$, non-regular	0	0	0	2	2	4	17	70	337	2080	16739	181834
$GF(3)$, non-regular	1	0	1	6	23	120	1045	14116	330470	?	?	?
$GF(4)$, non- $GF(2,3)$	0	2	2	8	69	748	15305	?	?	?	?	?

TAB. 1. The numbers of 3-connected matroids representable over small fields.

The results in Table 1 have been obtained using Theorem 1 and the following MACEK computations:

- The numbers in the first row have been computed via regular 3-connected extensions of all small wheels (removing duplicities).
- The numbers in the second row have been obtained using binary 3-connected extensions of the Fano matroid (the binary projective plane), which is the smallest binary non-regular matroid.
- In the third row, we have computed all ternary 3-connected extensions of the 3-whirl matroid, and added the larger whirls. (Although every non-binary matroid contains the 4-point line $U_{2,4}$ as a minor, that matroid has no ternary extensions, and so we had to use a detour in our computation.)
- In the fourth row, we have computed all quaternary 3-connected extensions of the 5-point line $U_{2,5}$, which is the smallest non-ternary matroid. Moreover, we have removed isomorphic pairs of matroids afterward, as quaternary matroids already may have non-equivalent representations.

3 OVERVIEW OF MACEK CAPABILITIES

We give a brief overview of our MACEK program in this section. As we have already mentioned, the program has been developed to assist matroid theory research with useful structural computations. It is designed in a command-line oriented form, which is suitable especially for large-scale batch computations, but answering (single) structural questions is also supported well. We refer to [6] for a full description and technical details (including an installation instructions).

Matrix representations

The MACEK program deals with \mathbb{P} -represented matroids (given by reduced matrix representations) in the sense of the definition from Section 2. \mathbb{P} may be an arbitrary finite partial field. Definitions of common small fields and partial fields are compiled in MACEK, and it is not difficult to add other partial fields via description of generators of the multiplicative subgroup. Representations of many well-known matroids are also distributed with the program.

Since the basic entity in MACEK is a \mathbb{P} -represented matroid – an equivalence class of matrices over \mathbb{P} , two non-equivalent matrices are considered distinct even if they represent isomorphic matroids. So the issue of inequivalent matroid representations has to be considered when it comes up, i.e. over fields larger than $GF(3)$. In this context, it is important to mention that matroid elements in MACEK are not explicitly labeled (though they get implicit labels for the purpose of display). So an “equivalence” is meant to be the strong unlabeled equivalence of matrices.

Structural functions

It is possible to compute various matroid tasks and properties with MACEK: Those include looking for specific minors in given matroids, finding an equivalence or an abstract isomorphism between matroids, computing matroid connectivity or girth (shortest cycle length), etc. Other specific functions test for branch-width three or for paving matroids, etc. All these functions can also be applied as filters to (generated) matroid lists.

We remark that such structural properties are usually computationally very hard, and hence we have to implement most of them using clever adaptations of brute-force methods. The bad side is that computational time grows exponentially, and usually only matroids on less than 20 elements could be efficiently handled. Still, the program functions seem to be enough powerful and fast to substantially help with matroid theory research.

Besides those, MACEK can compute and print out various structural information about a matroid itself, like bases, automorphism group orbits, small flats and separations, connectivity, and representability over other fields. For example, the following extensive information can be printed about the matroid R_{12} . (R_{12} is an interesting matroid playing a crucial role in Seymour's decomposition theorem [14] for regular matroids.)

```
MACEK 1.1.9999 (23/04/04) starting...
vv=====vv
^532~      Output of the command "!prmore ((t)) [1]":
~ -----
~ matrix 0x8190168 [R12], r=6, c=6, tr=0, ref=(nil)
~      '1')  '2')  '3')  '4')  '5')  '6')
~      '1')  1    1    1    o    o    o
~      '2')  1    1    o    1    o    o
~      '3')  1    o    o    o    1    o
~      '4')  o    1    o    o    o    1
~      '5')  o    o    1    o   -1   -1
~      '6')  o    o    o    1   -1   -1
~ -----
^532~ Number of matroid [R12] bases: 441
^532~   - per elements [1: 210] [2: 210] [3: 231] [4: 231] [5: 210] [6:210]
~                   [-1: 231] [-2: 231] [-3: 210] [-4: 210] [-5: 231] [-6: 231]
^532~ Automorphism group orbits of [R12] are (via first elem id):
~       (1, 1, 3, 3, 1, 1, 3, 3, 1, 1, 3, 3)
^535~ There are -NO- (nontrivial) flats in [R12] of rank 0.
^535~ There are -NO- (nontrivial) flats in [R12] of rank 1.
^535~ Listing all (nontrivial) flats in [R12] of rank 2:
~   - rank-2 flat (1)    { 1, 5, -3 }
~   - rank-2 flat (2)    { 2, 6, -4 }
^535~ Listing all (nontrivial) flats in [R12] of rank 3:
~   ..... <skipped> .....
^535~ There are -NO- exact separations in [R12] of lambda 1.
^535~ There are -NO- exact separations in [R12] of lambda 2.
^535~ Listing all exact separations in [R12] of lambda 3:
~   - 3-separation (1)    ( 1, 2, 5, 6, -3, -4, )
~   - 3-separation (2)    ( 1, 5, -3, )
~   - 3-separation (3)    ( 2, 6, -4, )
~   - 3-separation (4)    ( 3, -1, -5, )
~   - 3-separation (5)    ( 3, 4, -1, -2, -5, -6, )
~   - 3-separation (6)    ( 4, -2, -6, )
^535~ Matroid [R12] connectivity is 3.
^535~ Matroid [R12] girth (shortest cycle) is 3.
^535~ Matroid [R12] representability:
```

~~~~~

## Matroid generation

In order to use a computer in proving general statements about matroids, we need a suitable tool for exhaustive generation of matroids. Due to the existence of enormous numbers of matroids already on a few elements, MACEK supports generating matroid extensions rather than generating from scratch. This approach seems to be better suited for practical applications. A theoretical description of the (quite involved) generation algorithm used in MACEK is presented in [8]. Our algorithm allows for a multi-step equivalence-free generation of extensions, which can be, moreover, easily distributed in a parallel computing environment without need for inter-process communication.

Likewise, one can ask MACEK to generate all nonequivalent single-element 3-connected extensions and coextensions of the matroid  $R_{10}$  which are representable over  $GF(5)$ . The answer is as follows,

```
sh$ macek -pgf5 '!extend' R10
MACEK 1.1.9999 (23/04/04) starting...
~979~ Generated 12 non-equiv 3-conn row co-extensions of the sequence [R10] (5x5|5x5).
~985~ Generated 12 non-equiv 3-conn column extensions of the sequence [R10] (5x5|5x5).
~985~ In total 24 (co-)extensions of 1 matrix-sequences generated for "b" over GF(5).
```

and the 24 generated extensions can be readily used in further computations. For example, a subsequent test can find out that two of the 12 coextensions there have girth 5, i.e. they have no circuits on less than 5 elements. Or, that all generated extensions are pairwise non-isomorphic here. The multi-step feature of our generation algorithm allows to start next steps independently from each of the previous extensions, and yet to generate no duplicated extensions.

The above mentioned matroid  $R_{10}$  is well known for being a splitter for the class of regular matroids. (A *splitter* has no 3-connected extension or coextension in its class.) Using MACEK, one can easily prove that  $R_{10}$  is a splitter also for the class of all near-regular matroids (those representable over all fields larger than  $GF(2)$ , at least).

```
sh$ macek -pnreg '!extend' R10
MACEK 1.1.9999 (23/04/04) starting...
~126~ Generated 0 non-equiv 3-conn row co-extensions of the sequence [R10] (5x5|5x5).
~126~ Generated 0 non-equiv 3-conn column extensions of the sequence [R10] (5x5|5x5).
~126~ In total 0 (co-)extensions of 1 matrix-sequences generated for "b" over near-reg.
```

Besides matroid extensions, MACEK supports generation of all representations of a matroid over a given field. (That, of course, includes simply testing representability over a field.) For example, one may find out that the uniform matroid  $U_{3,6}$  has 140 representations over the field  $GF(7)$  that are distinct up to scaling, but only three of them are inequivalent (in the unlabeled sense). As another example, one may compute that each of the 6 single-element extensions of  $U_{3,6}$  over  $GF(7)$  have more than one pairwise non-equivalent representations there:

```
sh$ macek -pgf7 '!verbose;!extend c;!represgen "" allq' U36
MACEK 1.1.9999 (23/04/04) starting...
```

```

~333~   Generated 6 non-equiv 3-conn column extensions of the sequence [U36] (3x3|3x3).
~333~   In total 6 (co-)extensions of 1 matrix-sequences generated for "c" over GF(7).
~334~   There are 2 nonequiv GF(7)-representations of #1 matroid [U36_c1] (3x4, GF(7)).
~334~   There are 10 nonequiv GF(7)-representations of #2 matroid [U36_c2] (3x4, GF(7)).
~335~   There are 4 nonequiv GF(7)-representations of #3 matroid [U36_c3] (3x4, GF(7)).
~335~   There are 10 nonequiv GF(7)-representations of #4 matroid [U36_c4] (3x4, GF(7)).
~336~   There are 10 nonequiv GF(7)-representations of #5 matroid [U36_c5] (3x4, GF(7)).
~337~   There are 2 nonequiv GF(7)-representations of #6 matroid [U36_c6] (3x4, GF(7)).

```

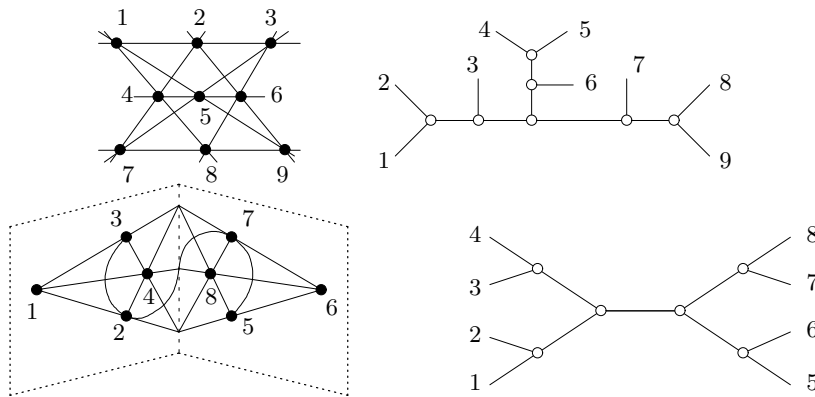
## Other capabilities

Lastly, we briefly mention other supplementary functions in MACEK. Those include mainly file reading and writing operations, and operations manipulating with single matrices and with whole lists of them. (Actually, all data in MACEK are structured in a tree-like fashion.) Moreover, MACEK offers basic scripting capabilities like procedures, conditions, jumps, and others. We refer to the manual for a full description, and for many examples of use.

### 4 EXCLUDED MINORS FOR BRANCH-WIDTH THREE

We now move to the main topic of research in this paper. The concept of graph tree-width is rather well known nowadays. A similar, but less known, structural parameter is called branch-width, and it is within a constant factor of tree-width on graphs.

Let  $\lambda$  be a symmetric function on the subsets of a ground set  $E$ . (Here  $\lambda \equiv \lambda_G$  is the connectivity function of a graph, or  $\lambda \equiv \lambda_M$  of a matroid.) A *branch decomposition* of  $\lambda$  is a pair  $(T, \tau)$  where  $T$  is a sub-cubic tree ( $\Delta(T) \leq 3$ ), and  $\tau$  is a bijection of  $E$  into the leaves of  $T$ . For  $e$  being an edge of  $T$ , the *width* of  $e$  in  $(T, \tau)$  equals  $\lambda(A) = \lambda(E - A)$ , where  $A \subseteq E$  are the elements mapped by  $\tau$  to leaves of one of the two connected components of  $T - e$ . The width of the branch decomposition  $(T, \tau)$  is maximum of the widths of all edges of  $T$ , and *branch-width* of  $\lambda$  is the minimal width over all branch decompositions of  $\lambda$ .



**Fig. 4.** Two examples of width-3 branch decompositions of the Pappus matroid (top left, in rank 3) and of the binary affine cube (bottom left, in rank 4). The lines in matroid pictures show dependencies among elements.

Recall the definitions of graph and matroid connectivity functions from Section 2. Then branch-width of  $\lambda \equiv \lambda_G$  is called *branch-width of a graph  $G$* , and that of  $\lambda \equiv \lambda_M$  is called *branch-width of a matroid  $M$* . (See examples in Fig. 4.) We remark that it is possible to define matroid tree-width [9] which is within a constant factor of branch-width, but this is not a straightforward extension of traditional graph tree-width.

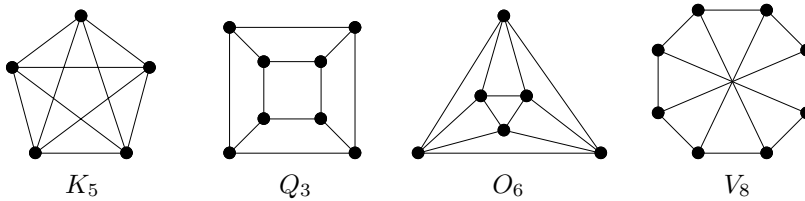
The main focus of this research is on the class  $\mathcal{B}_3$  of all matroids of branch-width at most three. Clearly, this class is minor-closed. A matroid  $N$  is said to be an *excluded minor* for a minor-closed family  $\mathcal{N}$  if  $N \notin \mathcal{N}$  but all proper minors of  $N$  belong to  $\mathcal{N}$ . The question is: What are the excluded minors for the class  $\mathcal{B}_3$ ? We base our (partial) answer to the question (further Theorems 4 and 5, Proposition ??? on the following theorem [4,5]:

**Theorem 2.** (Hall, Oxley, Semple, Whittle) If  $N$  is an excluded minor for the class  $\mathcal{B}_3$ , then  $N$  is a 3-connected matroid on at most 14 elements.

### The Binary Case

The story of the research originally started with considering the class of all graphs of branch-width at most three. All the excluded minors for this class were found first by Dharmatilake and others [3], but that research has not been publicized further. The same list was independently found later in [1].

**Theorem 3.** (Dharmatilake, Chopra, Johnson, Robertson) A graph has branch-width at most 3 if and only if it has no minor isomorphic to any one of the graphs  $\{K_5, Q_3, O_6, V_8\}$ . (See the graphs in Fig. 5.)



**Fig. 5.** The four excluded minors for graphs of branch-width at most 3.

It is easy to see that the cycle matroids of the graphs from Theorem 3 are also excluded minors for the matroid class  $\mathcal{B}_3$ . Moreover, the well-known regular matroid  $R_{10}$  is an excluded minor for  $\mathcal{B}_3$ . Let us denote

$$\mathcal{R}_3 = \{M(K_5), M(K_5)^*, M(Q_3), M(O_6), M(V_8), M(V_8)^*, R_{10}\}.$$

Dharmatilake then used a specialized computer program to search for all small binary matroids (up to 12 elements) that are excluded minors for  $\mathcal{B}_3$ . He found three more non-regular matroids, denoted by  $N_{11}, N_{23}, N_{11}^*$ , and he conjectured [3] that  $\mathcal{R}_3 \cup \{N_{11}, N_{23}, N_{11}^*\}$  is the complete set of binary excluded minors for  $\mathcal{B}_3$ .

$$R_{10} \begin{bmatrix} -1 & 1 & 0 & 0 & 1 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 1 & 0 & 0 & 1 & -1 \end{bmatrix}$$

35

**Fig. 6.** The matroid  $R_{10}$ , in a totally unimodular (regular) representation.

We have finished [7] a computerized search of binary matroids up to 14 elements (cf. Theorem 2) using functions of our program MACEK; which has turned out to be a much faster computation than Dharmatilake's one. (While Dharmatilake carried out a long computation in a supercomputing center, our search of binary matroids up to 12 elements took only a few seconds on a home PC computer. An extension up to 14 elements took another several hours.)

**Theorem 4.** (PH) A binary matroid has branch-width at most 3 if and only if it has no minor isomorphic to one of the members of  $\mathcal{R}_3 \cup \{N_{11}, N_{23}, N_{11}^*\}$ .

### The Ternary Case

A natural next step is to consider the same question – what are the excluded minors for the class  $\mathcal{B}_3$ , over ternary matroids, and so on. In theory, there is no problem with it, as an analogous MACEK computation can be run over the field  $GF(3)$ . However, the complexity of computation grows enormously. That is illustrated in the next Table 2 showing the numbers of small regular, binary, and ternary members of  $\mathcal{B}_3$ .

| <i>representable</i> \ <i>elements</i> | 4 | 5 | 6 | 7 | 8  | 9   | 10  | 11   | 12    | 13     | 14     |
|----------------------------------------|---|---|---|---|----|-----|-----|------|-------|--------|--------|
| regular                                | 0 | 0 | 1 | 0 | 1  | 4   | 4   | 8    | 23    | 46     | 123    |
| $GF(2)$ , non-regular                  | 0 | 0 | 0 | 2 | 2  | 4   | 14  | 38   | 125   | 432    | 1551   |
| $GF(3)$ , non-regular                  | 1 | 0 | 1 | 6 | 23 | 102 | 538 | 3008 | 18597 | 119594 | 796208 |

**Tab. 2.** The numbers of 3-connected matroids of branch-width three over small fields.

Yet we have been able to finish at least the search of ternary matroids up to 14 elements on a supercomputing cluster. Total computing time was equivalent to almost 2 years on a single 2GHz PC computer. Hence we have proved:

**Theorem 5.** There is a family  $\mathcal{T}_3$  of 49 ternary non-regular matroids; such that a ternary matroid has branch-width at most 3 if and only if it has no minor isomorphic to one of the 56 members of  $\mathcal{R}_3 \cup \mathcal{T}_3$ .

*Proof.* By [15], all non-binary matroids contain a  $U_{2,4}$ -minor. Unfortunately,  $U_{2,4}$  (isomorphic to the 2-whirl) is one of the exceptions in Theorem 1, but an enhancement of this theorem [2] (also in [Section 11.3]10) implies that all 3-connected ternary extensions of  $U_{2,4}$ , that are not whirls, contain a single-element extension or coextension of the 3-whirl  $\mathcal{W}^3$  as a minor. All whirls clearly have branch-width three.

Hence each excluded minor for our class  $\mathcal{B}_3$  contains a single-element extension or coextension of  $\mathcal{W}^3$  as a minor, and so Theorem 1 can be applied here. We proceed our computation along the following scheme:

- (1) Start with the family  $\mathcal{L}_6 = \{\mathcal{W}^3\}$ , and  $\mathcal{T}_3 = \emptyset$ .
- (2) For  $i = 6, 7, \dots, 13$ , compute a list  $\mathcal{X}_{i+1}$  of all single-element extensions and coextensions of the matroids in  $\mathcal{L}_i$ .
- (3) Set  $\mathcal{L}_{i+1}$  to be the set of all matroids from  $\mathcal{X}_{i+1}$  that have branch-width at most three.

- (4) Remove all matroids from  $\mathcal{X}_{i+1} - \mathcal{L}_{i+1}$  that have minors in the current set  $\mathcal{T}_3$  or in  $\mathcal{R}_3$ . Add the remaining matroids to the list  $\mathcal{T}_3$ .
- (5) If  $i < 14$ , then go to 2 with  $i + 1$ .

After the first iteration of the scheme,  $\mathcal{L}_7$  contains all 6 single-element extensions and coextensions of  $\mathcal{W}^3$ , all of them having branch-width three. Then every ternary excluded minor  $X$  for the class  $\mathcal{B}_3$  is eventually constructed in step 2 for  $i \in \{8, \dots, 13\}$ , as that follows from Theorems 1 and 2. Such excluded minors  $X$  are then identified in step 4, and stored in the list  $\mathcal{T}_3$ . On the other hand, every matroid  $X \in \mathcal{T}_3$  has branch-width larger than three, and  $X$  has no proper minor of branch-width more than three. So  $X$  is an excluded minor for  $\mathcal{B}_3$ .

### Future work

We have run the same procedure as described in the proof of Theorem 5 over other small fields  $GF(4)$ ,  $GF(5)$  and  $GF(7)$ . The only difference is that we have started the generating procedure from the list  $\mathcal{L}_5 = \{U_{2,5}, U_{3,5}\}$ , referring the result of [12]:

Any 3-connected non-binary non-ternary matroid representable over some field has a  $U_{2,5}$ - or  $U_{3,5}$ -minor.

Moreover, keeping in mind that matroids may have nonequivalent representations over fields larger than  $GF(3)$ , we have removed isomorphic pairs of matroids from the resulting lists. We present a summary of the results that we have obtained in the next Table 3.

| <i>representable</i> \ <i>elements</i> | 7 | 8   | 9   | 10 | 11 | 12 | 13 | 14 |
|----------------------------------------|---|-----|-----|----|----|----|----|----|
| regular                                | 0 | 0   | 0   | 3  | 0  | 4  | 0  | 0  |
| $GF(2)$ , non-regular                  | 0 | 0   | 0   | 3  | 0  | 0  | 0  | 0  |
| $GF(3)$ , non-regular                  | 0 | 0   | 18  | 31 | 0  | 0  | 0  | 0  |
| $GF(4)$ , non- $GF(2,3)$               | 0 | 5   | 90  | 32 | 0  | ?  | ?  | ?  |
| $GF(5)$ , non- $GF(2,3,4)$             | 0 | 38  | 444 | 29 | ?  | ?  | ?  | ?  |
| $GF(7)$ , non- $GF(2,3,4,5)$           | 2 | 119 | 344 | ?  | ?  | ?  | ?  | ?  |
| $GF(8)$ , non- $GF(2,3,4,5,7)$         | 0 | 5   | ?   | ?  | ?  | ?  | ?  | ?  |
| $GF(9)$ , non- $GF(2,3,4,5,7,8)$       | 0 | 0   | ?   | ?  | ?  | ?  | ?  | ?  |

**Tab. 3.** The numbers of excluded minors for matroids of branch-width three.

Notice, in particular, how many (small) excluded minors for the class  $\mathcal{B}_3$  are there. This shows that the matroid class  $\mathcal{B}_3$  has a quite rich structure, unlike its graphic counterpart which has only 4 excluded minors (Theorem 3).

**Proposition 6.** There are at least 1167 pairwise non-isomorphic excluded minors for the class  $\mathcal{B}_3$  of all matroids of branch-width at most three.

As one can see in Table 3, we have not been able to finish the exhausted search up to 14 elements. We would better say that we have hit really hard the “wall of intractability” here. It appears that the number of the members of  $\mathcal{B}_3$  up to 14 elements (regardless of representability) grows enormously, and hence it is simply impossible to finish the search for the excluded minors for  $\mathcal{B}_3$  in general, even if one tried to design much faster algorithms than we have used here. However, the numbers in Table 3 still give a hope of finishing up the whole problem – it looks likely that there are no more “large” excluded minors for  $\mathcal{B}_3$  than we already know.

Supported by our computing results, we propose the following strengthening of Theorem 2:

**Conjecture.** If  $N$  is a non-regular excluded minor for the class  $\mathcal{B}_3$  of all matroids of branch-width at most three, then  $N$  has at most 10 elements.

Having a theoretical result like that at hand, it could be possible to carry out an exhaustive search of all abstract matroids on up to 10 elements, we think. (Unfortunately, the current version of MACEK does not yet support computations with abstract, i.e. also non-representable, matroids.)

## 5 RELIABILITY OF COMPUTATIONS

A natural question a reader would probably ask here is: How reliable are the results of MACEK computations? Computer-assisted proofs do not fit into the traditional scheme of mathematical proofs which could be verified step-by-step by hand, and so their wide acceptance could be sometimes controversial. (For example, look at the story of the famous “Four colour theorem”.) However, everybody nowadays uses a calculator to do arithmetical operations, and nobody would doubt the results. Hence it is likely that a similar wide acceptance of computer-checked proofs will come soon.

In this section, we summarize the checks we have carried out to ensure that our computation results are correct. We divide the summary into two parts, one showing nontrivial internal relations between different parts of our computation, and the other one relating our computation results to other known research.

### Computing self-tests

- All computations in MACEK are backed by numerous internal self-checks, usually checking properties or relations, which follow from matroid theory but are not directly used in MACEK algorithms. More details can be found in MACEK source documentation.
- We have checked that the lists of excluded minors for  $\mathcal{B}_3$  are closed under duality.
- The lists of all matroids of branch-width at most three over the (respective) fields  $GF(2)$ ,  $GF(3)$  are obtained as side products in our computation. We have compared these lists with the lists independently computed via an enumeration of all small represented matroids (cf. Table 1), and selecting those members of branch-width at most three afterward. We have also verified that the intersection of the lists over  $GF(2)$  and  $GF(3)$  contains exactly the regular members.
- In the case of the fields  $GF(4)$ ,  $GF(5)$ ,  $GF(7)$ , over which a matroid may have inequivalent representations, we have checked that each isomorphism class of excluded minors generated in our computation really contains all possible inequivalent representations of it.
- We have also performed various “cross-representability” tests. That means, for  $p, q \in \{4, 5, 7\}$ , we have taken the lists  $\mathcal{L}^p$ ,  $\mathcal{L}^q$  of all generated matroids of branch-width three over  $GF(p)$  and over  $GF(q)$  (which are side products of our computation), and we have verified that the  $GF(q)$ -representable members of  $\mathcal{L}^p$  match the  $GF(p)$ -representable members of  $\mathcal{L}^q$ . (Notice that such a test does not work with  $p = 3$  since our procedure generates only non-ternary matroids over  $GF(q)$  for  $q > 3$ .)

Of course, one may think about other self-tests that could be run with MACEK, and the reader is welcome to download MACEK [6] and try the tests.

## Comparing with other research

- The binary excluded minors for the class  $\mathcal{B}_3$  have been found by Dharmatilake [3]. So, first of all, we have compared our results [7] obtained over  $GF(2)$  with that list. We remark that our computing approach to the problem has been quite different from Dharmatilake's approach.
- Moreover, a subsequent work of X. Zhou [16,17] has, among other interesting results, provided a hand-written proof of Theorem 4 (Dharmatilake's conjecture). Actually, his research has also been based on computations performed by MACEK, but then he has found clever arguments (based on the concept of internal 4-connectivity) that allowed him to narrow the exhausted search significantly, and so to write down all the steps and necessary arguments in a paper.
- Lastly we mention an exhaustive generation of matroids computed by R. Pendavingh [11], in a search for the excluded minors for matroids representable over  $GF(5)$  and  $GF(7)$ . (We have run recently a similar computation, and the common parts of the results matched each other.) Although it is not directly related to our paper, we consider this recent feedback very important since it independently confirms correctness of our exhaustive generation process in MACEK over other fields than  $GF(2)$ .

## ACKNOWLEDGMENTS

The author, besides his current grant support, acknowledges generous support from the Victoria University of Wellington and from the New Zealand Marsden Fund during his stay in Wellington in 2000–2002, where development of the MACEK program has begun. The author also thanks Geoff Whittle for helpful ideas and comments in early stages of MACEK development.

The large-scale computations used in the proof of Theorem 5 were mostly run on the `termit` computing cluster at the Technical University Ostrava. Additional computing data summarized in Table 1 result from author's current computing project run on the `minos` cluster at the West Bohemia University (the ITI center, supported by the Ministry of Education of the Czech Republic as the project LN00A056).

## REFERENCES

- [1] H. Bodlaender, D.M. Thilikos, *Graphs with Branch-Width at most Three*, Technical Report UU-CS-1997-37, Department of Computer Science, Utrecht University, Utrecht, the Netherlands, 1997.
- [2] C.R. Coullard, *Minors of 3-Connected Matroids and Adjoints of Binary Matroids*, Ph.D. thesis, Northwestern University, 1985.
- [3] J.S. Dharmatilake, *Binary Matroids of Branch-Width 3*, Ph.D. dissertation, Ohio State University, 1994.
- [4] R. Hall, *Excluded Minors for the Matroids of Branch-Width Three*, M.Sc. Thesis, Victoria University of Wellington, 2000.
- [5] R. Hall, J. Oxley, C. Semple, G. Whittle, *On Matroids of Branch-Width Three*, *J. Combin. Theory Ser. B* **86** (2002), 148–171.
- [6] P. Hliněný, *The MACEK Program*, <http://www.mcs.vuw.ac.nz/research/macek>, 2002–2004.
- [6a] P. Hliněný, *The MACEK Program*, <http://www.cs.vsb.cz/~hlineny/MACEK>, 2002–2004.
- [7] P. Hliněný, *On the Excluded Minors for Matroids of Branch-Width Three*, *Electronic Journal of Combinatorics* **9** (2002), no. #R32.
- [8] P. Hliněný, *Equivalence-Free Exhaustive Generation of Represented Matroids*, 2004 (submitted).

- [9] P. Hliněný, G.P. Whittle, *Matroid Tree-Width*, 2003, Extended abstract in: Eurocomb'03, ITI Series 2003–145, Charles University, Prague, Czech Republic, 202–205. (submitted).
- [10] J.G. Oxley, *Matroid Theory*, Oxford University Press, 1992.
- [11] R. Pendavingh, 2004, personal communication.
- [12] C. Semple, G.P. Whittle, *On Representable Matroids Having Neither  $U_{2,5}$ -nor  $U_{3,5}$ -minors*, Matroid Theory, Contemporary Math. 197, Amer. Math. Soc., 1995, pp. 377–386.
- [13] C. Semple, G.P. Whittle, *Partial Fields and Matroid Representation*, Advances in Appl. Math. **17** (1996), 184–208.
- [14] P.D. Seymour, *Decomposition of Regular Matroids*, J. Combin. Theory Ser. B **28** (1980), 305–359.
- [15] W.T. Tutte, *A Homotopy Theorem for Matroids*, Trans. Amer. Math. Soc. **88**, 144–174.
- [16] X. Zhou, *Some Excluded Minor Theorems for Binary Matroids*, PhD. Thesis, The Ohio State University, 2003.
- [17] X. Zhou, *On Internally 4-connected Non-regular Binary Matroids*, J. Combin. Theory Ser. B (2004) (to appear).

DEPARTMENT OF COMPUTER SCIENCE; VŠB – TECHNICAL UNIVERSITY OSTRAVA; 17. LISTOPADU 15, CZ–708 33 OSTRAVA; CZECH REPUBLIC

E-mail: petr.hlineny@vsb.cz

INSTITUTE OF MATHEMATICS AND COMPUTER SCIENCE; MATEJ BEL UNIVERSITY AND SLOVAK ACADEMY OF SCIENCES; SEVERNÁ 5, SK–974 00 BANSKÁ BYSTRICA ; SLOVAK REPUBLIC

E-mail: hlineny@savbb.sk

APPENDIX A

Here we present the list  $\mathcal{T}_3$  of all 49 non-regular ternary excluded minors for the class  $\mathcal{B}_3$  of matroids of branch-width at most three. Each one is given as a reduced matrix representation over  $GF(3)$ .

|           |           |             |             |
|-----------|-----------|-------------|-------------|
| 1 0 1     |           |             |             |
| 1 1 0     | 1 0 1 0   | 1 0 1 0     |             |
| 0 1 1     | 1 1 0 0   | 1 1 0 0     | 1 0 1 0 0   |
| 0 1 2     | 0 1 1 1   | 0 1 1 1     | 1 1 0 0 0   |
| 1 0 2     | 0 1 2 0   | 0 1 2 0     | 0 1 1 1 1   |
| 1 1 1     | 1 0 2 2   | 1 0 2 2     | 0 1 2 0 2   |
| 1 2 0     | 0 1 0 2   | 0 0 1 1     | 1 0 2 2 0   |
|           |           |             |             |
| 1 0 1 0 0 | 1 0 1 0 1 | 1 0 1 0 1   | 1 0 1 0 1   |
| 1 1 0 0 0 | 1 1 0 0 0 | 1 1 0 0 0   | 1 1 0 0 0   |
| 0 1 1 1 1 | 0 1 1 1 0 | 0 1 1 1 0   | 0 1 1 1 1   |
| 0 1 2 0 1 | 0 1 2 0 2 | 0 1 2 0 2   | 0 1 2 2 0   |
| 1 0 2 2 0 | 1 0 2 2 0 | 1 0 2 2 2   | 1 0 2 2 2   |
|           |           |             |             |
|           |           | 1 0 1 0     | 1 0 1 0     |
| 1 0 1 0 1 | 1 0 1 0 1 | 1 1 0 0     | 1 1 0 0     |
| 1 1 0 0 0 | 1 1 0 0 1 | 0 1 1 1     | 0 1 1 1     |
| 0 1 1 1 1 | 0 1 1 1 2 | 0 1 2 0     | 0 1 2 0     |
| 0 1 2 2 1 | 0 1 2 2 0 | 1 1 1 1     | 1 1 1 1     |
| 1 0 2 2 2 | 1 0 2 2 2 | 0 0 1 1     | 0 1 2 1     |
|           |           |             |             |
| 1 0 1 0 0 | 1 0 1 0 0 | 1 0 1 0 0   | 1 0 1 0 0   |
| 1 1 0 0 1 | 1 1 0 0 1 | 1 1 0 1 1   | 1 1 0 0 1   |
| 0 1 1 1 0 | 0 1 1 1 2 | 0 1 1 1 2   | 0 1 1 1 0   |
| 0 1 2 0 1 | 0 1 2 0 1 | 0 1 2 1 2   | 0 1 2 1 1   |
| 1 1 1 1 1 | 1 1 1 1 1 | 1 1 1 2 2   | 0 1 0 1 0   |
|           |           |             |             |
|           | 1 0 1 0   |             |             |
| 1 0 1 0 0 | 1 1 0 0   | 1 0 1 0 1   | 1 0 1 0 1   |
| 1 1 0 0 1 | 0 1 1 1   | 1 1 0 0 0   | 1 1 0 0 2   |
| 0 1 1 1 2 | 0 1 2 1   | 0 1 1 1 0   | 0 1 1 1 0   |
| 0 1 2 1 1 | 0 0 1 1   | 0 1 2 1 2   | 0 1 2 1 1   |
| 0 1 0 1 2 | 1 0 1 2   | 0 0 1 1 0   | 0 0 1 1 0   |
|           |           |             |             |
| 1 0 1 0   | 1 0 1 0   |             |             |
| 1 1 0 0   | 1 1 0 0   |             |             |
| 0 1 1 1   | 0 1 1 1   | 1 0 1 0 0 1 | 1 0 1 0 0 1 |
| 0 1 2 1   | 1 1 1 1   | 1 1 0 0 1 0 | 1 1 0 0 1 0 |
| 0 1 1 0   | 0 0 1 1   | 0 1 1 1 0 0 | 0 1 1 1 0 0 |
| 1 1 0 1   | 0 1 0 1   | 0 1 2 1 1 2 | 0 1 2 1 1 1 |

|             |             |             |             |
|-------------|-------------|-------------|-------------|
| 1 0 1 0 0 1 | 1 0 1 0 0 1 | 1 0 1 0 0 1 | 1 0 1 0 0 1 |
| 1 1 0 0 1 0 | 1 1 0 0 1 0 | 1 1 0 0 1 0 | 1 1 0 0 1 0 |
| 0 1 1 1 2 0 | 0 1 1 1 2 0 | 0 1 1 1 1 2 | 0 1 1 1 0 2 |
| 0 1 2 1 1 2 | 0 1 2 1 1 1 | 0 1 2 1 0 0 | 0 1 2 1 2 2 |

|           |             |               |         |
|-----------|-------------|---------------|---------|
| 1 0 1 0 1 |             |               | 1 0 1 0 |
| 1 1 0 0 0 | 1 0 1 0 0 1 |               | 1 1 0 0 |
| 0 1 1 1 0 | 1 1 0 0 1 0 | 1 0 1 0 1 1 1 | 0 1 1 0 |
| 1 1 1 1 1 | 0 1 1 1 0 0 | 1 1 0 1 0 1 2 | 0 1 2 1 |
| 0 0 1 1 1 | 1 1 1 1 1 1 | 0 1 1 2 2 1 0 | 1 0 2 2 |

|         |         |         |         |
|---------|---------|---------|---------|
| 1 0 1 0 | 1 0 1 0 | 1 0 1 0 | 1 0 1 0 |
| 1 1 0 0 | 1 1 0 0 | 1 1 0 0 | 1 1 0 1 |
| 0 1 1 0 | 0 1 1 1 | 0 1 1 1 | 0 1 1 0 |
| 0 1 2 1 | 0 1 2 1 | 0 1 2 1 | 0 1 2 2 |
| 1 0 2 1 | 1 0 2 2 | 1 0 2 1 | 1 0 2 2 |

|         |         |           |           |
|---------|---------|-----------|-----------|
| 1 0 1 0 | 1 0 1 0 |           |           |
| 1 1 0 0 | 1 1 0 1 | 1 0 1 0 1 | 1 0 1 0 1 |
| 0 1 1 1 | 0 1 1 2 | 1 1 0 0 2 | 1 1 0 0 2 |
| 0 1 2 1 | 0 1 2 1 | 0 1 1 1 0 | 0 1 1 1 2 |
| 1 1 1 2 | 1 1 1 2 | 0 1 2 1 2 | 0 1 2 1 0 |

|           |           |           |           |
|-----------|-----------|-----------|-----------|
| 1 0 1 0 1 | 1 0 1 0 1 | 1 0 1 0 1 | 1 0 1 0 1 |
| 1 1 0 0 1 | 1 1 0 0 1 | 1 1 0 1 1 | 1 1 0 1 0 |
| 0 1 1 1 0 | 0 1 1 1 0 | 0 1 1 0 2 | 0 1 1 2 2 |
| 0 1 2 1 2 | 0 1 2 1 1 | 0 1 2 2 2 | 0 1 2 0 0 |

|           |         |         |           |
|-----------|---------|---------|-----------|
|           | 1 0 1 0 | 1 0 1 1 |           |
| 1 0 1 0 1 | 1 1 0 0 | 1 1 0 1 | 1 0 1 1 1 |
| 1 1 0 1 1 | 0 1 1 1 | 0 1 1 2 | 1 1 0 1 2 |
| 0 1 1 1 0 | 1 1 2 1 | 1 1 2 2 | 0 1 1 2 1 |
| 0 1 2 0 1 | 1 2 1 1 | 1 2 1 2 | 1 1 2 2 0 |

1 0 1 0 0  
 1 1 0 0 1  
 0 1 1 1 0  
 1 1 1 2 2

## APPENDIX B

For interested readers we add a source listing of the MACEK procedure we have used to generate our results in Theorem 5 and in Table 3.

```

# Before starting the procedure, create files "bw3-gfX-" containing
# the starting list of matroids to generate from, and "bw3-gfX+exc"
# containing extra excluded minors for bwidth3 over other fields.
# Then run a sequence of commands like these:
# macek '&bw3excg gfX bw3 '
# macek '&bw3excg gfX bw3 b'
# ...
# macek '&bw3excg gfX bw3 bbb... '
# Those will generate the excluded minors step-by-step,
# storing them to "bw3-gfX-b..b-exc".
@subd-param1 "gf3"
@subd-param2 "bw3"
@subd-param3 ""
@subd-param4 "b"
!pfield $param1
@sub-usefilen ${param2}-${param1}
@sub-usefilenb ${usefilen}-${param3}
@sub-exceextra ${usefilen}+exc
@sub-treeall ${usefilenb}-all
@sub-listin ${usefilenb}
@sub-list3out ${usefilenb}${param4}
@sub-list4out ${usefilenb}${param4}-4
@sub-list4outn ${list4out}n
@sub-excllist ${listin}-exc
@sub-excllistout ${list3out}-exc
@sub-excluded "(((S)(S)|)"
@sub-excludedin "(((1)("
@sub-excludedout "(((2)("
{
@name "bw3excg-w"
@comment "bw3excg (over $param1) working subframe:"
{
@name "exc-known"
@comment "known bw3 excl minors - extra, smaller, and new (generated)"
{
@name $exceextra
!quiet
!iffile "$exceextra"
!skip 1
!skip 4
!read $exceextra
!filx-isompair ((s))
!pfield $param1
!represgen "((s)" allq >((0t))
}{

```

```

!quiet
!pfield $param1
!iffile "$exclist"
!mread $exclist >((0t))
}{ }
}{
@name extens1
@comment "all new ${param4}-extensions of input [${listin}]..."
}{
@name e-bwidth4
@comment "those generated with bwidth 4 get here:"
}{
@name e-bwidth4n
@comment "those new excl-minors with bwidth 4 get here:"
}{
@name e-bwidth3
@comment "those next with bwidth 3 get here:"
}}
@sub-input "((S))"
{
@inputpf $param1
<${listin}
@comment "this is the starting set of matroids $listin:"
}
@sub-gener3 "((4)("
@sub-generall "((1)("
@sub-gener4bw "((2)("
@sub-gener4n "((3)("
@extinherit ext-forbid
!extend b $input >${generall}(0t)|
!move ${generall}S| >${gener3}(0t)|
!rex-bwidth3 ${gener3}S|
!move ^1 >${gener4bw}(0t)|
!writetreeto ${list3out} ${gener3}T|
!iflist 0 "<" ${gener4bw}S|
!writetreeto ${list4out} ${gener4bw}T|
!move ${gener4bw}S| >${gener4n}(0t)|
!filx-minor ${gener4n}s| $excluded
!iflist 0 "<" ${gener4n}S|
!writetreeto ${list4outn} ${gener4n}T|
!move ${excludedin}S| >$excludedout(0t)|
!move ${gener4n}S| >$excludedout(0t)|
!iflist 0 "<" ${excludedout}S|
!writetreeto ${exclistout} ${excludedout}T|
!writetreeto ${treeall} (T)

```

**ORBITAL STRUCTURE OF THE DERIVATION  
OPERATOR ON A CERTAIN SEMIRING  
OF NONSINGULAR COMPLEX MATRICES**

JIŘINA NOVOTNÁ AND JAN CHVALINA

ABSTRACT. We consider a special semiring of complex matrices with real and imaginary parts formed by positive nonsingular matrices taken from sets of pairwise commuting matrices. We describe an orbital structure of a certain transformation of the mentioned semiring satisfying rules of derivation for sum and product.

PRELIMINARIES

Matrices with nonnegative or positive elements [2, 4, 10], the systematic study of which dates back to G. Frobenius (1912), belong to important mathematical tools of modelling especially in the theory of stochastic processes (modelling of Markoff processes), in mathematical economy and elsewhere. In the theory of ordinary differential equations the types of equations solutions of which and systems of differential equations are expressed by linear combinations of products of elementary functions and exponential functions or vector functions and exponential functions of functional matrices. Considering more details, let us remind the Floquet theorem [8] concerning systems of ordinary linear differential equations with periodical coefficients, which says that if  $U$  is the standard matrix of the Cauchy problem  $x' = A(t)x, x'(0) = \xi$  then there exists a continuously differentiable nonsingular  $n \times n$  matrix function  $P$  and an  $n \times n$  constant matrix  $R$ , such that function  $U(t)$  can be represented by the ordered pair of matrix functions  $[P(t), R(t)]$ . Calculations rules considered in this paper are motivated by calculations of these ordered pairs, e. g.  $[P_1(t), R_1(t)], [P_2(t), R_2(t)]$  can be added whenever  $R_1(t) = R_2(t)$ ; in the opposite case the sum of corresponding pair is substituted by an ideal element, whereas the usual product of the above pairs is the pair  $[P_1(t)P_2(t), R_1(t) + R_2(t)]$ . In connection with papers [5, 10] and monography [18, Chap. I.] we will analyze the orbital structure of a special differential operator defined on a certain semiring of complex matrices  $M = A + iB$ , where  $A, B$  are square nonsingular matrices of order  $n \geq 2$  with entirely positive elements (*i.e.* positive matrices). The considered

---

*2000 Mathematics Subject Classification.* Primary: 15A30; Secondary: 08A60, 13N15.

*Key words and phrases.* nonsingular complex matrices, semiring derivation operator, orbital structure of mapping, mono-unity algebra.

Received 29. 10. 2002; Accepted 21. 9. 2004

Authors are indebted to M. Grendár for his suitable comments.

semiring structure can be defined on more general carrier set formed by all complex matrices with square positive real and imaginary parts.

A mono-unary algebra (called also an unar) is a pair  $(L, f)$ , where  $L$  is a set and  $f : L \rightarrow L$  is a mapping [6, 7, 11-14]. If  $S \subseteq L$  such that  $f(S) \subseteq S$  then  $(S, f|_S)$  is called a subalgebra of the algebra  $(L, f)$ . An algebra  $(L, f)$  is said to be connected whenever for any pair  $a, b \in L$  of its elements there exists a pair of non-negative integers  $m, n \in \mathbb{N}_0$  such that  $f^m(a) = f^n(b)$ ; where  $f^m$  is the  $m$ -th iteration of the map  $f$ . A maximal (with respect to the set inclusion) subalgebra  $(S, \varphi)$  of a mono-unary algebra  $(L, f)$  is termed as a component of  $(L, f)$ . If  $\{(S_\gamma, \varphi_\gamma); \gamma \in \Gamma\}$  is a collection of all components of the unar  $(L, f)$ , we write

$$(L, f) = \sum_{\gamma \in \Gamma} (S_\gamma, \varphi_\gamma).$$

In fact  $\varphi_\gamma$  is the restriction of  $f : L \rightarrow L$  onto the subset  $S \subseteq L$ .

By a semiring we mean an algebra  $(S, +, \cdot)$ , where  $(S, +)$  is a commutative semigroup,  $(S, \cdot)$  is a semigroup and  $a \cdot (b + c) = a \cdot b + a \cdot c$ ,  $(a + b) \cdot c = a \cdot c + b \cdot c$  for any triad  $a, b, c \in S$ , *i. e.* both distributive laws are satisfied [5].

Denote by  $Matr_n(\mathbb{R}^+)$  the semiring (with respect to usual operations of addition and matrix multiplication) of all square matrices over  $\mathbb{R}^+$  (the set of all positive real numbers) of order  $n \geq 2$

It is convenient to deal with complex matrices instead of pairs of real matrices. Algebraic differential structures form an important transfer between algebraic structures and structures of mathematical analysis. We denote by

$$\mathcal{M} = \{M; M = A + iB; A, B \in Matr_n(\mathbb{R}^+) \cup \{O, iI\},$$

where  $O$  is the zero matrix and  $I$  the unit matrix, both of the order  $n$ . Let us denote  $\mathcal{M}^+ = \mathcal{M} - \{O, iI\}$ .

We define two binary operations  $\oplus, \odot$  on the set  $\mathcal{M}$ , which are derived from the calculus of solution sets of linear ordinary homogeneous differential equations or from properties of exponential function of matrices. For any pair of matrices  $M_1, M_2 \in \mathcal{M}^+$  where  $M_k = A_k + iB_k$ ;  $k = 1, 2, \dots$

$$M_1 \oplus M_2 = A_1 + A_2 + iB \quad \text{if } B_1 = B_2 = B, \quad (1)$$

$$M_1 \oplus M_2 = iI \quad \text{if } B_1 \neq B_2. \quad (2)$$

For  $M \in \mathcal{M}$  arbitrary we set

$$M \oplus O = O \oplus M = M, \quad (3)$$

$$M \oplus iI = iI \oplus M = iI. \quad (4)$$

Further we define for any pair  $M_1, M_2 \in \mathcal{M}^+$

$$M_1 \odot M_2 = A_1 A_2 + i(B_1 + B_2), \quad (5)$$

$$M \odot O = O \odot M = O \quad (6)$$

for any  $M \in \mathcal{M}$  and

$$M \odot iI = iI \odot M = iI \quad (7)$$

for any matrix  $M \in \mathcal{M} - \{O\}$ .

**Lemma 1.** The pair  $(\mathcal{M}, \oplus)$  is a commutative monoid.

*Proof.* We prove first, that the operation  $\oplus$  is commutative in the set  $\mathcal{M}^+$  and also in the set  $\mathcal{M}$ . Let  $M_1, M_2$  be matrices in  $\mathcal{M}^+$ , such that

- a)  $B_1 = B_2 = B$ ,  
then  $M_1 \oplus M_2 = A_1 + A_2 + iB = A_2 + A_1 + iB = (A_2 + iB_2) + (A_1 + iB_1) = M_2 \oplus M_1$ .
- b)  $B_1 \neq B_2$ ,  
then  $M_1 \oplus M_2 = (A_1 + iB_1) + (A_2 + iB_2) = iI = (A_2 + iB_2)(A_1 + iB_1) = M_2 \oplus M_1$ .
- c) If any of the matrices  $M_1, M_2$  is equal to the zero matrix or to the matrix  $iI$  then commutativity follows from (3) a (4).

The operation  $\oplus$  is thus commutative and we will use this property in the proof of associativity.

- a) Let  $M_k = A_k + iB_k$  for  $k \in \{1, 2, 3\}$  are matrices from  $\mathcal{M}^+$ , *i. e.* :
    - $\alpha$ ) if  $B_1 = B_2 = B_3 = B$ , then  $(M_1 \oplus M_2) \oplus M_3 = (A_1 + A_2 + iB) \oplus (A_3 + iB_3) = A_1 + A_2 + A_3 + iB = (A_1 + iB) \oplus (A_2 + A_3 + iB) = M_1 \oplus (M_2 \oplus M_3)$ ,
    - $\beta$ ) if  $B_1 = B_2 = B \neq B_3$ , then  $(M_1 \oplus M_2) \oplus M_3 = (A_1 + A_2 + iB) \oplus (A_3 + iB_3) = iI = (A_1 + iB) \oplus iI = M_1 \oplus (M_2 \oplus M_3)$ ,
    - $\gamma$ ) if  $B_1 \neq B_2 \neq B_3 \neq B_1$ , then  $(M_1 \oplus M_2) \oplus M_3 = ((A_1 + iB_1) \oplus (A_2 + iB_2)) \oplus (A_3 + iB_3) = iI \oplus (A_3 + iB_3) = iI = (A_1 + iB_1) \oplus iI = (A_1 + iB_1) \oplus ((A_2 + iB_2) \oplus (A_3 + iB_3)) = M_1 \oplus (M_2 \oplus M_3)$ .
  - b) Let  $M_1, M_2$  be any matrices from  $\mathcal{M}$  and
    - $\alpha$ ) if matrix  $M_3$  is zero matrix, then  $(M_1 \oplus M_2) \oplus M_3 = (M_1 \oplus M_2) \oplus O = M_1 \oplus M_2 = M_1 \oplus (M_2 \oplus O) = M_1 \oplus (M_2 \oplus M_3)$ ,
    - $\beta$ ) if  $M_3 = iI$ , then  $(M_1 \oplus M_2) \oplus M_3 = (M_1 \oplus M_2) \oplus iI = iI = M_2 \oplus iI = M_1 \oplus (M_2 \oplus iI) = M_1 \oplus (M_2 \oplus M_3)$ .
- The neutral element is matrix  $O$  by (3).  $\square$

**Lemma 2.** The pair  $(\mathcal{M}, \odot)$  is a (noncommutative) semigroup with zero  $O$ .

*Proof.* The operation  $\odot$  is noncommutative, because multiplication of square matrices  $n \times n$  for  $n \geq 2$  is noncommutative.

Let us prove that the operation  $\odot$  is associative.

- a) Let  $M_1, M_2, M_3$  be square matrices from  $\mathcal{M}^+$ . Then  $(M_1 \odot M_2) \odot M_3 = (A_1 A_2 + i(B_1 + B_2)) \odot M_3 = (A_1 A_2 + i(B_1 + B_2)) \odot (A_3 + iB_3) = (A_1 A_2) A_3 + i((B_1 + B_2) + B_3) = A_1(A_2 A_3) + i(B_1 + (B_2 + B_3)) = M_1 \odot ((A_2 A_3) + i(B_2 + B_3)) = M_1 \odot (M_2 \odot M_3)$ .
  - b) If at least one of matrices  $M_1, M_2, M_3 \in \mathcal{M}$  is a zero matrix, then:  $(M_1 \odot M_2) \odot M_3 = O = M_1 \odot (M_2 \odot M_3)$ .
  - c) Let  $M_1, M_2, M_3 \in (M)$ ,  $M_1, M_2, M_3 \neq O$  and at least one of matrices  $M_1, M_2$  equal to  $iI$ . Then  $(M_1 \odot M_2) \odot M_3 = iI \odot M_3 = iI = M_1 \odot (M_2 \odot M_3)$ .
  - d) Let  $M_1, M_2 \neq O$ ,  $M_1, M_2 \in \mathcal{M}$  and  $M_3 = iI$ . Then  $(M_1 \odot M_2) \odot M_3 = (M_1 \odot M_2) \odot iI = iI = (M_1 \odot iI) = M_1 \odot (M_2 \odot iI) = M_1 \odot (M_2 \odot M_3)$ .
- According to (6) is  $O$  zero.  $\square$

**Theorem 3.** The triad  $(\mathcal{M}, \oplus, \odot)$  is a noncommutative semiring.

*Proof.* By Lemma 1 the structure  $(\mathcal{M}, \oplus)$  is a commutative monoid and according to Lemma 2  $(\mathcal{M}, \odot)$  is a noncommutative semigroup, so we need to prove the validity of distributive laws:

$$M_1 \odot (M_2 \oplus M_3) = (M_1 \odot M_2) \oplus (M_1 \odot M_3),$$

$$(M_1 \oplus M_2) \odot M_3 = (M_1 \odot M_3) \oplus (M_2 \odot M_3).$$

a) Suppose  $M_2, M_3 \in \mathcal{M}$ ,  $B_2 = B_3$  and

$\alpha$ )  $M_1$  is a matrix from the set  $\mathcal{M}^+$ . First we prove the left distributive law.

$$\begin{aligned} M_1 \odot (M_2 \oplus M_3) &= (A_1 + iB_1) \odot ((A_2 + iB) + (A_3 + iB)) = (A_1 + iB_1) \odot \\ &(A_2 + A_3 + iB) = A_1(A_2 + A_3) + i(B_1 + B) = A_1A_2 + A_1A_3 + i(B_1 + B) = \\ &(A_1A_2 + i(B_1 + B_2)) \oplus ((A_1A_3 + i(B_1 + B))) = ((A_1 + iB_1) \odot (A_2 + iB)) \oplus \\ &((A_1 + iB_1) \odot (A_3 + iB)) = (M_1 \odot M_2) \oplus (M_1 \odot M_3). \end{aligned}$$

Then we prove the right distributive law:  $(M_2 \oplus M_3) \odot M_1 = ((A_2 + iB) \oplus (A_3 + iB)) \odot (A_1 + iB_1) = (A_2 + A_3 + iB) \odot (A_1 + iB_1) = (A_2 + A_3)A_1 + i(B + B_1) = A_2A_1 + A_3A_1 + i(B + B_1) = (A_2A_1 + i(B + B_1)) \oplus (A_3A_1 + i(B + B_1)) = ((A_2 + iB) \odot (A_1 + iB)) \oplus ((A_3 + iB) \odot (A_1 + iB)) = (M_2 \odot M_1) \oplus (M_3 \odot M_1).$

$\beta$ )  $M_1$  is a zero matrix.

Then:  $M_1 \odot (M_2 \oplus M_3) = O \odot (M_2 \oplus M_3) = O \odot ((A_2 + iB) \oplus (A_3 + iB)) = O \odot (A_2 + A_3 + iB) = O = O \oplus O = (O \odot M_2) \oplus (O \odot M_3) = (M_1 \odot M_2) \oplus (M_1 \odot M_3).$

$\gamma$ ) If  $M_1 = iI$ .

Then:  $M_1 \odot (M_2 \oplus M_3) = iI \odot (M_2 \oplus M_3) = iI \odot ((A_2 + iB) + (A_3 + iB)) = iI \odot (A_2 + A_3 + iB) = iI = iI \oplus iI = (iI \odot M_2) \oplus (iI \odot M_3) = (M_1 \odot M_2) \oplus (M_1 \odot M_3).$

Cases b) – f) can be proved similarly.

b) Consider matrices  $M_2, M_3$ , such that  $B_2 = B_3$ .

c) Exactly one of matrices  $M_2, M_3$  is a zero matrix and the other is from  $\mathcal{M}^+$ .

d) Exactly one of matrices  $M_2, M_3$  is a zero matrix and the other is  $iI$ .

e) Matrices  $M_2, M_3$  are zero matrices and  $M_1 \in \mathcal{M}^+$ .

f) At least one from matrices  $M_2, M_3$  is equal  $iI$ .  $\square$

Now, we define a mapping  $d : \mathcal{M} \rightarrow \mathcal{M}$  by

$$d(M) = AB + iB$$

for any  $M \in \mathcal{M}^+$  where  $M = A + iB$  and  $d(O) = O, d(iI) = iI$ .

It is easy to see (cf. paper [10]) that the mapping  $d$  is an endomorphism of the additive monoid  $(\mathcal{M}, \oplus)$ , *i. e.*

$$d(M_1 \oplus M_2) = d(M_1) \oplus d(M_2)$$

for any pair of matrices  $M_1, M_2 \in \mathcal{M}$ . Further, let  $\mathcal{N} \subset (M)^+$  be a non-empty subset of complex matrices from set  $\mathcal{M}^+$  with pairwise commuting real and imaginary parts of those, *i. e.* for every pair  $M_1, M_2 \in \mathcal{N}, M_k = A_k + iB_k, k = 1, 2$  we have  $XY = YX$  for any pair  $X, Y \in \{A_1, B_1, A_2, B_2\}$ . We will denote by  $C(\mathcal{N})$  the subalgebra of  $(\mathcal{M} - \{iI\}, \oplus, \odot)$  and  $C_1(\mathcal{N}) = C(\mathcal{N}) \cup \{iI\}$  with binary operations  $\oplus, \odot$  extended as above by  $M \oplus iI = iI \oplus M = iI, M \odot iI = iI \odot M = iI$  for any  $M \in C(\mathcal{N})$ . Consequently  $(C_1(\mathcal{N}), \oplus, \odot)$  is a semiring formed by pairwise commuting matrices. There is proven in [10] that the above defined operator  $d$  restricted on  $C_1(\mathcal{N})$ , also satisfies the rule for derivation of a product, *i. e.*

$$d(M_1 \odot M_2) = (d(M_1) \odot M_2) \oplus (M_1 \odot d(M_2))$$

for any pairs  $M_1, M_2 \in C_1(\mathcal{N})$ . Moreover, the Leibniz formula

$$d^n(M_1 \odot M_2) = \sum_{k=0}^n \oplus \binom{n}{k} (d^{n-k}(M_1) \odot d^k(M_2)),$$

where the symbol  $\sum_{k=0}^n \oplus$  is a natural extension of sum onto given finite system of matrices with arbitrary  $n \in \mathbb{N}$  is valid.

ORBITAL STRUCTURE OF THE DERIVATION  
 $d$  ON A CERTAIN SUBSEMIRING OF  $C(\mathcal{N})$

Now we describe the structure obtained by the above defined operator  $d$  which will be restricted onto a subsemiring of  $C(\mathcal{N})$  formed by matrices with nonsingular real and imaginary parts (with the exception of the zero matrix). So, let us denote by  $\mathcal{M}_{reg}$  the subset of all matrices  $A + iB \in C(\mathcal{N})$  such that  $\det A \neq 0 \neq \det B$ , *i. e.*  $A, B$  are nonsingular and further let us denote  $\mathcal{M}_{reg} = \mathcal{M} \cup \mathcal{O}$ . (Note that  $iI \in \mathcal{M}_{reg}$  as well.) Evidently with respect to binary operations  $\oplus, \odot$ , the set  $\mathcal{M}_{reg}$  is a semiring. Let us consider the usual quasi-ordering  $\leq$ , *i. e.* a reflexive and transitive binary relation on the set  $\mathcal{M}_{reg}$  defined by the rule:

For a pair  $M_1, M_2 \in \mathcal{M}_{reg}$  we set

$$M_1 \leq_d M_2$$

whenever  $M_2 = d^n(M_1)$  for some  $n \in \mathbb{N}_0$ .

In our case the relation  $\leq_d$  is also antisymmetric. Indeed, let us suppose  $M_1 \leq_d M_2, M_2 \leq_d M_1$  for a suitable pair of matrices  $M_1 = A_1 + iB_1, M_2 = A_2 + iB_2$  from  $\mathcal{M}_{reg}^*, \mathcal{O} \neq M_k \neq iI$  for  $k = 1, 2$ . Then there exist integers  $m, n \in \mathbb{N}_0$  such that  $M_2 = d^n(M_1), M_1 = d^m(M_2)$ , thus  $M_1 = d^{m+n}(M_1)$ , consequently

$$A_1 + iB_1 = A_1 B^{m+n} + iB_1,$$

which implies  $B_1^{m+n} = I$ . Since  $B_1$  is a matrix with positive entires we have  $B_1^{m+n} \neq I$ , therefore  $d^n(M) \neq M$  for each positive integer  $n$  and any matrix  $M \in \mathcal{M}_{reg}^* - \{O, iI\}$ . Thus  $M_1 = M_2$  and we obtain the following assertion.

**Lemma 4.** The relation  $\leq_d$  is an ordering of the set  $\mathcal{M}_{reg}^*, i. e.$   $(\mathcal{M}_{reg}^*, \leq_d)$  is an ordered set.

It is clear that the poset  $(\mathcal{M}_{reg}^*, \leq_d)$  has two isolated points  $(O, iI)$ . We show that the poset satisfies the descending chain condition. Moreover, we describe its structure in the following theorem. Let  $(\mathbb{N}, \leq)$  be the chain of all positive integer with the usual natural ordering.

**Theorem 5.** Let  $\Gamma$  be an antichain of cardinality  $2^{\aleph_0}$ . The poset  $(\mathcal{M}_{reg}^*, \leq_d)$  is a cardinal sum of a two-element antichain and a set of cardinality  $2^{\aleph_0}$  of countable chains isomorphic to  $(\mathbb{N}, \leq)$ , more precisely

$$(\mathcal{M}_{reg}^*, \leq_d) = G + \sum_{\gamma \in \Gamma} (K_\gamma, \leq_\gamma),$$

where  $G$  is a two-elements antichain and  $(K_\gamma, \leq_\gamma) \cong (\mathbb{N}, \leq)$  for any  $\gamma \in \Gamma$ .

*Proof.* Let us show first that the mapping  $d : \mathcal{M}_{reg}^* \rightarrow \mathcal{M}_{reg}^*$  is injective. Suppose on the contrary that  $d(M_1) = d(M_2)$ , where  $M_k = A_k + iB_k \in \mathcal{M}_{reg}^*, k = 1, 2$ . Then  $A_1 B_1 + iB_1 = A_2 B_2 + iB_2$  which implies  $B_1 = B_2$  and  $A_1 B_1 = A_2 B_1$ . Since  $B_1$  is a nonsingular matrix, we have  $A_1 = A_1 B_1 B_1^{-1} = A_2 B_1 B_1^{-1} = A_2$ , consequently

$M_1 = M_2$ . This fact implies that for any pair matrices  $M_1, M_2 \in \mathcal{M}_{reg}^*$  exactly one of the following cases occurs:

- a)  $M_1 \leq M_2$  or  $M_2 < M_1$ ,
- b)  $M_1, M_2$  are incomparable and the two-element set  $\{M_1, M_2\}$  possesses neither an upper bound nor a lower bound. Therefore any  $M \in \mathcal{M}_{reg}^*$  belongs to some subchain of  $(\mathcal{M}_{reg}, \leq_d)$ . Furthermore, any chain  $K_\gamma, \gamma \in \Gamma$  has the least element. Indeed, let us suppose  $M = A + iB \in \mathcal{M}_{reg}$  is an arbitrary matrix belonging to the chain  $K_\gamma$ . Since  $d(X + iY) = XY + iY$ , for any matrix  $X + iY \in \mathcal{M}_{reg}$ , we have

$$A(B^{-1})^n + iB <_d A(B^{-1})^{n-1} + iB <_d \dots <_d AB^{-1} + iB,$$

thus there exists a positive integer  $n \in \mathbb{N}$  such that

$$A(B^{-1})^n + iB \in \mathcal{M}_{reg}$$

and

$$A(B^{-1})^{n+1} + iB \notin \mathcal{M}_{reg},$$

thus the matrix  $A(B^{-1})^n + iB$  is the least element of the chain  $K_\gamma$ . The proof is complete.  $\square$

From the above proved theorem there follows immediately the following result describing the operator  $d : \mathcal{M}_{reg}^* \longrightarrow \mathcal{M}_{reg}^*$  in terms of mono-unary algebras theory see [6, 11, 13]. We denote by  $\nu : \mathbb{N} \longrightarrow \mathbb{N}$  the successor function  $\nu(n) = n + 1$ , *i. e.*  $(\mathbb{N}, \nu)$  is the Peano-algebra of all positive integers. Then we have

**Theorem 6.** Denote by  $\Gamma_{min}$  the set of all minimal elements of the poset  $(\mathcal{M}_{reg}, \leq_d)$ . Then

$$(\mathcal{M}_{reg}^*, d) = (\{O, iI\}, id) + \sum_{\gamma \in \Gamma_{min}} K_\gamma, d_\gamma,$$

where  $d_\gamma$  is the restriction of  $d$  onto  $K_\gamma$  for any  $\gamma \in \Gamma_{min}$  and every component  $(K_\gamma, d_\gamma), (\gamma \in \Gamma)$  is isomorphic to the Peano-algebra  $(\mathbb{N}, \nu)$ .

#### REPRESENTATIONS OF THE MONO-UNARY ALGEBRA $(\mathcal{M}_{reg}^*, d)$

Using simple tools we construct in this paragraph mono-unary algebras isomorphic to the algebra  $(\mathcal{M}_{reg}^*, d)$ . Thus certain representation theorems concerning  $(\mathcal{M}_{reg}^*, d)$  will be obtained. Let  $\infty$  be a symbol which does not belong to the set  $\mathbb{R}$  of all real numbers with the usual meaning, *i. e.*  $r < \infty$  for all  $r \in \mathbb{R}$ . Let us denote  $\bar{J} = \langle 2, \infty \rangle \cup \{\infty\}$ , where  $\langle 2, \infty \rangle = \{r \in \mathbb{R}; 2 \leq r\}$ . We define a function  $\varphi : \bar{J} \longrightarrow \bar{J}$  by the rule  $\varphi(x) = 2^x$  for any  $x \in \langle 2, \infty \rangle$  and  $\varphi(t) = t$  for  $t \in \{2, \infty\}$ . We are going to construct an isomorphism  $F : (\bar{J}, \varphi) \longrightarrow (\mathcal{M}_{reg}^*, d)$  in this way: Let us put  $F(2) = O, F(\infty) = iI$ . Further, let  $\xi : (2, 4) \longleftarrow \Gamma_{min}$  be an arbitrary bijection. For arbitrary  $x \in \langle 4, \infty \rangle$  let us denote  $n(x) \in \mathbb{N}_0$  and  $x_0 \in (2, 4)$  numbers with property  $\varphi^{n(x)}(x_0) = x$ . Then we set

$$F(x) = d^{n(x)}(\xi(x_0)).$$

In particular  $F(x) = \xi(x)$  for every  $x \in (2, 4)$ .

**Lemma 7.** The mapping  $F : \bar{J} \longrightarrow \mathcal{M}_{reg}^*$  is a bijection.

*Proof.* Let us denote  $\Gamma = \mathcal{M}_{reg}^* - (\{O, iI\} \cup \Gamma_{min})$  and consider the partition of the set  $\mathcal{M}_{reg}^*$  in the form

$$\mathcal{M}_{reg}^* = \{O, iI\} \cup \Gamma_{min} \cup \Gamma.$$

If  $M = O$  or  $M = iI$  then  $F^{-1}(M) \in \{2, \infty\}$ . If  $M \in \Gamma_{min}$ , then there exists a unique  $x \in (2, 4)$  such that  $\xi(M) = x$ . Suppose  $M \in \Gamma \setminus \Gamma_{min}$ . Then also for a suitable  $x_0 \in (2, 4)$  we have  $M = d^{n(x)}(\xi(x_0))$ . Then by definition of the mapping  $F$  we obtain

$$F(\varphi^{(n(x))}(x_0)) = M, \varphi^{(n(x))}(x_0) \in \langle 2, \infty \rangle,$$

consequently the mapping  $F : \bar{J} \longrightarrow \mathcal{M}_{reg}^*$  is surjective. We show that  $F$  is also injective. Suppose  $x, y \in \bar{J}$  are reals such that  $F(x) = F(y)$ . Then either

- a)  $F(x) = F(y) \in \{O, iI\}$  or
- b)  $F(x) = F(y) \in \mathcal{M}_{reg}^*$ .

In case a) we have  $x = 2 = y$  or  $x = \infty = y$ . Suppose the case b) occurs. Let  $M_0 \in \Gamma_{min}$  and  $n$  be a nonnegative integer such that  $F(x) = F(y) = d^n(M_0)$ . Then by the definition of the mapping  $F$  we have  $F^{-1}(M_0) \in (2, 4)$  and  $\varphi^n(\xi^{-1}(M_0)) = y$ , hence  $F : \bar{J} \longrightarrow \mathcal{M}_{reg}^*$  is injective. Therefore  $F$  is a bijection.  $\square$

**Theorem 8.** The mono-ary algebra  $(\mathcal{M}_{reg}^*, d)$  is isomorphic to the mono-ary algebra  $(\bar{J}, \varphi)$ , where  $\bar{J} = \langle 2, \infty \rangle \cup \{\infty\}$ .

*Proof.* We show that the above defined mapping  $F : \bar{J} \longrightarrow \mathcal{M}_{reg}^*$  satisfies the equality

$$F \circ \varphi = d \circ F.$$

Indeed, let  $x \in \bar{J}$  be an arbitrary element such that either  $x \in \{2, \infty\}$  or  $x \in (2, 4)$ . In the first case  $x = 2$  or  $x = \infty$  which implies  $F(x) = O$  or  $F(x) = iI$ , respectively. Then

$$(F \circ \varphi)(x) = F(\varphi(x)) = F(x) = d(F(x)) = (d \circ F)(x).$$

In the second case  $\xi(x) \in \Gamma$  and since  $F(x) = \xi(x)$  we have

$$(F \circ \varphi)(x) = F(\varphi(x)) = F(2^x) = d(\xi(x)) = (d \circ F)(x).$$

Now let us suppose  $x \in (4, \infty)$ ,  $x_0 \in (2, 4)$  and  $n(x) \in \mathbb{N}$  are members such that  $x = \varphi^{n(x)}(x_0)$ . Then

$$(F \circ \varphi)(x) = F(\varphi(x)) = F(\varphi^{n(x)+1}(x_0)) = d^{n(x)+1}(\xi(x_0)) = d(F(x)) = (d \circ F)(x).$$

Since the mapping  $F$  is bijective, we get that  $F : (\bar{J}, \varphi) \longrightarrow (\mathcal{M}_{reg}^*, d)$  is an isomorphism.  $\square$

Using the mono-ary algebra  $(\bar{J}, \varphi)$  we obtain another representation theorem for the mono-ary algebra  $(\mathcal{M}_{reg}^*, d)$ . Put

$$S = ((0, 1) \times \mathbb{N}) \cup \{[0, 0], [0, 1]\}$$

and define a function  $\psi : S \longrightarrow S$  by

$$\psi([x, y]) = \begin{cases} [x, y + 1] & \text{for any pair } [x, y] \in (0, 1) \times \mathbb{N} \\ [x, y] & \text{for any } [x, y] \in \{[0, 0], [0, 1]\} \end{cases}$$

Further we define a mapping  $\Phi : S \longrightarrow \bar{J}$  in a similar way as above:  
Consider an arbitrary bijection  $\eta : (0, 1) \longrightarrow (0, 4)$  (e.g.  $\eta = 2x + 2, x \in (0, 1)$ ).  
For any pair  $[x, y] \in (0, 1) \times \mathbb{N}$  we denote by  $n(x) \in \mathbb{N}$  and  $x_0 \in (0, 1)$  numbers such  
that  $\eta^{n(x)}(x_0) = x$ . Then we define

$$\Phi([x, y]) = \varphi^{n(x)}(\eta(x_0))$$

Moreover

$$\Phi([0, 0]) = 2, \Phi([0, 1]) = \infty$$

Then we obtain the following assertion, proof of which is rather technical and similar  
to the proof of Lemma 7. Thus it can be left to the reader.

**Lemma 9.** The mapping  $\Phi : S \longrightarrow \bar{J}$  is bijection.

Now we can easily proved:

**Proposition 10.** The mapping  $\Phi : S \longrightarrow \bar{J}$  is an isomorphism of the mono-  
unary algebra  $(S, \psi)$  onto the mono-unary algebra  $(\bar{J}, \phi)$ .

*Proof.* We show that the mapping  $\Phi : S \longrightarrow \bar{J}$  is a homomorphism.  
Let  $[x, n] \in S$  be an arbitrary element. If  $[x, n] = [0, 0]$  or  $[x, n] = [0, 1]$  then  
 $\Phi([x, n]) = 2$  or  $\Phi([x, n]) = \infty$ , respectively, and we have  $(\Phi \circ \psi)([x, n]) = (\varphi \circ$   
 $\Phi)([x, n])$ . Suppose  $[x, n] \in (0, 1) \times \mathbb{N}$  is a pair and  $0 < x_0 \leq 1, n(x) \in \mathbb{N}$  are  
numbers with the property  $[x, n] = \psi^{n(x)}(x_0)$  then

$$(\Phi \circ \psi)([x, n]) = \Phi(\psi([x, n])) = \Phi(\psi^{n(x)+1}(x_0)) = \varphi^{n(x)+1}(\eta(x_0)) = \varphi(\Phi([x, n])) = (\varphi \circ \Phi)([x, n]).$$

Consequently with respect to Lemma 9 we have that  $F : (S, \psi) \longrightarrow (\bar{J}, \varphi)$  is an  
isomorphism.  $\square$

Summarizing the obtained facts (Theorem 8, Proposition 10) we can formulate  
the main result of this paragraph:

**Theorem 11.** Let  $\bar{J} = (2, \infty) \cup \{\infty\} \subset \bar{\mathbb{R}}, S = ((0, 1) \times \mathbb{N} \cup \{[0, 0], [0, 1]\}) \subset \mathbb{R} \times \mathbb{N}$   
and  $\varphi : \bar{J} \longrightarrow \bar{J}, \psi : S \longrightarrow S$  be functions defined by:

$$\varphi(x) = \begin{cases} 2^x & \text{for any } x \in (2, \infty) \\ x & \text{for any } x \in \{2, \infty\} \end{cases}$$

$$\psi([x, y]) = \begin{cases} [x, y + 1] & \text{for any } [x, y] \in (0, 1) \times \mathbb{N} \\ [x, y] & \text{for any } [x, y] \in \{[0, 0], [0, 1]\} \end{cases}$$

Then  $(\bar{J}, \varphi) \cong (\mathcal{M}_{reg}^*, d) \cong (S, \psi)$ , i. e. mono-unary algebras  $(\bar{J}, \varphi), (\mathcal{M}_{reg}^*, d), (S, \psi)$   
are mutually isomorphic.

At the end of this paragraph we present — without technical details — another  
simple representations of  $(\mathcal{M}_{reg}^*, d)$ .

Let us describe some other possible simple representations of the mono-unary  
algebra  $(\mathcal{M}_{reg}^*, d)$ . Let us denote  $X_0 = \{0, 1\} \subset \mathbb{C}$ , (where  $\mathbb{C}$  is Gaussian plane of

all complex numbers),  $X_1 = \{z = x + yi, x \in (0, 1); y \in \mathbb{N}\} \subset \mathbb{C}$  and  $X = X_0 \cup X_1$ . Let us define the following complex function:

$$f(z) = \begin{cases} z & \text{for } z \in \{0, 1\} = X_0 \\ z + i & \text{for } z \in X_1 \end{cases}.$$

Then  $(\mathcal{M}_{reg}^*, d) \cong (X, f)$ .

Furthermore, let  $Y_0 = \{0, i\}, Y_1 = \{z = x + yi, x \in \mathbb{N}, y \in (0, 1)\}; Y_1 \subset \mathbb{C}$  and  $Y = Y_0 \cup Y_1$ . We define the function  $g(z) : Y \rightarrow Y$  by the rule:

$$g(z) = \begin{cases} z & \text{for } z \in Y_0 \\ z + i & \text{for } z \in Y_1 \end{cases}.$$

Again  $(\mathcal{M}_{reg}^*, d) \cong (Y, g)$ .

Let us denote  $K = \{1\} \cup (2, \infty)$  and define a real function  $u : K \rightarrow K$  in the following way:

$$u(x) = \begin{cases} x & \text{for } x \in \{1, 2\} \\ 2x & \text{for } x \in (2, \infty) \end{cases}.$$

In this case  $(\mathcal{M}_{reg}^*, d) \cong (K, u)$ .

The main contribution of the presented paper is divided into two directions: Firstly, a differential semiring of complex matrices with positive real and imaginary parts motivated by the above remark is constructed and secondly: the structure of a mono-unary algebra determined by the constructed differential operator including its representations is clarified.

In matrix theory including its various applications the concept of a pseudo-inverse matrix plays an important role [8]. One of so called More-Penrose conditions can be expressed also in terms of the semigroup theory. More precisely, a semigroup  $(S, \cdot)$  is said to be regular, if for any  $a \in S$  there exists  $b \in S$  such that  $aba = a$  [6, 7, 15]. It is easy to see, that the endomorphism monoid  $\text{End}(\mathcal{M}_{reg}^*, d)$  is not regular. However, if we restrict our solves onto  $(\mathcal{M}_{reg}, d)$ , then it is possible to construct a certain unique extension  $(\bar{\mathcal{M}}_{reg}, \bar{d})$  of this unar such that the monoid  $\text{End}(\bar{\mathcal{M}}_{reg}, \bar{d})$  is regular. But this seems to be a topic for an additional paper.

#### REFERENCES

- [1] Bapat, R. B., *Linear Algebra and Linear Models*, 2nd ed., Springer Verlag, New York, etc., 2000.
- [2] Bellman, R., *Introduction to Matrix Analysis*, McGraw-Hill Book Company, Inc., New York–Toronto–London, 1960.
- [3] Dupač V. and Dupačová, J., *Markoff Processes*, SPN, Praha, 1980. (Czech)
- [4] Gantmacher, F. R., *Matrizentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1986.
- [5] Chvalina, J., *Fractional iterations of derivatives on a certain semiring of complex numbers*, Department Mathematics Report Series **8** (2000), University of South Bohemia, České Budějovice, 77–86..
- [6] ———, *Functional Graphs, Quasi-ordered Sets and Commutative Hypergroups*, Masaryk University, Brno, 1995.
- [7] Moučka, J., *Connected functional graphs with regular endomorphism monoids and their hypergroups*, Matematika a didaktika matematiky, Sborník prací PdF MU Brno 152, Masaryk University, Brno, 2000, pp. 53–59.
- [8] Nagy, J., *Systems of Ordinary Differential Equations*, SNTL, Prague, 1980. (Czech)
- [9] Nashed, Z., *Generalized Inverses and Applications*, Academic Press, 1976.

- [10] Novotná, J., *Applications of Matrices in Economy*, II. konf. o matematice a fyzice na vysokých školách technických, Vojenská akademie v Brně, 2002, pp. 69–74.
- [11] Novotný, M., *Über Abbildungen von Mengen*, Pacific J. Math. **13** (1963), no. 4, 1359–1369.
- [12] ———, *Commutativity of endomorphism of linear spaces*, Čas. pěst. mat. **107** (1982), 24 – 138.
- [13] ———, *Mono-unary algebras in the work of Czechoslovak mathematicians*, Arch. Math **26** (1990), Brno, 155–164.
- [14] ———, *Construction of all homomorphisms of mono-unary algebras*, Seminář OAS PřF MU, Masarykova Universita, Brno, 1995.
- [15] Skornjakov, L. A., *Unary algebras with regular endomorphism monoids*, Acta Sci. Math. **40** (1978), 375–381.
- [16] Šik, F., *Linear Algebra directed to Numerical Analysis*, Masaryk University, Brno, 1998.
- [17] Šmarda, B., *Linear Programming in Exercises*, SPN, Praha, 1983.
- [18] Targonski, G., *Topics in Iteration Theory*, Vandenhoeck et Ruprecht, Gottingen - Zurich, 1981.

DEPT. OF MATHEMATICS, FACULTY OF EDUCATION; MASARYK UNIVERSITY;  
POŘÍČÍ 31; CZ-603 00 BRNO; CZECH REPUBLIC.

E-mail: novotna@jumbo.ped.muni.cz

DEPT. OF MATHEMATICS, FACULTY OF ELEKTRICAL ENGIN. AND COMMUNICA-  
TION; BRNO UNIVERSITY OF TECHNOLOGY; TECHNICKÁ 8;  
CZ-616 00 BRNO; CZECH REPUBLIC.

E-mail: chvalina@feec.vutbr.cz

## USING TRACE TO IDENTIFY IRREDUCIBLE QUADRATIC POLYNOMIALS

ONDREJ ŠUCH

ABSTRACT. In this note we prove a way to check that a quadratic polynomial is irreducible using a trace map and state a conjecture that this method works also for higher degree polynomials

### INTRODUCTION

In explicit computer computations with finite fields it is often important to find an irreducible polynomial of a given degree. While searching for such polynomial it is crucial to have an algorithm to find out whether a given polynomial is irreducible. This problem has been considered by many authors e.g. [2], Problem 7.1. In this note we present a novel way to check whether a *quadratic* polynomial is irreducible.

Consider a quadratic polynomial

$$f(x) = x^2 - ax - b$$

over a finite field  $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$  of characteristic  $p$ . If  $f$  is an irreducible polynomial, then its splitting field  $\mathbf{E}$  is a Galois extension (for definition and general properties used here see e.g. [1]) of  $\mathbf{F}_p$  of degree 2 and cardinality  $p^2$ . The Galois group  $\Gamma = \text{Gal}(\mathbf{E}/\mathbf{F}_p)$  of this extension is of order 2, generated by Frobenius automorphism  $\text{Frob} : x \mapsto x^p$ . Its square  $\text{Frob}^2$  is the trivial automorphism of  $\mathbf{E}/\mathbf{F}_p$ , that is it fixes all elements of  $\mathbf{E}$ , so that  $x^{p^2} = x$  for all elements of  $\mathbf{E}$ .

For any element  $x$  in  $\mathbf{E}$  the sum of all elements in the orbit of  $x$  by the action of Galois group defines a linear map called trace

$$(1) \quad \text{trace}_{\mathbf{E}/\mathbf{F}_p} : x \mapsto x + \text{Frob}(x) = x + x^p.$$

Since the orbit of  $x$  is permuted by the generator of  $\Gamma$ , the image of any element under trace map in fact lies in  $\mathbf{F}_p$ . In this note we ask the reverse. Namely, assume that for any element  $x$  in the  $\mathbf{F}_p$  module  $\mathbf{F}_p[x]/f(x)$ , the trace map defined by (1) lies in  $\mathbf{F}_p$ . Does it follow that  $f$  is an irreducible polynomial?

To this end we prove the following.

---

2000 *Mathematics Subject Classification.* Primary 11T06; Secondary 12E05.

*Key words and phrases.* finite field, irreducible polynomial, algorithm.

Received 17. 8. 2004; Accepted 21. 9. 2004

**Proposition 1.**

Let  $M = \mathbf{F}[x]/f(x)$ , where  $\mathbf{F}$  is a finite field of odd characteristic  $p$  and cardinality  $q$ . Suppose that  $x + x^q$  lies in the submodule  $\mathbf{F}$  of  $M$ . Then  $f(x)$  is an irreducible polynomial.

## PROOF OF MAIN RESULT.

We start with the following lemma.

**Lemma 2.**

Let  $M = \mathbf{Z}[x]/f(x)$ . Then in  $M$  for any odd  $n \geq 3$  we can write

$$x^n = P_n(a, b)x + Q_n(a, b)$$

where  $P_n$  when considered as a polynomial in  $b$  is monic and has degree  $\frac{n-1}{2}$ .

*Proof.* We proceed by induction proving a somewhat stronger statement. Namely, we also claim that  $Q_n$  has degree  $\leq \frac{n-1}{2}$  in  $b$ . For  $n = 3$  we compute directly

$$\begin{aligned} x^3 &= x \cdot x^2 = x \cdot (ax + b) \\ &= ax^2 + bx \\ &= (ax + b)a + bx \\ &= x \cdot (a^2 + b) + ab \end{aligned}$$

Now suppose that induction hypothesis holds for an odd  $n$ . Using relation  $x^2 = ax + b$  we compute

$$\begin{aligned} x^{n+2} &= x^2 \cdot x^n = (ax + b) \cdot (P_n(a, b)x + Q_n(a, b)) \\ &= x^2 a P_n(a, b) + x(b P_n(a, b) + a Q_n(a, b)) + b Q_n(a, b) \\ &= (ax + b)a P_n(a, b) + x(b P_n(a, b) + a Q_n(a, b)) + b Q_n(a, b) \\ &= x \cdot (a^2 P_n(a, b) + b P_n(a, b) + a Q_n(a, b)) + ba P_n(a, b) + b Q_n(a, b) \end{aligned}$$

This shows existence of  $P_{n+1}$  and  $Q_{n+1}$ , explicitly

$$\begin{aligned} P_{n+1} &= a^2 P_n + b P_n + a Q_n \\ Q_{n+1} &= ba P_n + b Q_n \end{aligned}$$

By induction hypothesis

$$\begin{aligned} \deg_b(a^2 P_n) &= \frac{n-1}{2} \\ \deg_b(b P_n) &= 1 + \frac{n-1}{2} \\ \deg_b(a Q_n) &\leq \frac{n-1}{2} \end{aligned}$$

so that

$$\deg_b(P_{n+1}) = 1 + \frac{n-1}{2} = \frac{(n+2)-1}{2}.$$

and since  $bP_n$  is monic, so is  $P_{n+1}$ . Similarly, it follows that  $\deg_b(Q_{n+1}) \leq \frac{(n+2)-1}{2}$  completing induction step.  $\square$

*Proof of Proposition 1.* Let  $p$  be an odd prime, and let us now count the number of points over  $\mathbf{F}$  on the affine curve  $C$  defined by  $P_q(x, y) = 0$ . On one hand, for any fixed  $x$  by Lemma 2 there are at most  $\frac{q-1}{2}$  values of  $y$  such that  $P_q(x, y) = 0$ . Since there are  $q$  possible values of  $a$ , the number of  $\mathbf{F}$ -valued points is  $\leq \frac{q(q-1)}{2}$ .

On the other hand, if  $f(x)$  is irreducible then  $P_q(x, y) = 0$  by properties of trace discussed in the beginning. The number of monic quadratic irreducible polynomials equals to the difference of numbers of monic polynomials over  $\mathbf{F}$  and those which are reducible. The former number is obviously  $q^2$ , the latter is  $q + \binom{q}{2}$ . It follows that the number of irreducible quadratic polynomials is  $\frac{q(q-1)}{2}$  and hence the number of  $\mathbf{F}$ -valued points on  $C$  is  $\geq \frac{q(q-1)}{2}$ .

Taking into account both bounds, it follows that the number of  $\mathbf{F}$ -valued points on  $C$  is precisely  $\frac{q(q-1)}{2}$  and they are in one-to-one correspondence with irreducible quadratic polynomials.  $\square$

#### COMPARISON WITH OTHER ALGORITHMS

Of course, there are many other algorithms to check if a given quadratic polynomial is irreducible. For instance, in [2, Theorem 7.5] an algorithm is shown with complexity  $O(\log q)$  (of operations in  $\mathbf{F}$ ) to find out if a given polynomial is irreducible. Using [2, Algorithm 5.2] we can compute the trace in  $O(\log q)$  steps and conclude that our algorithm also can be carried out in  $O(\log q)$  steps.

However, for the special case of checking irreducibility of quadratic polynomial there is a more direct algorithm, which we now explain. Assuming the characteristic of  $\mathbf{F}$  is  $\neq 2$ , we can write

$$x^2 - ax - b = (x - a/2)^2 - b - \frac{a^2}{4} = 0$$

so that  $f(x)$  has solution if and only if  $b + \frac{a^2}{4}$  is a square in  $\mathbf{F}$ , which happens if and only if the discriminant  $\Delta(f) = a^2 + 4b$  is a square in  $\mathbf{F}$ .

If we denote by  $n$  the degree  $\deg(\mathbf{F} : \mathbf{F}_p)$ , then one defines the norm map  $N_{\mathbf{F}/\mathbf{F}_p}(x)$

$$N_{\mathbf{F}/\mathbf{F}_p}(x) := x \cdot x^p \cdots x^{p^{n-1}} = x^{\frac{p^n-1}{p-1}}.$$

It is a homomorphism of the multiplicative group  $\mathbf{F}^\times$  of invertible elements in  $\mathbf{F}$  to  $\mathbf{F}_p^\times$ . Composing the norm map with Legendre symbol on  $\mathbf{Z}/p\mathbf{Z}$

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

we obtain a multiplicative map  $\chi_2 : \mathbf{F}^\times \rightarrow \{-1, 1\}$  given by

$$(2) \quad \chi_2(a) := \left(\frac{N_{\mathbf{F}/\mathbf{F}_p}(a)}{p}\right) = a^{\frac{p^n-1}{2}}$$

The group  $\mathbf{F}^\times$  is cyclic, of order  $p^n - 1$  [1, Theorem 12.3]. Thus  $a$  in  $\mathbf{F}$  is a square if and only if  $\chi_2(a) \neq -1$ . Since exponentiation to  $k$ -th power takes  $O(\log(k))$  operations, checking whether  $\Delta(f)$  is square takes using (2) at most  $O(\log q)$  operations. Thus even this specialized algorithm, taking advantage of the fact that  $f(x)$  is of degree 2, does not lead to (an asymptotic) speed up of finding out if the given polynomial is irreducible.

#### CONCLUSION

In conclusion we make the following conjecture concerning higher degree polynomials.

#### **Conjecture 3.**

A polynomial  $f(x)$  is irreducible over  $\mathbf{F}$  if and only if the trace map is of rank 1.

#### REFERENCES

- [1] D.J.H. Garling, *A Course in Galois Theory*, Cambridge University Press, 1986.
- [2] Victor Shoup, J. von zur Gathen, *Computing Frobenius maps and factoring polynomials*, Computational Complexity, vol. 2, 1992, pp. 187-224, Extended abstract in Proc. 24th ACM Symposium on Theory of Computing, pp. 97-105, available on <http://shoup.net/papers>.

INSTITUTE OF MATH. AND COMP.SCIENCE; MATHEMATICAL INSTITUTE OF SAS,  
SEVERNÁ 5, SK-974 01 BANSKÁ BYSTRICA, SLOVAKIA.

E-mail: [ondrejs@savbb.sk](mailto:ondrejs@savbb.sk)

## UPPER BOUND FOR QUEUE NUMBER OF SHUFFLE-EXCHANGE GRAPH

LUBOMÍR TÖRÖK

ABSTRACT. Shuffle-Exchange network has some good properties in parallel data processing. Its graph abstraction called Shuffle-Exchange graph is well known in the area of VLSI design. The concept of queue number is the abstraction of some problems from computer science, such as the design of fault-tolerant processor arrays, a problem of sorting with parallel queues, and a problem of scheduling parallel processors. In this paper we prove that Shuffle-Exchange graph has a 3-queue layout, while it is known that at least 2 queues are necessary. This value provides upper bound for queue number of Shuffle-Exchange graph.

### INTRODUCTION

#### Shuffle-Exchange Graph

**Definition 1.** The  $d$ -dimensional shuffle-exchange graph ( $SE_d$ ) has  $2^d$  nodes. Each vertex is numbered by unique binary string of length  $d$ . The edges are defined as follows. Vertex represented by binary string  $\alpha a$ , where  $\alpha \in \{0, 1\}^{(d-1)}$  and  $a \in \{0, 1\}$ , is connected with vertex  $\alpha \neg a$  and  $a\alpha$  (where  $\neg a$  is negation of  $a$ ). Edges directions, multiple edges and loops are ignored.

The edges between vertices  $\alpha a$  and  $\alpha \neg a$  are called *exchange* edges and the edges between vertices  $\alpha a$  and  $a\alpha$  are called *shuffle* edges.

The Shuffle-Exchange network provides suitable interconnection patterns for implementation of parallel algorithms like : *polynomial evaluation, fast Fourier transform, sorting* and *matrix transposition*.

#### Linear Layout of a Graph

The linear layout of a graph is such a layout in which the vertices are drawn on a horizontal line in some order (designated by  $\sigma$  in this paper). Although the graph is undirected, we consider the edges orientation given by the ordering of vertex set.

---

2000 Mathematics Subject Classification. 68R10.

Key words and phrases. shuffle-exchange graph, queue layout, queue number.

Research supported by grant No. 2/3164/23

Received 2. 3. 2004; Accepted 21. 9. 2004

## K-Queue Layout and Queue Number

A *k*-queue layout of an undirected graph  $G = (V, E)$  has two aspects. The first aspect is linear order of  $V$  (which we think of as being on a horizontal line). The second aspect is an assignment of each edge in  $E$  into one of  $k$  queues in such a way that the set of edges assigned to each queue obeys a first-in/first-out discipline. Each queue  $q_j$  operates as follows. The vertices of  $V$  are scanned in left-to-right ascending order. When vertex  $i$  is encountered, any edges assigned to  $q_j$  that have vertex  $i$  as their right endpoint must be at the front of that queue; they are removed (dequeued). Any edges assigned to  $q_j$  that have vertex  $i$  as their left endpoint are placed on the back of that queue (enqueued). Queue number ( $qn$ ) is smallest  $k$  such that  $G$  has *k*-queue layout. [heath]

This layout problem abstracts design problem of fault-tolerant processor arrays, a problem of sorting with parallel queues, and a problem of scheduling parallel processors.

The question of queue number of Shuffle-Exchange graph is still open, although it is known for deBruijn graph (close relative of Shuffle-Exchange). Heath and Rosenberg made the characterization of 1-queue graphs as arched leveled-planar graphs [heath]. Queue numbers of some typical graphs are also in [heath].

Leighton showed that crossing number of Shuffle-Exchange graph is  $\Theta(N^2/\log^2 N)$  [leighton].  $SE_d$  graph is therefore not planar in general (with exception for  $d \leq 3$ ) and for its quenumber holds  $qn(SE_d) \geq 2$ .

## K-Rainbow set of edges

**Definition 2.** Suppose we have a linear graph layout (all vertices are on the horizontal line) with some vertices ordering  $\sigma$ . Then a *k*-rainbow is a set of  $k$  edges  $e_i = (a_i, b_i), 1 \leq i \leq k$  such that

$$a_1 <_{\sigma} a_2 <_{\sigma} \cdots <_{\sigma} a_k <_{\sigma} b_k <_{\sigma} b_{k-1} <_{\sigma} \cdots <_{\sigma} b_2 <_{\sigma} b_1.$$

In other words, a rainbow is a *nested* matching. A rainbow is an obstacle for a queue layout because no two nested edges can be assigned to the same queue. [heath]

## Alternative definition of $SE_d$

**Definition 3.** Let  $G(V, E)$  be the graph with  $2^d$  vertices. Label the vertices with numbers  $0, 1, 2, \dots, 2^d - 1$ . The edges are defined as follows. Vertex with number  $n$  will be connected

- with vertex  $n + 1$  in case of even  $n$  or  $n = 0$ ,
- with vertex  $\frac{n}{2}$  in case of even  $n$ ,
- with vertex  $\frac{n-1}{2} + 2^{d-1}$  in case of odd  $n$ .

This definition is a modification of  $SE_d$  definition from [akl].

**Theorem 1.** Definitions 1 and 3 are equivalent.

*Proof.* From both definitions the vertex sets contain the same members only with different labelling. It is sufficient to prove that edge generating formulas will generate the edges of Shuffle-Exchange graph. In following two points we simply make the conversion from binary definition of edges to decadic one.

- (1) Exchange edges  $\alpha a \rightarrow \alpha \neg a$ 
  - (1a)  $\alpha 0 \rightarrow \alpha 1 \iff n \rightarrow (n + 1)$   
Note that number  $\alpha 0$  is even. So this will work for even  $n$  or  $n = 0$ .
  - (1b)  $\alpha 1 \rightarrow \alpha 0 \iff n \rightarrow (n - 1)$   
 $\alpha 1$  is odd number.  $n$  is also odd. The edges of the form (a) and (b) are identical with different directions. Since we ignore edge directions in  $SE_d$  we use only first form (a) of edges in our definition.
- (2) Shuffle edges  $\alpha a \rightarrow a\alpha$ 
  - (2a)  $\alpha 0 \rightarrow 0\alpha \iff n \rightarrow \frac{n}{2}$   $\alpha 0$  is even.  
Result of shuffle operation in this case is  $\alpha$ . This operation is division by the base of binary system. Equivalent operation in decadic system is  $\frac{n}{2}$ .
  - (2b)  $\alpha 1 \rightarrow 1\alpha \iff \frac{n-1}{2} + 2^{d-1}$ .  
The operation  $\alpha 1 \rightarrow 1\alpha$  is equivalent to  $(\alpha 1 \rightarrow \alpha 0 \rightarrow 0\alpha \rightarrow 1\alpha)$ .  
According to this operation equivalent formula in decadic system is  $\frac{n-1}{2} + 2^{d-1}$ .  $\square$

## Upper bound

**Lemma 2.** The queue number  $qn(G)$  of a graph  $G$  is a minimum, taken over all vertex orderings  $\sigma$  of  $G$ , of a maximum size of a rainbow in  $\sigma$ .

**Lemma 3.** Let  $p(n), n \in N$  be the non-descending sequence and let  $G$  be the graph  $G = (V, E)$ , where  $V = 0, 1, 2, \dots, n$  and all edges from  $E$  are of type  $(v, p(v)), v \in V$ . Then  $G$  has one-queue layout with natural  $(0, 1, \dots, n)$  ordering of vertices.

*Proof.* Let  $m_1, m_2, \dots, m_n; m_i \in N$  be the vertex indexes. From non-descending sequence  $p(m_i)$  we have

$$m_1 < m_2 < \dots < m_n \Rightarrow p(m_1) \leq p(m_2) \leq \dots \leq p(m_n).$$

Comparing this property with definition of  $k$ -rainbow set we see that in this type of graph the  $k$ -rainbow set can not exist with  $k > 1$ . According to Lemma 2 we have ordering with maximum rainbow size of 1, and therefore with queue number 1.  $\square$

**Theorem 4.** The  $SE_d$  graph has 3-queue layout with natural vertices ordering  $0, 1, \dots, 2^d - 1$ . The edges will be assigned to queues as follows.

- (1) queue : edges of type  $(m, m + 1)$  for even  $m$  or  $m = 0$ .
- (2) queue : edges of type  $(m, \frac{m}{2})$  for even  $m$ .
- (3) queue : edges of type  $(m, \frac{m-1}{2} + 2^{d-1})$  for odd  $m$ .

*Proof.* By assigning the edges into three queues we have three subgraphs of  $SE_d$ . It is sufficient to prove that these subgraphs have 1-queue layout with vertices ordering  $0, 1, 2, \dots, 2^d - 1$ .

- (1) queue : edges of type  $(m, m + 1)$  for even  $m$  or  $m = 0$ .  
Edges of this subgraph are generated by the formula  $p(m) = m + 1$ . It is ascending sequence and according to *Lemma 3* graph with such edges has 1-queue layout.
- (2) queue : edges of type  $(m, \frac{m}{2})$  for even  $m$ .  
Edges generating formula is  $p(m) = \frac{m}{2}$ . Again, it is ascending sequence and according to *Lemma 3* graph with such edges has 1-queue layout.
- (3) queue : edges of type  $(m, \frac{m-1}{2} + 2^{d-1})$  for odd  $m$ .  
Edges generating formula is  $p(m) = \frac{m-1}{2} + 2^{d-1}$ . Analogue to previous points graph with such edges has 1-queue layout.  $\square$

**Corollary 1.** The  $SE_d$  graph layed out on horizontal line with natural vertices ordering has k-rainbow set of edges with  $k = 3$ .

*Proof.* From our alternative definition of  $SE_d$  we have three types of edges. From proof of *Theorem 4* only edges of different types can nest. It means that maximal nested matching can have degree 3 (with respect to natural ordering of vertices). It is trivial to find such rainbow. For example one exists in  $SE_4$  and consists of edges  $\{(8, 9), (6, 12), (7, 11)\}$ . In  $SE_d$  where  $d > 4$  can be found for example this rainbow:  $\{(8, 9), (6, 12), (1, 2^{d-1})\}$ .  $\square$

*Theorem 4* gives upper bound for queue number of Shuffle-Exchange graph. The final value can be 3 (from *Theorem 4*) or 2 as a lower bound, since Shuffle Exchange can not have queue number 1 due to its non-planarity.

3-queue layout from *Theorem 4* is according to *Corollary 1* minimal. In other words, there exists no 2-queue layout of Shuffle-Exchange graph with natural order of vertices because of existence of 3-rainbow set of edges.

**Open problem.** To prove that  $qn(SE_d) = 2$  or  $qn(SE_d) > 2$ .

#### REFERENCES

- [1] Lenwood S. Heath and Arnold L. Rosenberg, *Laying out Graphs Using Queues*, SIAM J. Comput. **21** (1992), no. 5, 927-958.
- [2] S. Akl, *The Design and Analysis of Parallel Algorithms*, Prentice-Hall, Inc., 1989.
- [3] Frank T. Leighton, *Layouts for the Shuffle-Exchange Graph and Lower Bound Techniques for VLSI*, MIT, Cambridge, 1982.

INSTITUTE OF MATHEMATICS AND COMPUTER SCIENCE; MATHEMATICAL  
INSTITUTE OF SAS; SEVERNÁ 5; SK-97401 BANSKÁ BYSTRICA; SLOVAKIA  
E-mail: torok@savbb.sk