Czechoslovak Mathematical Journal

Ágnes Szendrei

On closed classes of quasilinear functions

Czechoslovak Mathematical Journal, Vol. 30 (1980), No. 3, 498–509

Persistent URL: http://dml.cz/dmlcz/101699

Czechoslovak Mathematical Journal, 30 (105) 1980, Praha

ON CLOSED CLASSES OF QUASILINEAR FUNCTIONS

ÁGNES SZENDREI, Szeged

(Received April 2, 1979)

1. INTRODUCTION

As will be pointed out in Section 2, among the maximal closed subclasses of the class of all functions over a nonvoid set A with $|A| = p^k$ (p prime, $p^k > 3$), the maximal classes of *quasilinear functions* (i.e. those determined by an elementary Abelian p-group operation on A) are distinguished by the property of having only countably many closed subclasses. There is another advantageous property of quasilinear functions: they have two different representations making them easy to handle, namely, one as polynomials of a special form over a finite field and the other as linear functions with coefficients in a matrix ring over a finite prime field (see Theorems 2.2 and 2.3 below).

If the cardinality of the base set A is a prime power p^n with $n > 2$ then a full description of the closed classes of quasilinear functions is not known. On the other hand, if A is of prime order then the two representations mentioned above coincide and the maximal closed classes of quasilinear functions have the form

$$\boldsymbol{L}_{Z_p} = \{ \sum_{i=1}^{k} a_i x_i + a_0 \mid k \geqq 1,\ a_j \in Z_p\ (j = 0, \ldots, k) \},$$

where Z_p is the p-element prime field. SALOMAA [10] and DEMETROVICS-BAGYINSZKI [1] have described the closed subclasses of $\boldsymbol{L}_{Z_p}$. In particular, it turned out that $\boldsymbol{L}_{Z_p}$ contains only finitely many closed subclasses.

The main aim of the present note is to generalize this result to arbitrary finite fields, i.e. to investigate the class

$$\boldsymbol{L}_F = \{ \sum_{i=1}^{k} a_i x_i + a_0 \mid k \geqq 1,\ a_j \in F\ (j = 0, \ldots, k) \}$$

of linear functions over a finite field F. I am indebted to W. HARNAU for calling my attention to this problem. Sections 3 and 4 below are devoted to the study of closed classes containing $\boldsymbol{L}_F$ or being contained in $\boldsymbol{L}_F$, respectively. In particular, we show that $\boldsymbol{L}_F$ is of finite height in the lattice of all closed classes of functions over F, and contains only finitely many closed subclasses.

2. PRELIMINARIES

We adopt the terminology of [9]. For any set $A(\neq\emptyset)$ and every positive integer n, $\boldsymbol{O}_A^{(n)}$ will stand for the set of n-ary operations on A. Set $\boldsymbol{O}_A = \bigcup_{n=1}^{\infty} \boldsymbol{O}_A^{(n)}$. An operation $f \in \boldsymbol{O}_A^{(n)}$ is said to *depend* on its i'th variable $(1 \leqq i \leqq n)$ if there exist elements a_j $(j = 1, \ldots, n)$, a_i' in A such that

$$f(a_1, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n).$$

An operation $f \in \boldsymbol{O}_A^{(n)}$ is termed *idempotent* if $f(a, \ldots, a) = a$ holds for every $a \in A$. Operations that are not projections will be referred to as *non-trivial operations*.

A subset $\boldsymbol{C}$ of $\boldsymbol{O}_A$ is called a *closed class* if together with any operation f, $\boldsymbol{C}$ contains all operations arising from f by interchanging or identifying its variables, and furthermore, $\boldsymbol{C}$ is closed under composition, i.e. if $f, g \in \boldsymbol{C}$, say f is m-ary and g is n-ary, then the operation $f * g \in \boldsymbol{O}_A^{(m+n-1)}$ defined by

$$(f * g)(a_1, \ldots, a_{m+n-1}) = f(g(a_1, \ldots, a_n), a_{n+1}, \ldots, a_{m+n-1})$$
$$(a_i \in A,\ i = 1, \ldots, m + n - 1)$$

also belongs to $\boldsymbol{C}$. The closed class generated by a subset H of $\boldsymbol{O}_A$ is denoted by $[H]$. Clearly, a closed class containing an at least binary projection contains all projections. Such a closed class is called a *clone*. A closed subclass $\boldsymbol{C}$ of $\boldsymbol{O}_A$ is termed *unary* if every member of $\boldsymbol{C}$ depends on at most one of its variables. The lattice of closed subclasses of $\boldsymbol{O}_A$ will be denoted by $\mathscr{L}_A$. Following GAVRILOV [4] (see also Salomaa [11]), we define the *height* of a closed class $\boldsymbol{C}(\subseteq \boldsymbol{O}_A)$ as the length of the longest finite chain in $\mathscr{L}_A$ connecting $\boldsymbol{C}$ to $\boldsymbol{O}_A$ provided such a chain exists; otherwise, $\boldsymbol{C}$ is said to be of *infinite height*.

Due to ROSENBERG [7, 8], we have a complete description of the closed classes of height 1, i.e. the maximal closed subclasses of $\boldsymbol{O}_A$. To be able to formulate this theorem, we need some more definitions.

Let A be a nonvoid finite set, $k, n \geqq 1$, $f \in \boldsymbol{O}_A^{(n)}$ and $\varrho \subseteq A^k$. The operation f is said to *preserve* the relation ϱ if ϱ is a subalgebra of the k'th direct power of the algebra $\langle A; f\rangle$; in other words, f preserves ϱ if for any $n \times k$ matrix with entries in A, whose rows belong to ϱ, the row of column values of f also belongs to ϱ. Clearly, the set of operations preserving a relation ϱ forms a clone, which will be denoted by Pol ϱ.

A k-ary relation ϱ on A is called *central* if $\varrho \neq A^k$ and there exists a nonempty subset C of A such that

(i) $\langle a_1, \ldots, a_k\rangle \in \varrho$ whenever at least one $a_j \in C$ $(1 \leqq j \leqq k)$;

(ii) $\langle a_1, \ldots, a_k\rangle \in \varrho$ implies $\langle a_{1\pi}, \ldots, a_{k\pi}\rangle \in \varrho$ for every permutation π of the indices $1, \ldots, k$;

(iii) $\langle a_1, \ldots, a_k\rangle \in \varrho$ if $a_i = a_j$ for some $i \neq j$ $(1 \leqq i, j \leqq k)$.

Let $2 < k \leqq |A|$, with $|A|$ standing for the cardinality of A, and $m \geqq 1$. A family $T = \{\theta_1, \ldots, \theta_m\}$ of equivalence relations on A is termed *k-regular* if

(iv) each θ_j has k equivalence classes $(j = 1, \ldots, m)$;

(v) the intersection $\bigcap_{i=1}^{m} \varepsilon_i$ of arbitary equivalence classes $\varepsilon_i \in \theta_i$ $(i = 1, \ldots, m)$ is non-empty.

The relation ϱ *determined by* T consists of all $\langle a_1, \ldots, a_k \rangle \in A^k$ having the property that for each $j = 1, \ldots, m$ at least two elements among $a_1, \ldots, a_k$ are equivalent modulo θ_j. Notice that ϱ has the properties (ii) and (iii).

Theorem 2.1 (Rosenberg [7, 8]). *For a finite set* $A(\neq \emptyset)$, Pol ϱ *is a maximal closed subclass of* $\boldsymbol{O}_A$ *provided* ϱ *is one of the following relations on* A:

(α) *a bounded partial order*;

(β) *a binary relation* $\{\langle a, a\pi \rangle \mid a \in A\}$ *where* π *is a permutation of* A *with* $|A|/p$ *cycles of the same prime length* p;

(γ) *a quaternary relation* $\{\langle a_1, a_2, a_3, a_4 \rangle \in A^4 \mid a_1 + a_2 = a_3 + a_4\}$ *where* $\langle A; + \rangle$ *is an elementary Abelian p-group*;

(δ) *a nontrivial equivalence relation*;

(ε) *a central relation*;

(ζ) *a relation determined by a k-regular family of equivalence relations on* A $(k > 2)$.

Moreover, every proper closed subclass of $\boldsymbol{O}_A$ *is contained in at least one of the clones listed above.*

Next we discuss in more detail the maximal classes of type (γ). Let $\langle F; +, \cdot \rangle$ be a finite field. The closed class $\boldsymbol{L}_{\langle F;+,\cdot\rangle}$ $(\subseteq \boldsymbol{O}_F)$ defined in the introduction is easily seen to be contained in the maximal class of type (γ) determined by the additive group $\langle F; + \rangle$ of the field $\langle F; +, \cdot \rangle$. This maximal class will be denoted by $\boldsymbol{Q}_{\langle F;+\rangle}$. If there is no danger of confusion we write $\boldsymbol{L}_F$ and $\boldsymbol{Q}_F$ instead of $\boldsymbol{L}_{\langle F;+,\cdot\rangle}$ and $\boldsymbol{Q}_{\langle F;+\rangle}$, respectively. It is well known that any operation in $\boldsymbol{O}_F$ is a polynomial over the field $\langle F; +, \cdot \rangle$. Those belonging to $\boldsymbol{Q}_F$ can be characterized as follows:

Theorem 2.2 (Rosenberg [8]). *Given an elementary Abelian p-group* $\langle F; + \rangle$ *of order* p^n (p *prime*, $n \geqq 1$), *for any field* $\langle F; +, \cdot \rangle$ *we have*

$$\boldsymbol{Q}_{\langle F;+\rangle} = \{a_0 + \sum_{i=1}^{k} \sum_{j=0}^{n-1} a_{ij} x_i^{p^j} \mid k \geqq 1,\ a_0, a_{ij} \in F\}\,.$$

Since any elementary Abelian p-group of order p^n is isomorphic to $\langle Z_p^n; + \rangle$, the following theorem gives another characterization of the maximal classes of type (γ).

Theorem 2.3 (Rosenberg [8]). *For any prime number p and $n \geqq 1$ we have*

$$\boldsymbol{Q}_{\langle Z_p{}^n;+\rangle} = \{\sum_{i=1}^{k} A_i x_i + a \mid k \geqq 1,\ A_i \in Z_p[n \times n]\ (i = 1, \ldots, k),\ a \in Z_p^n\}\ .$$

Here $Z_p[n \times n]$ stands for the full $n \times n$ matrix ring over the field Z_p.

Once we have at hand Rosenberg's description of the maximal closed subclasses of $\boldsymbol{O}_A$ (which are finite in number), it is of interest to have a look at the closed classes contained in a fixed maximal class. In case $3 \leqq |A| < \aleph_0$ JANOV and MUČNIK [14] have shown $\boldsymbol{O}_A$ to possess $2^{\aleph_0}$ closed subclasses, so it is natural to ask how many closed subclasses are contained in a fixed maximal class. This question is answered in the following

Theorem 2.4. *Let A be a finite set, $|A| \geqq 3$. Then in $\boldsymbol{O}_A$*

(i) *any maximal class of type* (γ) *has countably many closed subclasses;*

(ii) *any maximal class of type* (α), (δ), (ε) *or* (ζ) *has $2^{\aleph_0}$ closed subclasses;*

(iii) *if $|A| > 3$ then any maximal class of type* (β) *has $2^{\aleph_0}$ closed subclasses.*

One case remains unsettled:

Open problem: How many closed subclasses are contained in a maximal class of type (β) if $|A| = 3$?

(It is shown in [3] that there are infinitely many such closed subclasses.)

The first assertion of the theorem follows from a seemingly considerable generalization of a recent result of LAU [5]. In fact, however, her proof can be almost literally repeated to prove the following general result.

Let R be a ring and M a faithful left R-module. Consider the following set of operations on M:

$$\boldsymbol{L}_M = \{\sum_{i=1}^{k} r_i x_i + m \mid k \geqq 1,\ r_i \in R\ (i = 1, \ldots, k),\ m \in M\}\ .$$

Clearly, $\boldsymbol{L}_M$ is a closed subclass of $\boldsymbol{O}_M$.

Theorem 2.5. *For any finite ring R and finite faitful left R-module M, the number of closed subclasses of $\boldsymbol{L}_M$ is denumerable.*

In view of Theorem 2.3, Theorem 2.4(i) is indeed a corollary to Theorem 2.5.

The proof of the second assertion is based on the construction of Janov and Mučnik. They proved that for any three distinct elements a, b, c of the base set A ($3 \leqq |A| < \aleph_0$), the operations g_i ($i = 2, 3, \ldots$) defined by

$$g_i(x_1, \ldots, x_i) = \begin{cases} b & \text{if } \langle x_1, \ldots, x_i\rangle = \langle c, \ldots, c\rangle \text{ or } \langle c, \ldots, c, b, c, \ldots, c\rangle\ , \\ a & \text{otherwise} \end{cases}$$

have the property

$$g_k \notin [g_i \mid i = 2, 3, \ldots, i \neq k], \quad k = 2, 3, \ldots .$$

It suffices to show that if ϱ is a relation of type (α), (δ), (ε) or (ζ), then each g_i belongs to Pol ϱ provided a, b, c are chosen appropriately. According to the type of ϱ they are to be selected as follows:

(α) a the greatest element, c the smallest one and b an element covering c (i.e. a minimal element);

(δ) $a \neq b$ and $a \varrho b$, $c(\neq a, b)$ arbitrary;

(ε) $a \in C$, the centre of ϱ, while $c \notin C$, $b(\neq a, c)$ arbitrary;

(ζ) a, b, c arbitrary distinct elements.

We note here that Theorem 2.4 (ii) was also observed by DEMETROVICS and HANNÁK [2].

The third assertion of the theorem follows by combining a theorem of MARČENKOV [6] with a recent result of Demetrovics and Hannák [3]. In fact, they have proved the following stronger statement: for any permutation π of the set A with $|A| \geqq 3$, which is not a cycle of the length $|A|$ if $|A| \leqq 4$, the closed class Pol ϱ_π determined by the binary relation

$$\varrho_\pi = \{\langle a, a\pi\rangle \mid a \in A\}$$

has $2^{\aleph_0}$ closed subclasses.

Thus the proof of Theorem 2.4 is complete.

3. CLOSED CLASSES CONTAINING L_F

Consider a finite field F of order p^n (p prime, $n \geqq 1$). A straightforward computation shows that for any factor d of n,

$$[\boldsymbol{L}_F \cup \{x^{p^d}\}] = \{a_0 + \sum_{i=1}^{k} \sum_{j=0}^{n/d-1} a_{ij} x_i^{p^{dj}} \mid k \geqq 1,\ a_0, a_{ij} \in F\}\,.$$

This closed class will be denoted by $\boldsymbol{Q}_F^d$. In particular, for $d = 1$ and $d = n$ we have $\boldsymbol{Q}_F^1 = \boldsymbol{Q}_F$ (cf. Theorem 2.2) and $\boldsymbol{Q}_F^n = \boldsymbol{L}_F$. Clearly, the closed classes $\boldsymbol{Q}_F^d$ form a lattice under the set inclusion which is isomorphic to the lattice of divisors of n.

Theorem 3.1. *Let F be a finite field of order p^n (p prime, $n \geqq 1$). Then for any closed class $\boldsymbol{C}$ with $\boldsymbol{L}_F \subseteq \boldsymbol{C} \subset \boldsymbol{O}_F$, there exists a factor d of n such that $\boldsymbol{C} = \boldsymbol{Q}_F^d$.*

Corollary 3.2. *If the canonical factorization of n is $n = p_1^{k_1} \ldots p_r^{k_r}$ then the closed class $\boldsymbol{L}_F$ is of height $k_1 + \ldots + k_r + 1$.*

Theorem 3.1 immediately follows from the next two lemmas.

Lemma 3.3. *For any finite field F, $\boldsymbol{Q}_F$ is the unique maximal clone $\boldsymbol{L}_F$ is contained in.*

Proof. First we show that $\boldsymbol{L}_F \nsubseteq \mathrm{Pol}\,\varrho$ if ϱ is a relation of the type (α), (β), (δ), (ε) or (ζ). To this end it suffices to construct a non-singular square matrix M_ϱ with the

first row $\langle 1, \ldots, 1\rangle$ (1 is the identity element of F) and all other rows belonging to ϱ. Indeed, suppose $\varrho \subset F^k$ $(k \geqq 1)$ is an arbitrary relation and $M_\varrho = (m_{ij})_{i,j<k}$ is the required non-singular $k \times k$ matrix such that $m_{0j} = 1$ $(j = 0, \ldots, k-1)$. Furthermore, let $\langle m_0, \ldots, m_{k-1}\rangle \in F^k - \varrho$. Denote by $a_0, \ldots, a_{k-1}$ the solution of the system of linear equations

$$\sum_{i<k} \xi_i m_{ij} = m_j \quad (j < k),$$

and consider the operation $f \in \boldsymbol{L}_F$ defined by

$$f(x_1, \ldots, x_{k-1}) = a_0 + \sum_{i=1}^{k-1} a_i x_i .$$

Then the rows of the $(k-1) \times k$ matrix

$$\begin{pmatrix} m_{1,0} & \ldots & m_{1,k-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ m_{k-1,0} & \ldots & m_{k-1,k-1} \end{pmatrix}$$

belong to ϱ, while the row $\langle m_0, \ldots, m_{k-1}\rangle$ of column values of f fails to belong to ϱ. Thus $f \notin \mathrm{Pol}\,\varrho$, consequently, $\boldsymbol{L}_F \nsubseteq \mathrm{Pol}\,\varrho$.

It remains to describe the matrices M_ϱ corresponding to the relations of types $(\alpha), (\beta), (\delta), (\varepsilon)$ and (ζ). If ϱ is of type $(\alpha), (\beta)$ or (δ) then there exist elements $m, m' \in F$ such that $m \neq m'$ and $\langle m, m'\rangle \in \varrho$. Then the matrix

$$\begin{pmatrix} 1 & 1 \\ m & m' \end{pmatrix}$$

satisfies our requirements. If ϱ is a unary central relation, the matrix (1) is appropriate. Finally, if ϱ is a k-ary relation of type (ε) or (ζ) with $k \geqq 2$ or 3, respectively, then the $k \times k$ matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ m & m' & \ldots & m & m \\ \ldots\ldots\ldots\ldots & & & & \\ m & m & \ldots & m' & m \\ m & m & \ldots & m & m' \end{pmatrix}$$

meets our requirements provided $m, m' \in F$, $m \neq m'$ and m' belongs to the centre of ϱ if ϱ is of type (ε).

From the foregoing argument and Theorem 2.1 we can infer that $\boldsymbol{L}_{\langle F;+,\cdot\rangle} \subseteq \mathrm{Pol}\,\varrho$ for a relation of type (γ). We show that $\mathrm{Pol}\,\varrho = \boldsymbol{Q}_{\langle F;+\rangle}$. Let $\langle F; \oplus\rangle$ be the Abelian group determining ϱ. Clearly, for any elements $m_i \in F$ $(i = 1, 2, 3)$, the rows of the matrix

$$\begin{pmatrix} m_1 & m_2 & m_2 & m_1 \\ m_2 & m_2 & m_2 & m_2 \\ m_2 & m_3 & m_2 & m_3 \end{pmatrix}$$

belong to ϱ, so that the column values of the ternary operation $x_1 - x_2 + x_3 \in$

$\in \boldsymbol{L}_{\langle F;+,\cdot\rangle}$ must also belong to ϱ. This means that

$$\langle m_1, m_3, m_2, m_1 - m_2 + m_3\rangle \in \varrho\,, \quad \text{i.e.}$$

$$m_1 \ominus m_2 \oplus m_3 = m_1 - m_2 + m_3 \quad (m_i \in F,\ i = 1, 2, 3)\,.$$

Hence ϱ coincides with the relation of type (γ) determined by $\langle F; +\rangle$, implying that $\operatorname{Pol}\varrho = \boldsymbol{Q}_{\langle F;+\rangle}$, which was to be proved.

Lemma 3.4. *Let F be a finite field of order p^n (p prime, $n \geqq 1$). Then for any closed class $\boldsymbol{C}$ with $\boldsymbol{L}_F \subseteq \boldsymbol{C} \subseteq \boldsymbol{Q}_F$, there exists a factor d of n such that $\boldsymbol{C} = \boldsymbol{Q}_F^d$.*

Proof. First we show that whenever $\sum_{i<n} a_i x^{p^i} \in \boldsymbol{C}$ and $j < n$ such that $a_j \neq 0$, then $x^{p^j} \in \boldsymbol{C}$. We do this by eliminating successively all nonzero coefficients a_l with $l \neq j$ $(l < n)$. One step consists in constructing, for any $k \neq j$ $(k < n)$ with $a_k \neq 0$, a function $\sum_{i<n} b_i x^{p^i} \in \boldsymbol{C}$ with the properties

(i) $b_j = 1$ and $b_k = 0$;

(ii) $b_i = 0$ whenever $a_i = 0$.

Select a generator a of the multiplicative group of F. Then for any $a', a'' \in F$ the operation

$$a' \sum_{i<n} a_i x^{p^i} + a'' \sum_{i<n} a_i (ax)^{p^i} = \sum_{i<n} a_i (a' + a^{p^i} a'')\, x^{p^i}$$

belongs to $\boldsymbol{C}$ and its coefficients $b_i = a_i(a' + a^{p^i}a'')$ have the property (ii). On the other hand, since the matrix

$$\begin{pmatrix} a_k & a_k a^{p^k} \\ a_j & a_j a^{p^j} \end{pmatrix}$$

is non-singular (by the choice of a), there exist a' and a'' such that (i) is satisfied as well.

Now let us introduce the following notation:

$$I = \{j \mid 0 < j \leqq n,\ x^{p^j} \in \boldsymbol{C}\}\,, \quad d = \min I\,.$$

(Notice that we take x^{p^n} instead of x.) In the previous paragraph we proved that

$$\boldsymbol{C} = [\boldsymbol{L}_F \cup \{x^{p^j} \mid j \in I\}]\,. \tag{1}$$

Since for the greatest common divisor (i, j) of any two elements $i, j \in I$ there exist positive integers q, r, s such that $(i, j) + ns = iq + jr$, implying that

$$x^{p^{(i,j)}} = \left(x^{(p^n)^s}\right)^{p^{(i,j)}} = x^{p^{(i,j)+ns}} = x^{p^{iq+jr}} = \left(x^{(p^i)^q}\right)^{(p^j)^r} \in [x^{p^i}, x^{p^j}]\,,$$

therefore I is closed under taking the greatest common divisors of its members. Hence d divides the elements of I, in particular, it divides n. Thus $x^{p^j} \in [x^{p^d}]$ for any $j \in I$, so that

$$[x^{p^d}] \subseteq [x^{p^j} \mid j \in I] \subseteq [x^{p^d}]\,,$$

i.e., by (1) and by the definition of Q_F^d,

$$C = [L_F \cup \{x^{p^d}\}] = Q_F^d ,$$

completing the proof.

4. CLOSED SUBCLASSES OF L_F

Let F be a finite field and E a subfield of F; in symbols: $E \leqq F$. A subset of F will be called an *affine E-subspace* of F if it is closed with respect to the operations

$$\sum_{i=1}^{k} a_i x_i ; \quad k \geqq 1 , \quad a_i \in E \ (i = 1, \ldots, k) , \quad \sum_{i=1}^{k} a_i = 1 .$$

Equivalently, $S \subseteq F$ is an affine E-subspace of F iff $S = V + a$ for an element $a \in F$ and a subspace V of F, considered as a vector space over E. Denote by $\mathfrak{S}_E$ the family of affine E-subspaces of F. Furthermore, put $\mathfrak{S}_E^0 = \{S \in \mathfrak{S}_E \mid 0 \in S\}$, i.e. $\mathfrak{S}_E^0$ is the family of E-subspaces of F. For $S \in \mathfrak{S}_E$ and $S^0 \in \mathfrak{S}_E^0$, set

$$I(E, S) = \{ \sum_{i=1}^{k} a_i x_i + a_0 \mid k \geqq 1, \ a_i \in E \ (i = 1, \ldots, k) \quad \text{and} \quad a_0 = s - (\sum_{i=1}^{k} a_i) s' \quad \text{for some} \quad s, s' \in S \}$$

and

$$T(E, S^0) = \{ \sum_{i=1}^{k} a_i x_i + a_0 \mid k \geqq 1, \ a_i \in E \ (i = 1, \ldots, k) , \ \sum_{i=1}^{k} a_i = 1 \text{ and } a_0 \in S^0 \} .$$

A straightforward computation shows that $I(E, S)$ and $T(E, S^0)$ are subclones of O_F. Notice that $I(E, S)$ consists of those operations in $I(E, F)$ under which S is invariant.

Theorem 4.1. *For any finite field F, the non-unary closed subclasses of L_F are the following: $I(E, S)$ with $E \leqq F$ and $S \in \mathfrak{S}_E$, and $T(E, S^0)$ with $E \leqq F$ and $S^0 \in \mathfrak{S}_E^0$.*

Remark. The closed classes listed above are pairwise different; moreover, for any subfields E_i of F and for any $S_i \in \mathfrak{S}_E$, $S_i^0 \in \mathfrak{S}_E^0$ $(i = 1, 2)$, we have

$$\begin{aligned}
I(E_1, S_1) &\subseteq I(E_2, S_2) \quad \text{iff} \quad E_1 \leqq E_2 \quad \text{and} \quad S_1 \subseteq S_2 , \\
T(E_1, S_1^0) &\subseteq T(E_2, S_2^0) \quad \text{iff} \quad E_1 \leqq E_2 \quad \text{and} \quad S_1^0 \subseteq S_2^0 , \\
T(E_1, S_1^0) &\subseteq I(E_2, S_2) \quad \text{iff} \quad E_1 \leqq E_2 \quad \text{and} \quad S_1^0 \subseteq S_2 - S_2 , \\
I(E_1, S_1) &\subseteq T(E_2, S_2^0) \quad \text{never holds} .
\end{aligned}$$

Corollary 4.2. *For any finite field F, the closed class L_F has finitely many closed subclasses.*

Proof. In view of Theorem 4.1, $\boldsymbol{L}_F$ has finitely many non-unary closed subclasses. As regards the unary closed subclasses of $\boldsymbol{L}_F$, they are uniquely determined by their semigroups of unary operations and by their having or not having a binary constant operation or a binary projection. Hence $\boldsymbol{L}_F$ possesses only finitely many unary closed subclasses.

Now we turn to the proof of Theorem 4.1. As a preparation we establish two lemmas. In the first one we formulate a more general statement than is actually needed in this note. In this form it is a slight improvement of [12; Theorem 3].

Let R be a ring with 1 and M a faithful unitary left R-module. For any unitary subring T of R and any T-submodule N of $T \times M$ we define a closed subclass, in fact, a subclone of $\boldsymbol{L}_M$ (see the definition in Section 2) as follows:

$$\boldsymbol{K}(T, N) = \{ \sum_{i=1}^{k} r_i x_i + m \mid k \geqq 1,\ r_i \in T (i = 1, \ldots, k),\ \langle 1 - \sum_{i=1}^{k} r_i, m \rangle \in N \} .$$

Lemma 4.3. *Let M be a faithful unitary left module over a ring R with identity. Then for any closed subclass $\boldsymbol{C}$ of $\boldsymbol{L}_M$ containing the operation $x_1 - x_2 + x_3$, there exists a unique subring T of R and a unique T-submodule N of $T \times M$ such that $\boldsymbol{C} = \boldsymbol{K}(T, N)$.*

Proof. Uniqueness is an immediate consequence of the definition, so we can confine ourselves to the proof of existence. Let $\boldsymbol{C}$ be a closed class satisfying the hypotheses of Lemma 4.3. Clearly, $\boldsymbol{C}$ is a subclone of $\boldsymbol{L}_M$. Put

$$T = \{ r \in R \mid r x_1 + (1 - r) x_2 \in \boldsymbol{C} \} ,$$
$$N = \{ \langle r, m \rangle \mid (1 - r) x_1 + m \in \boldsymbol{C} \} .$$

Suppose $r, r' \in T$, $\langle r_i, m_i \rangle \in N$ $(i = 1, 2)$. Then

$$1 x_1 + 0 x_2 = x_1 - x_2 + x_2 \in \boldsymbol{C} ,$$
$$(r - r') x_1 + (1 - r + r') x_2 = (r x_1 + (1 - r) x_2) - (r' x_1 + (1 - r') x_2) + x_2 \in \boldsymbol{C} ,$$
$$r r' x_1 + (1 - r r') x_2 = r(r' x_1 + (1 - r') x_2) + (1 - r) x_2 \in \boldsymbol{C} ,$$

implying that T is a unitary subring of R. Furthermore,

$$r_1 x_1 + (1 - r_1) x_2 = ((1 - r_1) x_2 + m_1) - ((1 - r_1) x_1 + m_1) + x_1 \in \boldsymbol{C} ,$$
$$(1 - r_1 + r_2) x_1 + m_1 - m_2 =$$
$$= ((1 - r_1) x_1 + m_1) - ((1 - r_2) x_1 + m_2) + x_1 \in \boldsymbol{C}$$

and

$$(1 - r r_1) x_1 + r m_1 = r((1 - r_1) x_1 + m_1) + (1 - r) x_1 \in \boldsymbol{C} ,$$

so that $N \subseteq T \times M$ is in fact a T-submodule.

We show that $\boldsymbol{C} = \boldsymbol{K}(T, N)$. Assume first $\sum_{i=1}^{k} r_i x_i + m \in \boldsymbol{C}$. Then

$$(\sum_{i=1}^{k} r_i) x_1 + m \in \boldsymbol{C}$$

and for any $j = 1, \ldots, k$,

$$r_j x_1 + (1 - r_j) x_2 = (\sum_{i=1}^{k} r_i x_1 + m) - (\sum_{\substack{i=1 \\ i \neq j}}^{k} r_i x_1 + r_j x_2 + m) + x_2 \in \boldsymbol{C},$$

whence $\langle 1 - \sum_{i=1}^{k} r_i, m \rangle \in N$ and $r_j \in T$ $(j = 1, \ldots, k)$, i.e. $\sum_{i=1}^{k} r_i x_i + m \in \boldsymbol{K}(T, N)$. Conversely, let $\sum_{i=1}^{k} r_i x_i + m \in \boldsymbol{K}(T, N)$. Then, by definition, $(\sum_{i=1}^{k} r_i) x_1 + m \in \boldsymbol{C}$ and $r_j x_1 + (1 - r_j) x_2 \in \boldsymbol{C}$ $(j = 1, \ldots, k)$. Since $x_1 - x_2 + x_3 \in \boldsymbol{C}$, by induction on n it follows that $\pi_n = \sum_{i=1}^{n} 1 \cdot x_i - (n - 1) x_{n+1} \in \boldsymbol{C}$. Consequently, substituting in π_{k+1} the operation $r_i x_i + (1 - r_i) x_1 (\in \boldsymbol{C})$ for x_i $(i = 1, \ldots, k)$, the operation $(\sum_{i=1}^{k} r_i) x_1 + m (\in \boldsymbol{C})$ for x_{k+1} and x_1 for x_{k+2}, we get that

$$\sum_{i=1}^{k} r_i x_i + m = \sum_{i=1}^{k} (r_i x_i + (1 - r_i) x_1) + (\sum_{i=1}^{k} r_i) x_1 + m - k x_1 \in \boldsymbol{C},$$

concluding the proof of Lemma 4.3.

Lemma 4.4. *For any finite field F, the non-unary closed subclasses of $\boldsymbol{L}_F$ contain the ternary operation $x_1 - x_2 + x_3$.*

Proof. Suppose F is a field of order p^n (p prime, $n \geqq 1$). We have to prove that for any operation $f \in \boldsymbol{L}_F$ depending on at least two of its variables, the closed class $[f]$ generated by f contains the operation $x_1 - x_2 + x_3$. First we show that $[f]$ contains a nontrivial idempotent operation. Let $f \in \boldsymbol{L}_F \cap \boldsymbol{O}_F^{(k)}$, $k \geqq 2$,

$$f(x_1, \ldots, x_k) = \sum_{i=1}^{k} a_i x_i + a_0$$

and, say, $a_1, a_2 \neq 0$. Set $a = \sum_{i=1}^{k} a_i$. We can assume that $a \neq 0$, for $a = 0$ implies the sum of the coefficients of $f * f$ to be $-a_1 (\neq 0)$. Thus $a x_1 + a_0 \in [f]$ and by induction on m it follows that

$$a^m x_1 + (a^{m-1} + \ldots + a + 1) a_0 \in [f].$$

In particular, this holds for $m = p^n - 2$, too, so that since $a^{p^n - 1} = 1$, the operation

$$a^{p^n - 2} (\sum_{i=1}^{k} a_i x_i + a_0) + (a^{p^n - 3} + \ldots + a + 1) a_0 \in [f]$$

depends on at least two of its variables and has coefficients whose sum is 1, i.e. we have an operation

$$\sum_{i=1}^{k} a_i' x_i + a_0' \in [f] \quad \text{with} \quad \sum_{i=1}^{k} a_i' = 1, \quad a_1', a_2' \neq 0.$$

However, then $x_1 + a_0' \in [f]$, hence $x_1 + m a_0' \in [f]$ for $m = 1, 2, \ldots$, in particular, for $m = p - 1$, too, whence

$$\sum_{i=1}^{k} a_i' x_i = (\sum_{i=1}^{k} a_i' x_i + a_0') + (p - 1) a_0'$$

is a nontrivial idempotent operation in $[f]$.

Once this is established, our result follows immediately from the description in [13] of the idempotent closed subclasses of $\boldsymbol{L}_M$ for any finite unitary module M. Here we present a direct proof.

We have to prove that the ternary operation $x_1 - x_2 + x_3$ belongs to $[f]$ for any nontrivial idempotent operation f in $\boldsymbol{L}_F$. Let $f \in \boldsymbol{L}_F \cap \boldsymbol{O}_F^{(k)}$, $k \geqq 2$,

$$f(x_1, \ldots, x_k) = \sum_{i=1}^{k} a_i x_i, \quad a_i \in F, \quad \sum_{i=1}^{k} a_i = 1.$$

We may suppose $a_i \neq 0$ $(i = 1, \ldots, k)$. If $a_i = 1$ for all $i = 1, \ldots, k$ and $p = 2$ then, clearly, k is odd and $x_1 - x_2 + x_3 \in [f]$. Otherwise, $[f]$ contains a nontrivial binary idempotent operation $(a_i x_1 + (1 - a_i) x_2$ if $a_i \neq 1$ or $2x_1 - x_2$ if $a_i = 1$ for all i). It suffices to prove that $x_1 - x_2 + x_3 \in [ax_1 + (1 - a) x_2]$ whenever $a \in F$ with $a(1 - a) \neq 0$. Let us denote the closed class $[ax_1 + (1 - a) x_2]$ by $\boldsymbol{C}(a)$. By induction on m it is easy to verify that

$$a^m x_1 + (1 - a^m) x_2 = a(a^{m-1} x_1 + (1 - a^{m-1}) x_2) + (1 - a) x_2 \in \boldsymbol{C}(a)$$
$$(m = 1, 2, \ldots)$$

and, similarly,

$$(1 - (1 - a)^m) x_1 + (1 - a)^m x_2 \in \boldsymbol{C}(a) \quad (m = 1, 2, \ldots).$$

Thus, taking into consideration that $a^{p^n - 1} = (1 - a)^{p^n - 1} = 1$ holds in F, we have

$$x_1 - x_2 + x_3 = a(a^{p^n - 2} x_1 + (1 - a^{p^n - 2}) x_2) +$$
$$+ (1 - a)((1 - (1 - a)^{p^n - 2}) x_2 + (1 - a)^{p^n - 2} x_3) \in \boldsymbol{C}(a).$$

This completes the proof of the lemma.

Proof of Theorem 4.1. Lemmas 4.3 and 4.4 immediately imply that for any non-unary closed subclass $\boldsymbol{C}$ of $\boldsymbol{L}_F$ there exist a subfield E of F and an E-subspace V of the vector space $E \times F$ (over E) such that $\boldsymbol{C} = \boldsymbol{K}(E, V)$. We show that $\boldsymbol{K}(E, V)$ coincides with one of the closed classes listed in the theorem.

Let us introduce the following notation:

$$V_1 = \{u \in E \mid \langle u, v \rangle \in V \text{ for some } v \in F\},$$
$$V_2[e] = \{v \in F \mid \langle e, v \rangle \in V\} \quad (e \in E).$$

Since V is an E-subspace of $E \times F$, V_1 is an ideal of E and $V_2[e] \in \mathfrak{S}_E$ for every $e \in E$. Thus the following two cases are to be considered.

Case 1. If $V_1 = E$ then $\boldsymbol{K}(E, V) = \boldsymbol{I}(E, V_2[1])$. Indeed, an operation $\sum_{i=1}^{k} a_i x_i + a_0$ belongs to $\boldsymbol{K}(E, V)$ if and only if $a_i \in E$ $(i = 1, \ldots, k)$ and $\langle 1 - \sum_{i=1}^{k} a_i, a_0 \rangle \in V$. On the other hand, $\sum_{i=1}^{k} a_i x_i + a_0 \in \boldsymbol{I}(E, V_2[1])$ if and only if $a_i \in E$ $(i = 1, \ldots, k)$ and $a_0 = v - \sum_{i=1}^{k} a_i v'$ for some $v, v' \in V_2[1]$. Now,

$$\langle 1 - \sum_{i=1}^{k} a_i, a_0 \rangle = \langle 1, a_0 + \sum_{i=1}^{k} a_i v' \rangle - \sum_{i=1}^{k} a_i \langle 1, v' \rangle \in V$$

for some $v' \in V_2[1]$ if and only if $a_0 + \sum_{i=1}^{k} a_i v' = v \in V_2[1]$, which proves the required identity.

Case 2. If $V_1 = \{0\}$ then $V = \{0\} \times V_2[0]$ and, clearly, $V_2[0] \in \mathfrak{S}_E^0$. Thus the identity $\boldsymbol{K}(E, V) = \boldsymbol{T}(E, V_2[0])$ follows immediately from the definitions.

The proof of the theorem is complete.

Finally, we note that the inclusion properties formulated in the Remark after Theorem 4.1 can be derived from the definitions, taking into consideration that for a constant operation c_s with value $s(\in F)$, $c_s \in \boldsymbol{I}(E, S)$ iff $s \in S$, while for a translation $x_1 + s$ $(s \in F)$, $x_1 + s \in \boldsymbol{T}(E, S^0)$ iff $s \in S^0$.

References

[1] *J. Demetrovics - J. Bagyinszki:* The lattice of linear classes in prime-valued logics, Banach Center Publications, to appear.

[2] *J. Demetrovics - L. Hannák:* The cardinality of closed sets in pre-complete classes in k-valued logics, Acta Cybernetica, *4* (1979), 273—277.

[3] *J. Demetrovics - L. Hannák:* On the cardinality of self-dual closed classes in k-valued logics, MTA SZTAKI Közlemények, *22* (1979), 7—18.

[4] *Г. П. Гаврилов:* О мощности множеств замкнутых классов конечной высоты в $P_{\aleph_0}$, Д.А.Н. СССР, *158* (1964), 504—506.

[5] *D. Lau:* Über die Anzahl von abgeschlossenen Mengen linearer Funktionen der n-wertigen Logik, EIK, *14* (1978), 567—569.

[6] *С. С. Марченков:* О замкнутых классах автодуалных функций в k-значных логиках, Проблемы Кибернетики, *36* (1979), 5—22.

[7] *I. G. Rosenberg:* La structure des fonctions de plusieurs variables sur un ensemble fini, C.R. Acad. Sci. Paris Ser A, *260* (1965), 3817—19.

[8] *I. G. Rosenberg:* Über die funktionale Vollständigkeit in dem mehrwertigen Logiken (Struktur der Funktionen von mehreren Veränderlichen auf endlichen Mengen), Rozpravy Čs. Akademie Věd. Ser. Math. Nat. Sci., *80* (1970), 3—93.

[9] *I. G. Rosenberg:* Completeness properties of multiple-valued logic algebras; in: Computer Science and Multiple-valued Logic. Theory and Applications (ed. D. C. Rine), North Holland, Amsterdam—New York—Oxford, 1977.

[10] *A. A. Salomaa:* On infinitely generated sets of operations in finite algebras, Ann. Univ. Turku Ser. A, *74* (1964), 1—12.

[11] *A. A. Salomaa:* On the heights of closed sets of operations in finite algebras, Ann. Acad. Sci. Fenn. Ser. A, *363* (1965), 1—12.

[12] *Á. Szendrei:* On affine modules, in: Contribution to Universal Algebra, Colloq. Math. Soc. J. Bolyai, vol. *17*, 457—464; North Holland (1977).

[13] *Á. Szendrei:* Idempotent reducts of modules I—II, in: Universal Algebra, Colloq. Math. Soc. J. Bolyai, vol. *23*, to appear.

[14] *Ю. И. Янов - А. А. Мучник:* О существовании k-значных замкнутых классов, не имеющих конечного базиса, ДАН СССР, *127* (1958), 44—46.

Author's address: Bolyai Intézet, Szeged, Aradi vértanúk tere 1, H-6720 Hungary.