Werk

Label: Article

Jahr: 1984

PURL: https://resolver.sub.uni-goettingen.de/purl?312901348_44-45|log6

UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XLIV—XLV—1984

THE SEMIGROUP OF GENERAL CIRCULANT MATRICES

JAROSLAV GURIČAN, Bratislava

1. Introduction

It is well-known (see [2] or [3]) that a finite commutative semigroup S can be partitioned into maximal subsemigroups $\{P(e_i)\colon i=1, 2, \ldots, r\}$, where $\{e_1, \ldots, e_r\}$ is the set of all idempotents of S and $x \in P(e_i)$ iff $x^k = e_i$ for some k, moreover, there are the smallest positive integers K and D such that

$$x^K = x^{K+D} \tag{1}$$

for all $x \in S$. Š. Schwarz [5] called identity (1) the Euler—Fermat theorem for S.

Š. Schwarz mentioned in [4] and [5] that a small number of semigroups S is known for which (a) the idempotents e_i $1 \leqslant i \leqslant r$ are characterized, (b) the decomposition $S = \bigcup(P(e_i)\colon i=1, \ldots, r)$ and cardinalities $|P(e_i)|$ are established and (c) the integers K and D for the Euler—Fermat theorem are calculated. In [1], [4] and [5] he investigated from this point of view the multiplicative semigroup C_n of circulant matrices over a two-elements Boolean algebra **2**.

The aim of this note is to extend these results and investigate the multiplicative semigroups of circulant matrices over arbitrary finite Boolean algebras (finite distributive lattices or $GF(p^k)$).

2. Preliminaries

Let $\mathcal{U} = (U, F)$ denote a finite universal algebra. In the whole paper we will assume that F contains two binary operations "$+$" and "$\cdot$" as well as two nulary operations 0 and 1 such that $(U, +, \cdot, 0, 1)$ is semiring. That means, $+$ and $\cdot$ are associative, commutative and distributive, i.e.

$$x \cdot (y+z) = x \cdot y + x \cdot z$$

for all $x, y, z \in U$ and 0, 1 are neutral elements with respect to $+$ and $\cdot$, respectively. In this note we will consider three classes of algebras satisfying these conditions:

(i) finite Boolean algebras $\mathcal{B} = (B, +, \cdot, 0, 1)$

(ii) finite distributive lattices $\mathcal{D} = (D, +, \cdot, 0, 1)$

(iii) finite commutative rings $\mathcal{R} = (R, +, \cdot, 0, 1)$ satisfying identities $x^{p^k} = x$ and $p \cdot x = 0$.

Consider a finite algebra $\mathcal{U} = (U, F)$ and $n > 1$.

Take $a_0, a_1, \ldots, a_{n-1} \in U$. We can form a circulant matrix

$$\boldsymbol{A} = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ & & & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}$$

It is easy to verify that $\boldsymbol{A}$ can be (uniquely) written in the form (see [4])

$$\boldsymbol{A} = a_0\boldsymbol{E} + a_1\boldsymbol{P} + \ldots + a_{n-1}\boldsymbol{P}^{n-1},$$

where

$$\boldsymbol{E} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \quad \text{and} \quad \boldsymbol{P} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \vdots \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Now it is not difficult to show that the product of two circulant matrices is again a circulant matrix. So all circulant matrices over $\mathcal{U}$ form a finite commutative semigroup $S_{\mathcal{U}}(n)$, the semigroup of circulant matrices over $\mathcal{U}$. A general reference for semigroups and universal algebras can be find in [2] and [3], respectively.

3. A General Result

We need the following result which is a direct consequence of two theorems from [3] (p. 121 and pp. 124—125):

Lemma 1. Let $\mathcal{U}$ be a finite universal algebra from an equational class K. Then there is in K a finite family of finite subdirectly irreducible algebras $\{\mathcal{U}_i \in K: i = 1, \ldots, k\}$ such that

$$\mathcal{U} = \prod_s (\mathcal{U}_i: i = 1, 2, \ldots, k),$$

i.e. $\mathcal{U}$ is a subdirect product of $\{\mathcal{U}_i: i = 1, 2, \ldots, k\}$.

Now we can prove

Lemma 2. Let $\mathcal{U}=(U, F)$ be a finite algebra from an equational class K. Let F contain operations $+, \cdot, 0, 1$ such that $(U, +, \cdot, 0, 1)$ is a semiring. Suppose that $\mathcal{U}=\prod_s(\mathcal{U}_i: i=1, \ldots, k)$. Then for the semigroup of circulant matrices $S_{\mathcal{U}}(n)$ the following statement is true:

$$S_{\mathcal{U}}(n)=\prod_s (S_{\mathcal{U}_i}(n): i=1, \ldots, k)$$

Proof: Suppose that $p_i: \mathcal{U}\to\mathcal{U}_i$ is the projection corresponding to the subdirect product $\mathcal{U}=\prod_s(\mathcal{U}_i: i=1, \ldots, k)$ $(i=1, \ldots, k)$. Take a circulant matrix $\boldsymbol{A}\in S_{\mathcal{U}}(n)$. The homomorphism p_i can be extended to the $\bar{p}_i: S_{\mathcal{U}}(n)\to S_{\mathcal{U}_i}(n)$ in the following way:

$$\bar{p}_i(\boldsymbol{A})=\begin{pmatrix} p_i(a_0) & \ldots & p_i(a_{n-1}) \\ p_i(a_{n-1}) & \ldots & p_i(a_{n-2}) \\ \vdots & & \vdots \\ p_i(a_1) & \ldots & p_i(a_0) \end{pmatrix}$$

It is easy to check that $\bar{p}_i(\boldsymbol{A}\cdot\boldsymbol{B})=\bar{p}_i(\boldsymbol{A})\cdot\bar{p}_i(\boldsymbol{B})$, $i=1, \ldots, k$. Hence $\bar{p}_i: S_{\mathcal{U}}(n)\to S_{\mathcal{U}_i}(n)$ is a homomorphism for every $i=1, \ldots, k$. Since p_i are epimorphisms, we obtain epimorphisms $\bar{p}_i$ again. Now we can define the map:

$$\varphi: \varphi(\boldsymbol{A})=(\bar{p}_1(\boldsymbol{A}), \bar{p}_2(\boldsymbol{A}), \ldots, \bar{p}(\boldsymbol{A}))$$

from $S_{\mathcal{U}}(n)$ into the direct product $\prod(S_{\mathcal{U}_i}(n): i=1, \ldots, k)$. Obviously φ is injective and Im φ is a subdirect product of the semigroups $S_{\mathcal{U}_i}(n)$; $i=1, \ldots, k$.

The proof of the following theorem is straightforward.

Theorem 3. Let S be a finite commutative semigroup $S=\prod_s(S_i: i=1, \ldots, k)$. Let $p_i: S\to S_i$ be projection $(i=1, \ldots, k)$ corresponding to this subdirect product. Then

(i) $e\in S$ is an idempotent of S iff $p_i(e)\in S_i$ is an idempotent of S_i for every $i=1, \ldots, k$;

(ii) If $e\in S$ is an idempotent of S then $a\in P(e)$ (i.e. $a^r=e$ for some $r\in N$) iff $p_i(a)\in P(p_i(e))$ in S_i for every $i=1, \ldots, k$;

(iii) Let $a\in S$. Let $(p_i(a))^{r_i}=(p_i(a))^{r_i+d_i}$ $i=1, \ldots, k$ so that $r_i\geqslant 0$, $d_i>0$ and none of numbers r_i, d_i can be replaced by a smaller one. Denote

$$r=\max\{r_i: i=1, \ldots, k\}, \qquad d=\text{l.c.m.}\{d_i: i=1, \ldots, k\}.$$

Then $a^r=a^{r+d}$ and none of the integers r, d can be replaced by a smaller one. In particular, if r_i, d_i are integers from the Euler—Fermat theorem for S_i then

$$r = \max\{r_i : i = 1, \ldots, k\}, \quad \text{and} \quad d = \text{l.c.m.}\{d_i : i = 1, \ldots, k\}$$

are integers for the Euler—Fermat theorem for S.

(iv) If $S = \prod(S_i : i = 1, \ldots, k)$ is a direct product then

$$|P(e)| = |P(p_1(e))| \cdot |P(p_2(e))| \cdot \ldots \cdot |P(p_k(e))|$$

for any idempotent $e \in S$.

Lemmas 1,2 and Theorem 3 show that the investigation of the semigroup of circulant atrices $S_{\mathfrak{A}}(n)$ can be reduced to the study of semigroups $S_{\mathfrak{A}_i}(n)$ for subdirectly irreducible algebras $\mathfrak{A}_i$ only.

4. Circulant Matrices over Boolean Algebras and Distributive Lattices

In this section we will apply Theorem 3 to the semigroup of circulant matrices over a finite Boolean algebra or a finite distributive lattice. It is well-known that every finite Boolean algebra is a direct product of the two-element Boolean algebras **2** and similarly every finite distributive lattice is a subdirect product of the two-element lattices.

Combining Theorem 3 with [1], [4] and [5] we obtain

Theorem 4. Let $\mathfrak{A}$ be a finite Boolean algebra $\mathfrak{B}$ with $\mathfrak{B} = \prod(B_i : i = 1, \ldots, k)$ or a finite distributive lattice $\mathfrak{D}$ with $\mathfrak{D} = \prod_s(D_i : i = 1, \ldots, k)$ and $B_i, D_i \cong 2$ $(i = 1, \ldots, k)$. Then in the semigroup $S_{\mathfrak{A}}(n)$, $n > 1$, of circulant matrices over $\mathfrak{A}$ the following holds:

(i) $\boldsymbol{A} \in S_{\mathfrak{A}}(n)$ is an idempotent in $S_{\mathfrak{A}}(n)$ iff for all $i = 1, \ldots, k$ there are integers d_i such that

$$d_i \neq 0, \quad d_i \mid n, \quad d_i \cdot t_i = n$$

and

$$\bar{p}_i(\boldsymbol{A}) = \boldsymbol{E} + \boldsymbol{P}^{d_i} + \boldsymbol{P}^{2d_i} + \ldots + \boldsymbol{P}^{(t_i-1)d_i} (= \boldsymbol{E}(d_i))$$

or

$$\bar{p}_i(\boldsymbol{A}) = \boldsymbol{0} \ (\boldsymbol{0} \text{ denotes the zero matrix}) \text{ for } d_i = 0$$

We can denote this idempotent as $\boldsymbol{A} = \boldsymbol{E}(d_1, \ldots, d_k)$.

(ii) Let $\boldsymbol{A} \in S_{\mathfrak{A}}(n)$. Then $\boldsymbol{A}$ belongs to the idempotent $\boldsymbol{E}(d_1, \ldots, d_k)$ iff for arbitrary i

$$\bar{p}_i(\boldsymbol{A}) = \boldsymbol{0} \text{ for } d_i = 0$$

or

$$\bar{p}_i(\boldsymbol{A}) = \boldsymbol{P}^m(\boldsymbol{E} + \boldsymbol{P}^{u_1 d_i} + \ldots + \boldsymbol{P}^{u_s d_i}) \text{ for } d_i \neq 0$$

such that

$$1 \leqslant u_1 < u_2 < \ldots < u_s < t_i, \quad m < n$$

and

$$\text{g.c.d.}\ \{u_1, \ldots, u_s, t_i\} = 1$$

(iii) Having $\boldsymbol{A} \in P(\boldsymbol{E}(d_1, \ldots, d_k))$ denote by

$$t = \max\left\{\frac{n}{d_i} : i = 1, \ldots, k,\ d_i \neq 0\right\}$$

and

$$d = \text{l.c.m.}\ \{d_i : i = 1, \ldots, k,\ d_i \neq 0\}$$

Then

$$\boldsymbol{A}^{t-1} = \boldsymbol{A}^{t-1+d}$$

and none of integers t and d can be replaced by a smaller one. In particular,

$$\boldsymbol{A}^{n-1} = \boldsymbol{A}^{2n-1}$$

is the Euler—Fermat theorem for $S_{\mathcal{U}}(n)$.

(iv) If $\mathcal{U}$ is a Boolean algebra then

$$|P(\boldsymbol{E}(d_1, \ldots, d_k)| = n^k \cdot \prod\left(\Phi\left(\frac{n}{d_i}\right) : i = 1, \ldots, k,\ d_i \neq 0\right),$$

where

$$\Phi(t) = \frac{1}{t}\sum_{h|t} h \cdot \mu(h) \cdot (2^h - 1)$$

and μ is the Möbius function, $t \in N$.

5. Circulant Matrices over Finite Rings

In this section we will investigate semigroups of circulant matrices $S_{\mathcal{R}}(n)$ over a finite commutative ring $\mathcal{R} = (R, +, \cdot, 0, 1)$ with unit satisfying identities

$$x^{p^k} = x \quad \text{and} \quad p \cdot x = 0$$

(for some prime number p). We will present solutions to the questions formulated in the introduction only partly. We have necessary conditions describing idempotents in $S_{\mathcal{R}}(n)$ and, in particular, for $p = 2$ there are necessary and sufficient conditions.

Let T_{p^k} denote the class of all commutative rings with unit satisfying these identities. Evidently, T_{p^k} is an equational class.

We start with the description of the finite subdirectly irreducible rings belonging to T_{p^k}.

Theorem 5. Let $\mathcal{R}$ be a finite commutative ring with unit and satisfying the identity $x^r = x$, $r \geq 2$.

Then $\mathcal{R}$ is subdirectly irreducible iff $\mathcal{R}$ is a field.

Proof: Suppose that $\mathcal{R}$ is subdirectly irreducible. Since every congruence relation on $\mathcal{R}$ is uniquely determined by its kernel, it is sufficient to consider the ideals of $\mathcal{R}$ only. According to the hypothesis the smallest nontrivial ideal J of $\mathcal{R}$ exists. Take $0 \neq a \in J$. Then we have $(a) \subset J$, where (a) is the principal ideal generated by a. Therefore $(a) = J$. We claim that $\mathcal{R}$ is an integral domain. To the contrary suppose that there are $0 \neq c$, $0 \neq d$ in R such that

$$c \cdot d = 0.$$

Clearly $(a) \subset (c)$, by hypothesis. Therefore $b \cdot c = a$ for some $b \in R$. It follows that $a \cdot d = (b \cdot c) \cdot d = b \cdot (c \cdot) = b \cdot 0 = 0$. We can consider the ideal $I = \{x \in R: x \cdot a^{r-1} = 0\}$. It is easy to check that $d \in I$ and $a \notin I$. Hence $(a) \not\subseteq I$, what is a contradiction. Thus $\mathcal{R}$ is an integral domain, as claimed. It is well-known that a finite integral domain is a field. The rest of the proof is trivial.

Corollary 1. Every finite ring $\mathcal{R} \in T_{p^k}$ is a subdirect product of a finite family of fields $GF(p^{r_1}), \ldots, GF(p^{r_s})$, where $r_i \mid k$ for $i = 1, \ldots, s$.

Suppose that $\mathcal{R}$ is a finite ring from T_{p^k}. Consider $\boldsymbol{A} \in S_{\mathcal{R}}(n)$ satisfying

$$\boldsymbol{A}^p = \boldsymbol{A}.$$

Assume

$$\boldsymbol{A} = a_0\boldsymbol{E} + a_1\boldsymbol{P} + \ldots + a_{n-1}\boldsymbol{P}^{n-1}$$

and

$$\boldsymbol{A}^p = c_0\boldsymbol{E} + c_1\boldsymbol{P} + \ldots + c_{n-1}\boldsymbol{P}^{n-1}$$

Therefore,

$$c_i = \sum (a_{j_1} a_{j_2} \ldots a_{j_p}: j_1 + j_2 + \ldots + j_p \equiv i (\mathrm{mod}\ n), j_k < n)$$

We can verify without any difficulties that

$$c_i = \sum (a_j^p: j \cdot p \equiv i (\mathrm{mod}\ n), j < n) + \sum \left(\frac{p!}{k_1! \ldots k_r!} a_{j_1}^{k_1} \ldots a_{j_r}^{k_r}: \right.$$

$$\left. k_1 j_1 + \ldots + k_r j_r \equiv i (\mathrm{mod}\ n), k_1 + \ldots + k_r = p, r \geq 2, j_k < n \right)$$

Since $p \cdot x = 0$ in $\mathcal{R}$ and $\boldsymbol{A}^p = \boldsymbol{A}$, we obtain

$$a_i = c_i = \sum (a_j^p: p \cdot j \equiv i (\mathrm{mod}\ n), j < n) \tag{1}$$

Two cases can arise: $(p, n) = 1$ or $(p, n) \neq 1$.

In the firs case we have

Lemma 6. Let $(p, n)=1$. Then for every $x \in I_p$ is $x/p \in I_p$. ($I_p=\{x \in Z_n$: $x \equiv p^s \pmod n$, $s=1, \ldots, \varphi(n)\}\varphi(n)$ is the Euler function and $x/p=j$ iff $p \cdot j \equiv x \pmod n$ and $j<n$).

Proof: It is well-known that $\{x \in Z_n: (x, n)=1\}=G$ forms a subgroup of the multiplicative semigroup $(Z_n, \cdot)$. Evidently, $|G|=\varphi(n)$. Therefore I_p is the cyclic subgroup of G generated by $y \in Z_n$ satisfying $y \equiv p \pmod n$. The proof is complete.

Now we are ready to formulate the main result.

Theorem 7. Let $\mathcal{R}$ be a finite ring from the equational class T_{p^k}. Let $\boldsymbol{A} \in S_{\mathcal{R}}(n)$ and let

$$\boldsymbol{A}=a_0\boldsymbol{E}+a_1\boldsymbol{P}+\ldots+a_{n-1}\boldsymbol{P}^{n-1}$$

(a) Suppose that $(p, n)=1$. Then $\boldsymbol{A}^p=\boldsymbol{A}$ iff

$$a_0^p=a_0 \text{ and } a_r^{p^s}=a_j$$

whenever

$$j \equiv r \cdot p^s \pmod n \text{ for } 1 \leqslant r, j<n \text{ and } 1 \leqslant s \leqslant \varphi(n).$$

(b) Suppose that $n=p^r m$, where $r \geqslant 1$ and $(p, m)=1$.

Then $\boldsymbol{A}^p=\boldsymbol{A}$ iff the following conditions are fulfiled:

(i) $a_s=0$ for $(p^r, s) \neq p^r$

(ii) $\boldsymbol{B}^p=\boldsymbol{B}$ for $\boldsymbol{B}=a_0\boldsymbol{E}+a_{p^r}\boldsymbol{P}+a_{2p^r}\boldsymbol{P}^2+\ldots+a_{(m-1)p^r}\boldsymbol{P}^{(m-1)}$

Proof: The part (a) follows from Lemma 6 as well as from the condition (1).

(b) Necessity. Assume $\boldsymbol{A}^p=\boldsymbol{A}$ and $s=p^t v$, $(p, v)=1$. We will prove (i) by induction on t. At first suppose $t=0$. It is easy to check that there is no $0 \leqslant j<n$ such that $p \cdot j \equiv s \pmod n$. Therefore $a_s=0$.

Now suppose $t \geqslant 1$ and that $a_{s'}=0$ for all $s'=p^h u$, where $0 \leqslant h<t$ and $(p, u)=1$. We claim that $p \cdot j \equiv s \pmod n$ iff $j=\dfrac{s+in}{p}$, where $0 \leqslant i<n$. Evidently, $p \cdot j \equiv s \pmod n$ is equivalent to $p \cdot j=n \cdot q+s$ for some $0 \leqslant q<n$ and consequently $j=\dfrac{n \cdot q+s}{p}$. On the other hand, it is easy to check that $p \cdot \left(\dfrac{n \cdot i+s}{p}\right) \equiv s \pmod n$.

As it was mentioned $a_s=\sum(a_j^p: p \cdot j \equiv s \pmod n)$ by (1). By induction assumption, $a_j=0$ because $p^{t-1} \mid j$ and $p^t \nmid j$. Hence $a_s=0$ and (i) is proved.

(ii) According to (i) $\boldsymbol{A}$ can be written in the following form

$$\boldsymbol{A}=a_0\boldsymbol{E}+a_{p^r}\boldsymbol{P}^{p^r}+a_{2r^r}\boldsymbol{P}^{2p^r}+\ldots+a_{(m-1)p^r}\boldsymbol{P}^{(m-1)p^r}.$$

Since $\boldsymbol{A}^p=\boldsymbol{A}$, it is easy to verify that $\boldsymbol{B}^p=\boldsymbol{B}$.

The converse implication can be easily proved by a direct computation. This completes the proof of Theorem 7.

Remark: Since $\boldsymbol{A}^2 = \boldsymbol{A}$ implies $\boldsymbol{A}^p = \boldsymbol{A}$, Theorem 7 gives necessary condition for a circulant matrix $\boldsymbol{A} \in S_{\mathscr{R}}(n)$ in order to be an idempotent in the semigroup $S_{\mathscr{R}}(n)$.

Clearly, Theorem 7 characterizes idempotents in $S_{\mathscr{R}}(n)$ for $\mathscr{R} \in T_{2^k}$.

REFERENCES

[1] Hang Butler, K. K.—Schwarz, Š.: The Semigroup of Circulant Boolean Matrices, Czech. Math. J. 26 101 1976 632-635

[2] Clifford, A. H.—Preston, G. B.: The Algebraic Theory of Semigroups, Vol. 1, Math. Surveys No. 7, Am. Math. Soc., Providence, R. I., 1964 Russian translation 1972

[3] Grätzer, G.: Universal Algebra, von Nostrand, 1968, Chapter 3.

[4] Schwarz, Š.: A Counting Theorem in the Semigroup of Circulant Boolean Matrices, Czech. Math. J. 27 102 1977 504—510

[5] Schwarz, Š.: The Euler—Fermat Theorem for the Semigroup of the Circulant Boolean Matrices, Czech. Math. J. 30 105 1980 135—141

Author's address:

Received: 30. 11. 1982

Jaroslav Guričan
Katedra algebry a teórie čísel MFF UK
Matematický pavilón
Mlynská dolina
Bratislava
842 15

SÚHRN

POLOGRUPA VŠEOBECNÝCH CIRKULANTNÝCH MATÍC

J. Guričan, Bratislava

V článku študujeme pologrupy cirkulantných matíc nad nasledovnými konečnými univerzálnymi algebrami: konečnými Boolovými algebrami, konečnými distributívnymi zväzmi a konečnými komutatívnymi okruhmi s 1 spĺňajúcimi identitu $x^{p^k} = x$. Pre tieto pologrupy hľadáme charakterizáciu idempotentov, charakterizáciu prvkov patriacich ku jednotlivým idempotentom e (t. j. takých prvkov x, že $x^r = e$ pre nejaké $f \in N$) a hľadáme aj počty takýchto prvkov pre jednotlivé idempotenty. Nakoniec, hľadáme najmenšie kladné čísla k, d také, aby identita $x^k = x^{k+d}$ bola splnená v našej pologrupe.

РЕЗЮМЕ

ПОЛУГРУППА ОБЩИХ ЦИРКУЛЯНТНЫХ МАТРИЦ

Я. Гуричан, Братислава

В статье изучаются полугруппы циркулянтных матриц над следующими конечными универсальными алгебрами: конечными Булевыми алгебрами, конечными дистрибутивными решетками и конечными коммутативными кольцами с 1, в которых выполняется идентита $x^{p^k} = x$.

Для этих полугрупп ищется характеризация идемпотентов, характеризация элементов принадлежащих какому-то идемпотенту e (это значит тех элементов x, для которых $x^r = e$ для некоторого $r \in N$) и количества этих элементов для какого-то идемпотента e. И, наконец, ищутся найменьшие положительные числа k, d для того, чтобы идентита $x^k = x^{k+d}$ выполнялась в нашей полугруппе.