DISCRETE MATHEMATICS
BANACH CENTER PUBLICATIONS, VOLUME 7
PWN—POLISH SCIENTIFIC PUBLISHERS
WARSAW 1982

THE LATTICE OF LINEAR CLASSES IN PRIME-VALUED LOGICS

JÀNOS DEMETROVICS

Computer and Automation Institute, Hungarian Academy of Sciences, Budapest, Hungary

JÀNOS BAGYINSZKI

Central Research Institute for Physics, Hungarian Academy of Sciences, Budapest, Hungary

1. Introduction

In this paper we study the superposition of certain linear functions. The complete lattice of closed classes for 2-valued logics was given by E. Post in 1921 ([8], [6]). Several results about closed and maximal sets in P_k for $k \geqslant 3$ were given in a paper of Jablonskiĭ in 1958 [5]. All maximal sets in P_3 were determined by Jablonskiĭ in 1953 [5]. According to a result of Janov and Mučnik [7], in k-valued logics, for $k \geqslant 3$, there are both closed subsets infinitely generated and a continuum of closed subsets, unlike the case $k = 2$. Consequently, Post's method of determining all closed subsets in P_k cannot be successful for $k \geqslant 3$.

Still we think that in spite of these principal difficulties the structure of P_k is "almost completely" describable. In our opinion, the whole structure—except some sublattices of cardinality continuum which are well separated in the complete lattice—can be described. This is in accordance with a result of Salomaa ([12], Theorem 8) stating within a "large enough" (but not sequentially infinite) distance from the identity P_k there are only countably many elements of the lattice.

The method of Post consists of the following steps:

(1) determine a base set B of the closed set P,

(2) determine maximal sets P' in P,

(3) prove that all maximal sets are given in step 2.

Ivo Rosenberg presented all maximal sets in P_k, $k \geqslant 3$, by a sieve method in relation terminology in 1965 [10]. Infinitely generated maximal sets contained only in finitely generated closed sets were constructed by Salomaa at 1964, [11], and also some maximal classes in $L(k)$ with the proof that $L(p)$'s have only a finite number of closed subsets, where p is a prime number.

This is the state of k-valued logics in brief. We rediscovered the results of Salomaa about $L(p)$ (as we had not known about it) [1]. Moreover, our paper contains

(a) The complete lattice of closed linear classes in $L(p)$, and therefore the exact (finite) number of these classes;

(b) All bases with a minimal number of elements and the rank of each linear class;

(c) The lengths of the maximal and minimal chains of the lattice.

In preprint [2] we deal with a (regular) language-representation of linear classes. A forthcoming paper presents the corresponding complete lattice for a generalized case where the number k is square free [3].

For integer $k \geq 2$, let $V_0 = \{0, 1, \ldots, k-1\}$, $V = V_0 \setminus \{0\}$, $P_k^{(n)} = \{f \mid f(x_1, \ldots, x_n): V_0^n \to V_0\}$, $n = 1, 2, \ldots$, and let $P_k = \bigcup_{n=0}^{\infty} P_k^{(n)}$, where $P_k^{(0)}$ is the set of constant functions. In this paper addition "+" and multiplication "$\cdot$" are carried out modulo k. The main purpose of this paper is to investigate the set of linear functions (= linear polynomial functions) over the ring $R_0 = \langle V_0, +, \cdot \rangle$. This set is denoted by $L(k)$. It is known that for a commutative ring R with identity, which is not a field, there are functions $f \in P_k$ that are not R-polynomials, but for a field R each element of P_k is an R-polynomial function [9]. It is also known [5] that $L(k)$ is maximal in P_k if and only if $k = p$ is prime. We shall also use the fact that $a^{p-1} = 1 (\mathrm{mod}\, p)$ by the Fermat principle, and therefore the value $x = a^{p-2}$ is a solution of the equation $ax = 1 (\mathrm{mod}\, p)$.

Let

$$\tilde{x} = (x_1, \ldots, x_n), \quad E(\tilde{x}) = \{e \mid e = e_j(\tilde{x}) = x_j, 1 \leq j \leq n\}.$$

Superpositions over the set $P \subseteq P_k$ are functions obtained from P by using the operation $f(x_1, \ldots, x_n) \,\Box_i\, g(y_1, \ldots, y_m) = f(x_1, \ldots, x_{i-1}, g(y_1, \ldots, y_m), x_{i+1}, \ldots, x_n)$ with $f \in P$, $g \in P \cup E(\tilde{x})$ a finite number of times.

The *closure* $[P]$ of a subset $P \subseteq P_k$ is the set of all superpositions over P.

A set $P \subseteq P_k$ is said to be a *closed set* if $[P] = P$. Let $P \subseteq P_k$ be a closed set, $P', P'' \subseteq P$. The set P' is *complete in* P if $[P'] = P$. The set P' is a *base in* P if $[P'] = P$ and $[P''] \neq P$ for $P' \setminus P'' \neq \emptyset$, $P'' \subseteq P'$.

The closed set P' is *maximal* (= *precomplete*) *in* P if for every $P'' \neq P'$, $P' \subset P'' \subseteq P$, the equality $[P''] = P$ holds. It can be checked that the following sets are closed subsets of linear functions (with the notation: $a_0 \in V_0$, $a_i \in V$ for $i \geq 1$, $\sum_{i=1}^{n} a_i = a$, $f(\tilde{x}) = a_0 + a_1 x_1 + \ldots + a_n x_n$):

$$L(k) = \{f(\tilde{x}) \mid n = 1, 2, \ldots\} \cup P_k^{(0)},$$
$$L_\Delta = \{f(\tilde{x}) \mid a = 1, n = 1, 2, \ldots\},$$
$$L_\alpha = \{f(\tilde{x}) \mid f(\alpha, \alpha, \ldots, \alpha) = \alpha, \quad n = 1, 2, \ldots\} \cup \{\alpha\}, \quad \alpha = 0, 1, \ldots, k-1,$$
$$L^{(1)} = \{a_0 + a_1 x_1\} \cup P_k^{(0)},$$
$$L^{(0)} = P_k^{(0)},$$

$$L^{(1)} \setminus L^{(0)} = \{a_0 + a_1 x_1\},$$
$$L_{\Delta\alpha} = L_\Delta \cap L_\alpha = L_{\Delta 0},$$
$$L_\Delta^{(1)} = L_\Delta \cap L^{(1)} = \{x, x+1, \ldots, x+k-1\},$$
$$L_\alpha^{(1)} = L_\alpha \cap L^{(1)} = \{a_0 + a_1 x_1 \mid a_0 = \alpha(1-a_1)\} \cup \{\alpha\}; \quad \alpha = 0, 1, \ldots, k-1,$$
$$L_\alpha^{(1)} \setminus \{\alpha\} = L_\alpha \cap (L^{(1)} \setminus L^{(0)}); \quad \alpha = 0, 1, \ldots, k-1,$$
$$L_\alpha^{(0)} = L_\alpha \cap L^{(0)} = \{\alpha\}; \quad \alpha = 0, 1, \ldots, k-1,$$
$$L_\alpha^{(1)} \cup L^{(0)}, \quad \alpha = 0, 1, \ldots, k-1.$$

Remarks. (1) $L^{(n)}$ is not a closed subset of $L(k)$ for $n \geq 2$.

(2) The closedness of the subsets $L_{\Delta\alpha}$, $L_\Delta^{(1)}$, $L_\alpha^{(1)}$, $L_\alpha^{(1)} \setminus \{\alpha\}$, $L_\alpha^{(0)}$ is a consequence of the fact that the lattice of subalgebras of an algebra is also closed under the (set-theoretical) intersection "$\cap$".

It is a well-known theorem in algebra that every partially ordered set H having both $\sup(h_1, h_2)$ and $\inf(h_1, h_2)$ for all elements $h_1, h_2 \in H$ constitutes a lattice.

Let $\mathscr{L}$ denote the class of closed subsets of $L(k)$. Because of the fact that in the set $\mathscr{L}$ with partial ordering there are elements $\sup(L', L'')$ and $\inf(L', L'')$ for every $L', L'' \in \mathscr{L}$, we infer that $\langle \mathscr{L} \cup \emptyset, \subseteq \rangle$ is a lattice.

THEOREM 1. *If $k = p$ is a prime number, then $\langle \mathscr{L} \cup \emptyset, \subseteq \rangle$ is a finite lattice with the identity $L(p)$ and zero element $\emptyset$ (empty set).*

To prove this statement, we shall present the exact finite cardinal number $|\mathscr{L}|$ in Theorem 15.

The lattice $\langle \mathscr{L} \cup \emptyset, \subseteq \rangle$ for $p = 2$ is given in Fig. 1. (This is a sublattice of the Post lattice.)

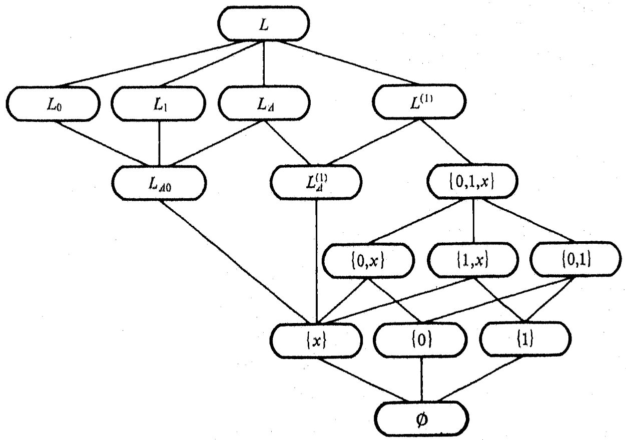

Fig. 1

We may assume further that $k = p \geqslant 3$ (prime number). The next four lemmas are useful. The proofs are omitted, except in Lemma 3.

LEMMA 1. *For elements of* $L^{(1)}$ *we have*:

(a) $a_0+x \in L_\alpha^{(1)}$ *if and only if* $a_0 = 0$, *for* $\alpha = 0, 1, \ldots, p-1$;

(b) $a_0+ax \in L_\alpha^{(1)}$, $a > 1$ *if and only if* $a_0 = \alpha(1-a)$ *for* $\alpha = 0, 1, \ldots, p-1$;

(c) $a_0 \in L_\alpha^{(1)}$ *if and only if* $a_0 = \alpha$. ∎

LEMMA 2. *Let* L' *be one of the sets* L_Δ, L_α, $L^{(1)}\setminus L^{(0)}$, $L_\Delta^{(1)}$, $L_\alpha^{(1)}$, *and* $f \notin L'$, $g \in L'$. *Then* $g \,\square\, f \notin L'$. ∎

LEMMA 3. *Let* $f(x_1, x_2) = a_0+a_1x_1+a_2x_2$, $a_2^h = 1$, $h \geqslant 2$, $a_2^j > 1$, *if* $1 \leqslant j < h$. *Then the functions*

$$f_0(x_1, x_2, x_3) = a_{0h}+a_1x_1+a_{1h}x_2+x_3$$

and

$$g_0(x_1, x_2, x_3) = b_{0h}+b_{1h}x_1+x_2+x_3$$

are contained in $[\{f(x_1, x_2)\}]$ *with*

$$T_h = 1+a_2+\ldots+a_2^{h-1}, \quad a_{0h} = a_0T_h, a_{1h} = a_1(T_h-1),$$

$$b_{0h} = a_0a_1^{p-2}T_h, \quad b_{1h} = T_h-1.$$

Proof. With the notation

$$f_1(x_1, x_2) = f(x_1, x_2), \quad f_{m+1}(x_1, x_2) = f(x_1, f_m(x_1, x_2)), \ m \geqslant 1,$$

$$f_0^{n+1}(x_1, x_2, x_3) = f_0(x_1, x_2, f_0^n(x_1, x_2, x_3))$$

the functions $f_0(x_1, x_2, x_3) = f(x_1, f_{h-1}(x_2, x_3))$ and $g_0(x_1, x_2, x_3) = f_0^{n_0}(x_2, x_1, x_3)$, $n_0 = a_1^{p-2}$, are obtained. ∎

LEMMA 4. $[\{a_0+x\}] = L_\Delta^{(1)}$ *if and only if* $a_0 \neq 0$.

From the definitions and Lemma 1 we have $L(k) = L_\Delta = L_\Delta \cup \bigcup_{\alpha=0}^{k-1} L_\alpha$. ∎

2. Bases, maximal sets in $L(p)$, and bases of those maximal sets

It is a well-known fact that the set $\{x+1, x+y\}$ is a base of $L(k)$ for every $k \geqslant 2$. In the next theorem we give all bases of $L(p)$ having a function from $L^{(2)}$ and a function from $L^{(0)}$.

THEOREM 2. *The following sets are bases in* $L(p)$ (*with the notation* $f = f(x_1, x_2) = a_0+a_1x_1+a_2x_2$):

(a) $\{f, b_0, c_0\}, \quad a = 1, a_0 = 0, b_0 \neq c_0;$

(b) $\{f, b_0\}, \quad a = 1, a_0 \neq 0;$

(c) $\{f, b_0\}, \quad a \neq 1, b_0 \neq (p-a_0)(a-1)^{p-2}.$

Proof. We shall generate the base $\{x+1, x+y\}$.

(a)–(b): If $a = 1$, then $a_1 > 1$, $a_2 > 1$. Moreover,

$$\{x_1+x_2+(p-1)x_3, a_1x_1+(p-a_1)x_2+x_3\} \subseteq [\{f\}]$$

by Lemma 3. The function $x+1$ is obtained from $a_1b_0+(p-a_1)c_0+x_3 = a_1(b_0-c_0)+x_3$ in case (a) and from $x+a_0$ in case (b) by Lemma 4. We have the function $x_1+x_2+(p-1)b_0 = x_1+x_2+p-b_0$ and hence also the function x_1+x_2.

(c): If $a_1 = 1$ or $a_2 = 1$, for example $a_1 = 1$, then $a_0+x_1+a_2b_0 = a_0'+x_1$, with $a_0' = a_0+a_2b_0 \neq a_0+a_2(p-a_0)(a_1+a_2-1)^{p-2} = a_0+p-a_0 = 0$, therefore $x+1 \in [\{a_0'+x\}]$ by Lemma 4.

If $a_1 \geqslant 2$ and $a_2 \geqslant 2$, then $a_0'+a_1'x+y \in [\{f\}]$ holds with $a_1' \neq 0$ by Lemma 3. According to Lemma 1, $f \in L_\alpha$ for $\alpha = (p-a_0)(a-1)^{p-2}$, and this fact implies $a_0'+a_1'x+y \in L_\alpha$, therefore $a_0' = \alpha(1-(a_1'+1)) = \alpha(p-a_1') \neq 0$ if $a_0 \neq 0$ as in the previous case. If $a_0 = 0$, then $a_0' = 0$, $b_0 \neq (p-a_0)(a-1)^{p-2} = 0$; hence $[\{a_1'b_0+y\}] \ni x+1$ by Lemma 4. In both cases the function $x+y$ is obtained as at the points (a)–(b). To complete the proof, we must check the minimality of the sets in question. But it can be seen that

(1) $L'\setminus L^{(1)} = \emptyset$ implies $[L'] \neq L(k)$;

(2) $[\{x+y\}] \not\ni x+1$;

(3) $[\{a_1x_1+(1-a_1)x_2, b\}] \cap L^{(0)} = \{b\} \neq L^{(0)}$;

(4) $[\{a_0+a_1x_1+(1-a_1)x_2\}] \subseteq L_\Delta \neq L(p)$;

(5) $[\{a_0+a_1x_1+a_2x_2\}] \subseteq L_\alpha \neq L(p)$, $\alpha = (p-a_0)(a-1)^{p-2}$ if $a \neq 1$. ∎

COROLLARY. $[\{f(\tilde{x}), g_1(y), g_2(z)\}] = L(p)$ *for all* $f(\tilde{x}) \in L\setminus L^{(1)}$, $g_1(y)$, $g_2(z) \in L^{(0)}$.

The maximal classes in $L(p)$ are presented in the following theorem.

THEOREM 3. (a) *The classes* L_α *are maximal in* $L(p)$, $\alpha = 0, 1, \ldots, p-1$.

(b) *The class* L_Δ *is maximal in* $L(p)$.

(c) *The class* L^1 *is maximal in* $L(p)$.

Proof. It can be seen that the classes given in Theorem 3 are not complete in $L(p)$. Let us denote by L' one of the sets L_α, L_Δ, $L^{(1)}$, $h \in L\setminus L'$ and $\bar{h}(x) = h(x, x, \ldots, x)$.

In order to prove the theorem we shall generate over the set $\{h(\tilde{x})\} \cup L'$ a set $\{f(\tilde{x}), g_1(y), g_2(z)\}$ appearing in Corollary of Theorem 2.

(a) $f(\tilde{x}) = x_1+x_2+(p-\alpha) \in L_\alpha$, $g_1(y) = \alpha \in L_\alpha$, $g_2(z) = \bar{h}(\alpha) \in L^{(0)}$, $\bar{h}(\alpha) \neq \alpha$.

(b) If $\bar{h}(x) \in L^{(0)}$, then the functions $\bar{h}(y) = g_1(y)$, $g_2(z) = \bar{h}(z)+1$ ($x+1 \in L_\Delta$), $f(\tilde{x}) = x_1+(p-1)x_2 \in L_\Delta$ constitute a suitable set.

Let us suppose that $\bar{h}(x) = d_0+dx \notin L^{(0)}$; therefore $d > 1$. Then $f(\tilde{x}) \in L_\Delta\setminus L_\Delta^{(1)}$ holds for the function $f(\tilde{x}) = e_1x_1+e_2x_2$ with $e_1 = (d-1)^{p-2}+1$, $e_2 = p-e_1+1 = (1-d)^{p-2}$, hence the functions

$$f(x, h(x)) = e_1 x + e_2 h(\bar{x}) = e_2 d_0 + (e_1 + e_2 d)x$$
$$= e_2 d_0 + (1 + (d-1)e_2)x = e_2 d_0 = g_1(x) \in L^{(0)},$$
$$g_2(x) = g_1(x) + 1$$

are obtained.

(c) $f(\tilde{x}) = h(\tilde{x}), g_1(x) = 0, g_2(x) = 1$. ∎

To prove that all the maximal sets in $L(p)$ are given in Theorem 3, we need the bases of those maximal sets. A base with one element is the simplest one.

THEOREM 4. (1) *The set of base functions (bases with one element) in the set* L_α *is* $L_\alpha \setminus (L_\Delta \cup L^{(1)})$.

(2) *The set of base functions in the set* L_Δ *is* $L_\Delta \setminus (L_{\Delta 0} \cup L^{(1)})$.

(3) *The set of base functions in the set* $L_{\Delta 0}$ *is* $L_{\Delta 0} \setminus L^{(1)}$.

Proof. The necessity of the conditions is clear.

(1): We shall first prove that $f(\tilde{x}) = x_1 + x_2 + (p-\alpha)$ is a base function and second that for an arbitrary function $\tilde{y}g() \in L_\alpha \setminus (L_\Delta \cup L^{(1)})$ we have $f(\tilde{x}) \in [\{g(\tilde{y})\}]$. With the notations $f_1 = f(\tilde{x}), f_{m+1} = f(x_1, f_m), m = 1, 2, \ldots,$ functions $f_m(x_1, x_2, \ldots \ldots, x_{m+1}) = x_1 + x_2 + \ldots + x_{m+1} + (p-m)\alpha$ are generated. To generate an arbitrary function $g(\tilde{y}) = a_1 y_1 + \ldots + a_n y_n + \alpha(1-a)$ for $n \geqslant 1$, we must choose $m = a_1 + a_2 + \ldots + a_n - 1 \geqslant 1$, $y_1 = x_1 = x_2 = \ldots = x_{a_1}$, $y_2 = y_{a_1+1} = y_{a_1+2} = \ldots \ldots = y_{a_1+a_2}, \ldots, y_n = y_{a-a_n+1} = \ldots = y_a$ in $f_m(x_1, \ldots, x_{m+1})$: $f(y_1, \ldots, y_1, y_2, \ldots, y_n) = g(\tilde{y})$. The function $g_0(\tilde{x}) = \alpha$ is obtained from the function $f_{p-1}(x_1, \ldots, x_p) = x_1 + \ldots + x_p + \alpha$ by identifying the variables: $g_0(\tilde{x}) = f_{p-1}(x, \ldots, x)$. Let $g(\tilde{y}) = a_0 + a_1 y_1 + \ldots + a_n y_n \in L_\alpha \setminus (L_\Delta \cup L^{(1)})$ (therefore $a_0 = \alpha(1-a), a \neq 1, n \geqslant 2$). The function $g_0(x_1, x_2, x_3) = b_0 + b_0 x_1 + x_2 + x_3$ can be obtained by Lemma 3. Therefore we have the function $f(\tilde{x}) = x_1 + x_2 + (p-\alpha) = g_{m_0}(x_1, x_2)$ from the following construction:

$$g_1(x_1, x_2) = g_0(x_1, x_2, x_1) = b_0 + (b_1+1)x_1 + x_2,$$
$$g_m(x_1, x_2) = g(x_1, g_{m-1}(x_1, x_2)) = mb_0 + m(b_1+1)x_1 + x_2, \quad m \geqslant 2,$$

with $b_0 = (b_1+1)^{p-2}$.

(2)–(3): Cases (2) and (3) can be considered together because of the fact that $L_{\Delta 0}$ is a closed set and $[L_{\Delta 0} \cup \{h(x, \ldots, x)\}] = L_\Delta$ if and only if $h(\tilde{x}) \in L_\Delta \setminus L_{\Delta 0}$. A method similar to that used in part (1) can be used to prove that $f(x, y, z) = x + y + (p-1)z + c_0$ is a base function in L_Δ if $c_0 \neq 0$ (in $L_{\Delta 0}$ if $c_0 = 0$) and, moreover, that

$$f(x, y, z) \in [\{g(\tilde{x})\}] \quad \text{if} \quad g(\tilde{x}) \in L_\Delta \setminus (L_{\Delta 0} \cup L^{(1)})$$

(in case $c_0 = 0$: if $g(\tilde{x}) \in L_{\Delta 0} \setminus L^{(1)}$). ∎

We can see by Theorem 4 that almost all the elements of L_α (L_Δ, $L_{\Delta 0}$) constitute a base. In order to investigate the bases of $L^{(1)}$ and $L^{(1)} \setminus L^{(0)}$ we shall need some properties of the structure defined by multiplication "$\cdot$" mod p over the set V. It is well known that the set V constitutes a cyclic group having $\varphi(p-1)$ one-element bases, $\varphi(x)$ denoting Euler's φ-function.

We shall mean by the *multiplicative order of* $a \in V$ the least integer $r(a) = r \geqslant 1$ for which $a^r = 1$ holds. If $p-1$ is divisible by m, then V has $\varphi(m)$ elements with order m. Let $c_0 \in L^{(0)}$, $a_{i0} + a_i x \in L^{(1)} \setminus L^{(0)}$, $i \geqslant 1$, $r(a_i) = r_i$. Let us denote by l.c.m. $\{r_1, r_2, \ldots\}$ the least common multiple of the numbers $r_1, r_2, \ldots$

THEOREM 5. (A) *The following statements are all equivalent:*

(1) $B = \{a_{10} + a_1 x, a_{20} + a_2 x, \ldots, a_{s0} + a_s x\}$ *is a basis of* $L^{(1)} \setminus L^{(0)}$.

(2) $B_0 = \{c_0\} \cup B$ *is a basis of* $L^{(1)}$.

(3) *The following three statements hold true for the elements of* B:

(a) l.c.m. $\{r_1, \ldots, r_s\} = p-1$,

(b) $B \setminus L^1_\alpha \neq \emptyset$, $\alpha = 0, 1, \ldots, p-1$,

(c) *statements* (a) *and* (b) *do not hold simultaneously for any non-trivial subset of* B.

(B) *The cardinality of the bases of* $L^{(1)}$ *and of* $L^{(1)} \setminus L^{(0)}$ *is* $\geqslant 3$ *and* $\geqslant 2$, *respectively*.

Proof. (A). (1) ⇒ (2): As a consequence of $[B] = L^{(1)} \setminus L^{(0)} \ni x+1$ we have $(L^{(1)} \supseteq)[B_0] \supseteq [B] \cup \{x+1, c_0\} = (L^{(1)} \setminus L^{(0)}) \cup (L^{(0)} \cup L^{(1)}_\Delta) = L^{(1)}$.

(2) ⇒ (3): Let $a \in V$, $r(a) = p-1$, and consider a function $a_0 + ax \in L^{(1)}$. As a consequence of $a_0 + ax \in [B] \subseteq [B_0]$, $r(a)$ will be a divisor of l.c.m. $\{r_1, r_2, \ldots, r_s\}$. As $(b_0 + bx) \square (c_0 + cx) = (b_0 + bc) + (bc)x$, and b, c belong to the multiplicative group mod p over V, we have by a well-known group theory method

$$r(bc) = \text{l.c.m.}\{r(b), r(c)\}.$$

Thus, if $a = \gamma_1 \gamma_2 \ldots \gamma_u$, $\gamma_{j0} + \gamma_j x \in B$, $j = 1, 2, \ldots, u$, then $r(\gamma_j) \in \{r_1, \ldots, r_s\}$, and so $r(a) = \text{l.c.m.}\{r(\gamma_1), \ldots, r(\gamma_u)\}$ is indeed a divisor of l.c.m. $\{r_1, \ldots, r_s\}$. Finally, according to the theorem of Lagrange, $r_1, \ldots, r_s$ are divisors of $p-1$ and thus so is the l.c.m. $\{r_1, \ldots, r_s\}$, which implies (3a).

If statement (b) were not fulfilled, that is if $B \subseteq L^{(1)}_\alpha \setminus \{\alpha\}$ did not hold for any α, it would result in $x+1 \in L^{(1)} \setminus L^{(0)} = [B] \subseteq [L^{(1)}_\alpha \setminus \{\alpha\}] \subseteq L^{(1)}_\alpha$, contradicting Lemma 1. Statement (c) is a consequence of the fact that the set B is a basis.

(3) ⇒ (1): Suppose that (3a) and (3b) are valid. Let $a = a_1 a_2 \ldots a_s$ and let us compose the function $a_0 + ax \in [B]$ from the elements of B. It remains to prove that the function $x+1$ can also be constructed, since some composition of any function $A_0 + Ax \in L^{(1)} \setminus L^{(0)}$ can be obtained in the following way: $(x + p - a_0) \square \square (ax + a_0) = ax$, $A_0 + Ax \in [\{x+1, ax\}]$, u being a number satisfying the equation $a^u = A$. If $a_t = 1$ (and thus, by statement (c), $a_{t0} \neq 0$), for any t with $1 \leqslant t \leqslant s$, then it is easy to see that $x+1 \in [B]$. If $a_t \geqslant 2$ for all t, then, according to Lemma 1, there is exactly one value of α, namely $\alpha = (p-1)a_0(a-1)^{p-2}$ fulfilling $a_0 + ax \in L^{(1)}_\alpha$. Thus choosing j so as to satisfy $a_i a^j = 1$ for the function $a_{i0} + a_i x \in B \setminus L^{(1)}_\alpha$, we shall have $b_0 + x \in [\{a_{i0} + a_i x, a_0 + ay\}]$ with $b_0 + x \notin L^{(1)}_\alpha$, as a consequence of Lemma 2.

In this case, using Lemma 4 again, we get $b_0 \neq 0$ and thus $x+1 \in [\{b_0+x\}]$. So we have proved the completeness of the set B.

The fact that B is a minimal set and thus a basis follows from statement (3c). ■

To conclude this section we shall prove that no other maximal subsets are contained in L than the $p+2$ ones described before.

THEOREM 6. *Every non-trivial subset of L in $\mathscr{L}$ is contained in at least one of the subsets $L_0, L_1, \ldots, L_{p-1}, L_\Delta, L^{(1)}$.*

Proof. If we take for an indirect proposition a subset $(L \neq)P \in \mathscr{L}$ not contained in any of the maximal sets specified in the statement of the theorem, it will consequently contain at least one function of each of the following types:

$$c_{\alpha 0} \neq \alpha \quad \text{or} \quad c_{\alpha 0}+c_\alpha x,\ c_{\alpha 0} \neq \alpha(1-c_\alpha), \quad \alpha = 0, 1, \ldots, p-1,$$

$$c_{p0} \quad \text{or} \quad c_{p0}+c_p x,\ c_p \neq 1,$$

$$\tilde{c} = c_{p+1,0}+c_{p+1,1}x_1+ \ldots +c_{p+1,n}x_n, \qquad n \geqslant 2.$$

Let

$$c_{p+1,0}+c_{p+1,1}x+ \ldots +c_{p+1,n}x = c_{p+1,0}+c_{p+1}x.$$

We shall distinguish three cases; in each of them we shall generate some of the maximal classes, which it will be complete together with an element of P chosen arbitrarily.

Case 1. $c_{p+1} = 1$, $c_{p+1,0} = 0$. According to Lemma 1 we have

$$\tilde{c} \in (L_\Delta \bigcap_{\alpha=0}^{p-1} L_\alpha) \setminus L^{(1)}.$$

If $c_0 = 1$, then by Theorem 4 and Lemma 2 we have $[\{c_{00}+c_0x, \tilde{c}\}] = L_\Delta$ and thus $[\{c_{00}+c_0x, \tilde{c}, c_{p0}+c_px\}] = L$. If $c_0 > 1$, let $a_2 = (p-1)(c_0-1)^{p-2}$, $a_1 = p-a_2+1$ and so $a_1x_1+a_2x_2 \in L_{\Delta 0}$, and we have $[\{\tilde{c}\}] = L_{\Delta 0}$ by Theorem 4. Therefore $[\{a_1x_1+a_2x_2,\ c_{00}+c_0x\}] \ni c_0' = a_2c_{00}$ and $x_1+x_2+(p-1)x_3 \in L_{\Delta 0}$ and thus $x_1+x_2+(p-1)c_0' \in L_{c_1'}$. Using Theorems 3 and 4, we get $[\{x_1+x_2+(p-1)x_3, c_0'\}] \supseteq [L_{c_0'} \cup \{c_{c_0'0}\}] = L$. Finally, if the contained function is c_{00}, then $L_{\Delta 0}$ and $L_{c_0'}$ can be obtained in the same way that as for $c_0 > 1$.

Case 2. $c_{p+1} = 1$, $c_{p+1,0} \neq 0$. By Theorem 4 we have $[\{\tilde{c}\}] = L$, and thus $\tilde{c}$ together with the function of type p constitutes a complete system.

Case 3. $c_{p+1} \neq 1$. There is (by Lemma 1) exactly one α_0 with $\tilde{c} \in L_{\alpha_0} \setminus (L_\Delta \cup L^{(1)})$, and so, by Theorem 4, $[\{\tilde{c}\}] = L_{\alpha_0}$ holds. As L_{α_0} is a maximal set, we have a complete system $\{\tilde{c}, \tilde{d}\}$, $\tilde{d}$ being a function of type α_0.

3. The maximal subclasses of $L_0, L_1, \ldots, L_{p-1}, L_\Delta, L^{(1)}$ and their bases

The intersection of any two classes is a subclass of both of them but not always a maximal one. We have seen that $L_{\alpha\Delta} = L_{\Delta 0}$; from Lemma 1 we can also deduce that $L_{\alpha\beta} = L_{\Delta 0}$ if $\alpha \neq \beta$.

THEOREM 7. (1) *$L_{\Delta 0}$ is maximal in each of the classes $L_0, L_1, \ldots, L_{p-1}$.*

(2) *For all $\alpha \in V_0$, $L_\alpha^{(1)}$ is maximal in the class L_α.*

(3) *There is no other maximal class in L_α for any $\alpha \in V_0$ than $L_\alpha^{(1)}$ and $L_{\Delta 0}$.*

Proof. (1): With $\alpha \in V_0$ fixed, let $c_0+c_1x_1+ \ldots +c_nx_n \in L_\alpha \setminus L_{\Delta 0}$. Let us compose the function $c_0+c'x = c_0+c_1x+ \ldots +c_nx$. Since, by our assumption, $c' \neq 1$, we have $c_0 = (1-c')\alpha$. In the case $c' = 0$ from the function $x_1+x_2+(p-1)x_3 \in L_{\Delta 0}$ we get $(p-\alpha)+x_1+x_2$, which we know by Theorem 4 to be a basis of the class L_α.

In the case of $c_0 = \alpha(1-c')$, $c' > 1$, let $a_2 = (p-1)(c'-1)^{p-2}$, $a_1 = p-a_2+1$ ($\neq 0$ with $c' \neq 0$; hence $a_2 \neq 1$). As

$$(a_1x_1+a_2x_2)\square(c_0+c'x_1) = a_2c_0+(a_1+a_2c')x_1$$
$$= \alpha+(p-a_2+1+a_2c')x_1 = \alpha+\big(1+a_2(c'-1)\big)x_1 = \alpha,$$

the problem has been reduced to the previous case, i.e. to the case of $c_0 = \alpha$.

(2): Let $\tilde{c} \in L_\alpha \setminus L_\alpha^{(1)}$. If $\tilde{c} \in L_{\alpha\Delta} \setminus L_\alpha^{(1)} = L_{\Delta 0} \setminus L_\alpha^{(1)}$, then by Theorem 4 we have $[\{\tilde{c}\}] = L_{\Delta 0}$ and, $L_{\Delta 0}$ being maximal in the class L_α by (1), using $2x+p-\alpha \in L_\alpha^{(1)} \setminus L_{\Delta 0}$, we get $[L_{\Delta 0} \cup \{(p-\alpha)+2x\}] = L_\alpha$. On the other hand, if $\tilde{c} \notin L_{\Delta 0} \setminus L_\alpha^{(1)}$, we have $\tilde{c} \in L_\alpha \setminus (L_\Delta \cup L^{(1)})$ and thus by Theorem 4 $[\{\tilde{c}\}] = L_\alpha$ as well.

(3): Let $P \subseteq L_\alpha$, $P \in \mathscr{L}$ and $P \setminus L_{\Delta 0} \neq \emptyset$, $P \setminus L_\alpha^{(1)} \neq \emptyset$. We are going to prove that $P = L_\alpha$. Indeed, on the one hand, if $P' = (P \setminus L_{\Delta 0}) \cap (P \setminus L_\alpha^{(1)}) \neq \emptyset$, then by Theorem 4 we have $[\{\tilde{c}\}] = L_\alpha$ for any $\tilde{c} \in P'$; on the other hand, if $P' = \emptyset$, we have $[\{\tilde{c}\}] = L_{\Delta 0}$ for the function $c \in P \cap (L_{\Delta 0} \setminus L_\alpha^{(1)})$; thus $[\{\tilde{c}, \tilde{c}'\}] = L_\alpha$ with $\tilde{c}' \in P \cap (L_\alpha^{(1)} \setminus L_{\Delta 0})$. ■

THEOREM 8. (1) *$L_{\Delta 0}$ and $L_1^{(1)}$ are maximal classes in L_Δ.*

(2) *The class L_Δ has no other maximal classes than $L_{\Delta 0}$ and $L_\Delta^{(1)}$.*

Proof. (1): Let $\tilde{c} \in L_\Delta \setminus L_{\Delta 0}$, as $\tilde{c}(x, \ldots, x) = c_0+cx$ with $c = 1$, $c_0 \neq 0$, since, as we have seen $[\{c_0+x\}] = L_\Delta^{(1)}$, it is enough to prove $L_\Delta^{(1)}$ to be maximal, because, having been enlarged by the function $2x+(p-1)y \in L_{\Delta 0}$ the set $\{2x+ +(p-1)y\} \cup L_\Delta^{(1)}$ will be complete in the class L_Δ if $L_\Delta^{(1)}$ is maximal.

Let $\tilde{d} \in L_\Delta \setminus L_\Delta^{(1)}$, $\tilde{d} = d_0+d_1x_1+ \ldots +d_nx_n$; owing to $n \geqslant 2$ and using the fact that $1-d_0+x \in L_\Delta^{(1)}$, we get $((1-d_0)+x)\square\tilde{d} = 1+d_1x_1+ \ldots +d_nx_n$ which by Theorem 4 is a basis of the class L_Δ.

(2): Let $P \subseteq L_\Delta$, $P \in \mathscr{L}$ satisfy $P \setminus L_{\Delta 0} \neq \emptyset$, $P \setminus L_\Delta^{(1)} \neq \emptyset$. We shall prove $P = L_\Delta$ in this case. Let $\tilde{c} \in P \setminus L_{\Delta 0}$, $\tilde{d} \in P \setminus L_\Delta^{(1)}$, i.e. let the functions c_0+cx and $\tilde{d}$ satisfy $c = 1$, $c_0 \neq 0$, $d = 1$, $n \geqslant 2$. As $[\{c_0+cx\}] = L_\Delta^{(1)}$ is a maximal class, we have $[P] \supseteq [L_\Delta^{(1)} \cup \{\tilde{d}\}] = L_\Delta$, i.e. $P = L_\Delta$. ■

We are now going to investigate the maximal classes of $L^{(1)}$ and $L^{(1)} \setminus L^{(0)}$ together, as in determining the bases in Theorem 5. One can easily check that $L^{(1)} \setminus L^{(0)}$ is a (non-commutative) group of order $p(p-1)$ with respect to the superposition. Let the numer $p-1$ have the decomposition to powers of primes $p-1 = q_1^{\varkappa_1}q_2^{\varkappa_2} \ldots q_u^{\varkappa_u}$ with all $q_1 = 2 < q_2 < \ldots < q_u$ primes, $\varkappa_i \geqslant 1$, $p_i = (p-1)/q_i$ and $L^{(1,i)} = \{a_0+ax \mid r(a)\ (\geqslant 1) \text{ divides } p_i\}$, $i = 1, 2, \ldots, u$.

THEOREM 9. (A) *In the class* $L^{(1)} \setminus L^{(0)}$ *the following* $p+u$ *classes in* $\mathscr{L}$ *are maximal*:

(1) $L^{(1,i)}$, $i = 1, 2, \dots, u$,

(2) $L_\alpha^{(1)} \setminus \{\alpha\}$, $\alpha = 0, 1, \dots, p-1$.

(B) *In the class* $L^{(1)}$ *the following* $p+u+1$ *classes in* $\mathscr{L}$ *are maximal*:

(1) $L^{(1,i)} \cup L^{(0)}$, $i = 1, 2, \dots, u$,

(2) $L_\alpha^{(1)} \cup L^{(0)}$, $\alpha = 0, 1, \dots, p-1$,

(3) $L^{(1)} \setminus L^{(0)}$.

(C) I. *There are no more maximal classes of* $L^{(1)} \setminus L^{(0)}$ *but those given in* (A1), (A2).

II. *There are no more maximal classes of* $L^{(1)}$ *but those given in* (B1)–(B3).

Proof. (A1): The closedness of $L^{(1,i)}$ is a consequence of $r(ab) = \text{l.c.m.}\{r(a), r(b)\}$ and thus, $r(ab)$ being a divisor of p_i provided so are $r(a)$ and $r(b)$. So $L^{(1,i)}$ is a non-trivial subset of $L^{(1)} \setminus L^{(0)}$ because $r(a) = p-1$ implies $a_0 + ax \notin L^{(1,i)}$. So, $L^{(1,i)}$ is maximal, because, according to the definition of $L^{(1,i)}$, if $a_0+ax \in (L^{(1)} \setminus L^{(0)}) \setminus L^{(1,i)}$, then $q_i^{\varkappa_i}$ divides $r(a)$ and thus, by the use of a function $b_0+bx \in L^{(1,i)}$ satisfying $r(b) = p_i$ assumption (3a) of Theorem 5 is satisfed for the set $\{a_0+ax, b_0+bx\}$. Assumption (3b) of the same theorem is fulfilled by the subset $\{1+x\} \subset L^{(1,i)}$.

(A2): Let $a_0+ax \in (L^{(1)} \setminus L^{(0)}) \setminus L_\alpha^{(1)}$. Since, by definition $\{a_0+ax\} \setminus L_\alpha^{(1)}$ is non-void, the set $(L_\alpha^{(1)} \setminus \{\alpha\}) \cup \{a_0+ax\} = \{x, (p-\alpha)+2x, \dots, 2\alpha+(p-1)x, a_0+ax\}$ fulfils assumptions (3a) and (3b) of Theorem 5.

(B1): It is a consequence of $(A1)$ as $L^{(1)} \setminus (L^{(1,i)} \cup L^{(0)}) = (L^{(1)} \setminus L^{(0)}) \setminus L^{(1,i)}$. In a similar way we obtain (B2) from (A2) and the identity

$$L^{(1)} \setminus (L_\alpha^{(1)} \cup L^{(0)}) = (L^{(1)} \setminus L^{(0)}) \setminus (L_\alpha^{(1)} \setminus \{\alpha\}).$$

(B3): Let $c_0 \in L^{(0)}$. As $L_A^{(1)} \subset L^{(1)} \setminus L^{(0)}$, $[\{c_0\} \cup L_A^{(1)}] = L^{(0)} \cup L_A^{(1)}$ implies $[\{c_0\} \cup (L^{(1)} \setminus L^{(0)})]$.

(CI): Suppose $P \subseteq L^{(1)} \setminus L^{(0)}$, $P \in \mathscr{L}$ and $P \setminus L^{(1,i)} \neq \emptyset$, $i = 1, 2, \dots, u$, $P \setminus L_\alpha^{(1)} \neq \emptyset$, $\alpha = 0, 1, \dots, p-1$. Let $a_{i0}+a_i x \in P \setminus L^{(1,i)}$, $i = 1, 2, \dots, u$, and $b_{\alpha 0}+b_\alpha x \in P \setminus L_\alpha^{(1)}$, $\alpha = 0, 1, \dots, p-1$, i.e. $b_{\alpha 0} = \alpha(1-b_\alpha)$. So the set $A = \{a_{10}+a_1 x, \dots, a_{u0}+a_u x_u\}$ will fulfil assumption (3a) of Theorem 5 and the set $B = \{b_{00}+b_0 x_0, b_{10}+b_1 x_1, \dots, b_{p-1,0}+b_{p-1} x_{p-1}\}$ will fulfil (3b) of Theorem 5. Thus $[A \cup B] = L^{(1)} \setminus L^{(0)}$, and so $P = L^{(1)} \setminus L^{(0)}$.

(C II): The way we shall prove this statement is similar to that of (CI). We shall only use the class P' with $P' \subseteq L^{(1)}$, $P' \in \mathscr{L}$ satisfying $P' \setminus L^{(0)} = P$. As a consequence of the identities

$$P' \setminus (L_\alpha^{(1)} \cup L^{(0)}) = (P' \setminus L^{(0)}) \setminus L_\alpha^{(1)},$$
$$P' \setminus (L^{(1,i)} \cup L^{(0)}) = (P' \setminus L^{(0)}) \setminus L^{(1,i)},$$

P' contains the class $L^{(1)} \setminus L^{(0)}$; hence by the assumption $P' \setminus (L^{(1)} \setminus L^{(0)}) \neq \emptyset$ by (B3) we have $P' = L^{(1)}$. ■

Next we shall determine the bases of the maximal classes described in Theorems 7, 8 and 9.

THEOREM 10. (1) *The bases of the class* $L_A^{(1)}$ *are elements of* $L_A^{(1)} \setminus \{x\}$.

(2) *The set of one-element bases of the class* $L_\alpha^{(1)} \setminus \{\alpha\}$ *is* $\{a_0+ax \mid a_0 = \alpha(1-a), r(a) = p-1\} = A$.

(3) *The minimal cardinality bases of the class* $L_\alpha^{(1)}$ *have two elements*; $\{a(x), \alpha\}$ *is a basis iff* $a(x) \in A$.

(4) *The minimal cardinality bases of the class* $L_\alpha^{(1)} \cup L^{(0)}$ *have three elements*; $\{a(x), \alpha, \beta\}$ *is a basis iff* $a(x) \in A$ *and* $\beta \in L^{(0)} \setminus \{\alpha\}$.

Proof. Statement (1) is equivalent to Lemma 4.

(2)–(3): As the set $L_\alpha^{(1)} \setminus \{\alpha\} = \{a_0+ax \mid a_0 = \alpha(1-a), a \in V\}$ has exactly $p-1$ elements and $|\{b_0+bx\}| = r(b)$, $\{a_0+ax\}$ is a basis of the class $L_\alpha^{(1)} \setminus \{\alpha\}$ if $r(a) = p-1$. This involves (3), also, for in order to generate α we also need an element of $L^{(0)}$, and in $L_\alpha^{(1)}$ α is the only such function.

(4): According to Lemma 2, $\alpha \notin [L_\alpha^{(1)} \cup L^{(0)} \setminus \{\alpha\}]$ and so α must belong to the basis considered. As both $L_\alpha^{(1)} \setminus \{\alpha\}$ and $L^{(0)} \setminus \{\alpha\}$ are closed with respect to the superposition, we shall need elements of both. However, one of each will suffice, for by (2) any of the elements of A generates the class $L_\alpha^{(1)} \setminus \{\alpha\}$, and $[L_\alpha^{(1)} \cup \{\beta\}] = L_\alpha^{(1)} \cup \{\beta, 2\beta+(p-1)\alpha, 3\beta+(p-2)\alpha, \dots, (p-1)\beta+2\alpha\} = L_\alpha^{(1)} \cup L^{(0)}$ also holds, since from the equality $a_1\beta+(1-a_1)\alpha = a_2\beta+(1-a_2)\alpha$ we have $(a_1-a_2)(\beta-\alpha) = 0$, which in the case of $a_1 \neq a_2$ can hold only if $\alpha = \beta$. ■

Remark. The one-to-one correspondence between the mod$p$ multiplicative group C_p and the group $L_\alpha^{(1)} \setminus \{\alpha\}$ is:

$$C_p \ni c \leftrightarrow cx+\alpha(1-c) \in L_\alpha^{(1)} \setminus (\alpha\}.$$

The next theorem with its proof is similar to Theorem 5; therefore we present it without proof. In this theorem $L^{(1,i)} \cup L^{(0)}$, $L^{(1,i)}$ and p_i are written instead of $L^{(1)}$, $L^{(1)} \setminus L^{(0)}$ and $(p-1)$ in Theorem 5, respectively.

THEOREM 11. (A) *The following statements are equivalent*:

(1) *The set* $B = \{a_{10}+a_{11}x_1, a_{20}+a_{21}x_2, \dots, a_{s0}+a_{s1}x_s\}$ *is a base in* $L^{(1,i)}$.

(2) *The set* $B_0 = B \cup \{c_0\}$ *is a base in* $L^{(1,i)} \cup L^{(0)}$.

(3) *For elements of the set* B *we have*:

(a) l.c.m. $\{r_1, \dots, r_s\} = p_i$,

(b) $B \setminus L_\alpha^{(1)} \neq \emptyset$, $\alpha = 0, 1, \dots, p-1$,

(c) *Statements* (a) *and* (b) *do not hold both for any proper subset of* B.

(B) *If* B *is a base of* $L^{(1,i)}$, *then* $|B| \geqslant 2$ *and* $|B_0| \geqslant 3$. ■

4. The description of the rest of the classes of the lattice

After describing further lattice elements we shall present a maximal and a minimal chain, and also the cardinality of $\mathscr{L}$. The lattice structure is demonstrated by Fig. 2. The enclosed table contains bases and their orders n of the different types of classes. An immediate consequence of Theorems 4 and 10 is

THEOREM 12. (1) *The classes $L_{\Delta 0}$ and $L_\Delta^{(1)}$ both have only a unique maximal class, which is the trivial class $\{x\}$.*

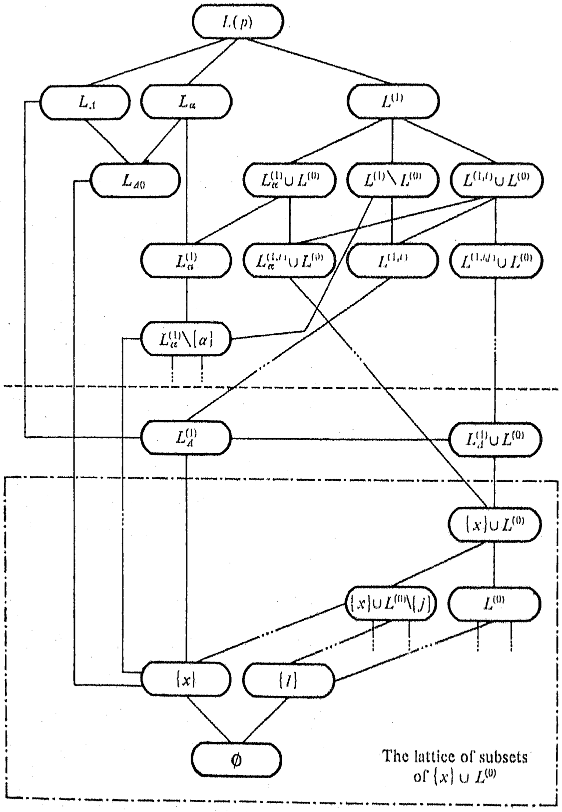

Fig. 2

(2) *The set $L_\alpha^{(1)} \setminus \{\alpha\}$ with operation superposition is a cyclic group of order $p-1$ having α as a fixed point.*

(3) *The class $L_\alpha^{(1)} \setminus \{\alpha\}$ is maximal in $L_\alpha^{(1)}$.*

(4) *The class $L_\alpha^{(1)}$ is maximal in $L_\alpha^{(1)} \cup L^{(0)}$.* ■

It can be shown by arguments similar to those used earlier, with the notation $L_\alpha^{(1,i)} = L^{(1,i)} \cap L_\alpha^{(1)}$, that the class $\{\alpha\} \cup L_\alpha^{(1,i)}$ is maximal in $L_\alpha^{(1)}$, etc. It should be noticed that the every closed class $L' \subseteq L^{(1)}$ has the form $G \cup F$, where G is a closed subset of $L^{(1)} \setminus L^{(0)}$ and $F \subseteq L^{(0)}$ is also a closed set. The restrictions of F are determined by the structure of G. By the theorem of Lagrange we know that the order of the subgroup G of the group $L^{(1)} \setminus L^{(0)}$ is a divisor of $p(p-1)$. We shall see that if q' divides $p(p-1)$, then there is a unique closed class G' in $L^{(1)} \setminus L^{(0)}$ with order $q' = |G'|$. These closed classes are sorted out onto two classes by

LEMMA 5. *The subgroup $L_\Delta^{(1)}$ is contained in the subgroup G of the group $L^{(1)} \setminus L^{(0)}$ iff the order of G is $|G| \geqslant p$.*

Proof. The necessity of condition is obvious: $|L_\Delta^{(1)}| = p$. Let us suppose $|G| \geqslant p$. If $c_0 + x \in G$ for $c_0 \neq 0$, then $L_\Delta^{(1)} \subseteq G$ by Lemma 4. If $G \setminus \{x\} \subseteq \{a_0 + ax \mid a > 1\}$, then, the elements of $G \setminus \{x\}$ being written in the form $b_0 + bx$, for $b_0 = \beta(1-b)$ there are two elements, $b_{10} + b_1 x_1, b_{20} + b_2 x_2 \in G \setminus \{x\}$, such that $b_{10} = \beta_1(1-b_1)$, $b_{20} = \beta_2(1-b_2)$, $\beta_1 \neq \beta_2$ because of $|L_\alpha^{(1)} \setminus \{x\}| = p-2 < |G \setminus \{x\}|$. Furthermore $(a_0 + ax, b_0 + ax \in L_\alpha^{(1)} \setminus \{\alpha\}) \Rightarrow a_0 = b_0$; hence there are $\alpha_1 \neq \alpha_2$ such that $a_{10} + ax$, $a_{20} + ax \in G$, $a_{10} = \alpha_1(1-a)$, $a_{20} = \alpha_2(1-a)$. But from the sequence $(a_{20} + ax) \square (a_{20} + ax) = A_{02} + a^2 x, \ldots, (a_{20} + ax) \square (A_{0h-1} + a^{h-1} x) = A_{0h} + a^h x$, we obtain $(a_{10} + ax) \square (A_{0p-2} + a^{p-2} x) = A_0' + x$ and $[\{A_0' + x\}] = L_\Delta^{(1)}$ because $A_0' = a_{10} + aA_{0p-2} = a_{10} - a_{20} = (\alpha_1 - \alpha_2)(1-a) \neq 0$. ■

LEMMA 6. *The subgroup $G \subseteq L^{(1)} \setminus L^{(0)}$ of order $|G| \leqslant p-1$ is cyclic, and G is a subgroup of $L_\alpha^{(1)} \setminus \{\alpha\}$ for suitable α.*

Proof. Clearly, $L^{(1)} \setminus L^{(0)} = L_\Delta^{(1)} \bigcup_{\alpha=0}^{p-1} (L_\alpha^{(1)} \setminus \{\alpha\})$, is a union of cyclic groups. By Lemma 5 $G \cap L_\Delta^{(1)} = \{x\}$. Let us suppose that there are $\alpha_1 \neq \alpha_2$, such that $a_{10} + a_{11} x \in G \cap L_{\alpha_1}^{(1)}$, $a_{20} + a_{21} x \in G \cap L_{\alpha_2}^{(1)}$, $a_{10} = \alpha_1(1-a_{11}) \neq 0 \neq \alpha_2(1-a_{21}) = a_{20}$ $(a_{11} > 1, a_{21} > 1)$. Let $a = a_{11} a_{21}$; then

$$r_1 = r(a_{11}), \quad r_2 = r(a_{21}), \quad r = r(a) = \text{l.c.m.}\{r_1, r_2\}, \quad r_1 \leqslant r_2.$$

Forming the sequences $(a_0 + ax) \square (a_0 + ax) = a_{02} + a^2 x, \ldots, (a_0 + ax) \square (a_{0u-1} + a^{u-1} x) = a_{0u} + a^u x$ and $(a_{20} + a_{21} x) \square (a_{20} + a_{21} x) = A_{02} + a_{21}^2 x, \ldots, (a_{20} + a_{21} x) \square (A_{0v-1} + a_{21}^{v-1} x) = A_{0v} + a_{21}^u x$, we can obtain from them $(a_{0r_1} + a^{r_1} x) \square (A_{0r_2 - r_1} + a_{21}^{r_2 - r_1} x) = A_0' + x$, $A_0' \neq 0$ because $a^{r_1} = a_{11}^{r_1} a_{21}^{r_1} = a_{21}^{r_1}$, $A_0' \neq 0$ by Lemma 2, and this contradicts Lemma 5. Therefore, we cannot have $\alpha_1 \neq \alpha_2$ as we supposed. ■

The structure of a cyclic group may be obtained from the main theorem on Abelian groups. Accordingly, the lattice of subgroups of $L_\alpha^{(1)} \setminus \{\alpha\}$ is isomorphic to the lattice of divisors of $p-1$. (Lattice operations: $\bigvee$ = l.c.m.; $\bigwedge$ = g.c.d.)

Notice that this statement also holds for the non-Abelian group $L^{(1)}\setminus L^{(0)}$, as a consequence of Lemmas 5 and 6 and the fatc that every subgroup G in $L^{(1)}\setminus L^{(0)}$ of order $|G| = pq$, can be given in the form $G = [G' \cup L_{\Delta}^{(1)}]$ ($|G'| = q$ divides $p-1$).

Now we can state a theorem about the structure of $L^{(1)}$ and $L^{(1)}\setminus L^{(0)}$.

First, let us associate the sequence $\mu_0\mu_1 \dots \mu_{p-1}\lambda_1 \dots \lambda_u$ with the subgroup G_α of order $p^{\lambda_0}q_1^{\lambda_1} \dots q_u^{\lambda_u}$ in the following way:

$$\mu_i = \begin{cases} 1 & \text{if} \quad \lambda_0 = 1, \\ 0 & \text{if} \quad \lambda_0 = \lambda_1 = \dots = \lambda_u = 0, \\ 1-(i-\alpha)^{p-1} \bmod p & \text{in other cases.} \end{cases}$$

Moreover, let $\mu_p = 1$ if $G \neq \emptyset$ and $\mu_p = 0$ if $G = \emptyset$. Let us associate the sequence $\mu_0\mu_1 \dots \mu_p\lambda_1 \dots \lambda_u\nu_0\nu_1 \dots \nu_{p-1} = \mu\lambda\nu$ with the class $G \cup F \subseteq L^{(1)}$ with its first $p+u+1$ elements constituting the subsequence corresponding to G and the next p elements being the characteristic sequence of F: $\nu_0\nu_1 \dots \nu_{p-1}$ with

$$\nu_i = \begin{cases} 1 & \text{if} \quad i \in F, \\ 0 & \text{if} \quad i \in V_0 \setminus F. \end{cases}$$

These sequences have been constructed in such a way that their usual partial ordering preserves the ordering of the corresponding sets. (The partial ordering of sequences is: $\gamma_1\gamma_2 \dots \gamma_k \leqslant \delta_1\delta_2 \dots \delta_k$ if $\gamma_j < \delta_j$, $j = 1, 2, \dots, k$). Let us denote by $s(\gamma)$ the sum of the elements of the binary sequence γ, and let

$$N_\mu = \begin{cases} \{0, p\} & \text{if} \quad s(\mu) = p, \\ \{lg, lg+1|\ g = q_1^{\lambda_1} \dots q_u^{\lambda_u}, l = 0, 1, \dots, (p-1)/g\} & \text{if} \quad s(\mu) = 1, \\ \{0, 1, \dots, p\} & \text{if} \quad s(\mu) = 0. \end{cases}$$

(The operations $\cdot$ and $+$ are the usual ones, not mod p.)

THEOREM 13. (A) *The subgroup lattice of the group $L^{(1)}\setminus L^{(0)}$ is isomporhic to the lattice of the partially ordered set*

$$R = \{\mu\lambda|\ \mu_i \in \{0, 1\}, 0 \leqslant \lambda_j \leqslant \varkappa_j, i \in V_0, j = 1, 2, \dots, \mu, \quad s(\mu) \in \{0, 1, p\}\}.$$

(B) *The subsemigroup lattice of the semigroup $L^{(1)}$ is isomorphic to the lattice of the partially ordered set*

$$Q = \{\mu\lambda\nu|\ \mu\lambda \in R, s(\nu) \in N\mu, \text{ and } \nu_i \geqslant \mu_i \text{ if } s(\mu) = 1\}.$$

Proof. Let G_α be an α-preserving subgroup of order $g = |G_\alpha|$ ($\leqslant p-1$) with $h = (p-1)/g$. Let us consider the sequence

$$F_0 = G_\alpha \cup \{\alpha\}, \quad F_1 = [F_0 \cup \{\beta_1\}], \dots, F_i = [F_{i-1} \cup \{\beta_i\}], \dots$$
$$\dots, F_h = [F_{h-1} \cup \{\beta_h\}] = G_\alpha \cup L^{(0)}$$

with

$$\beta_i \in L^{(0)} \setminus F_{i-1}, \quad i = 1, 2, \dots, h.$$

Clearly, F_{i-1} is maximal in F_i for $i = 1, \dots, h$, the chains $G_\alpha \subset F_0 \subset F_1 \subset \dots \subset F_h$ being of $(p-1)/g+2$ elements according to the fact that the same partition of $(p-1)/g+1$ elements on the set V_0 is induced by the disjoint cyclic decomposition of any base element of G_α. In this partition $\{\alpha\}$ has cardinality 1 and the rest of the $h+1$ subsets have cardinality g.

Similarly, if $|G| \geqslant p$, only the two-element chain $G \subset G \cup L^{(0)}$ will belong to G. On the contrary, any chain of the lattice of subsets of V_0 can be related to the trivial group $\{x\}$ and to the empty set $\emptyset$; thus chains of type

$$\{x\} \subset \{x\} \cup \{0\} \subset \{x\} \cup \{0, 1\} \subset \dots \subset \{x\} \cup L^{(0)}$$

have length $p+1$, in accordance with $\{x\}$ being α-preserving and $h = p-1$.

Let a binary sequence corresponded to each closed class $F = G \cup K \subseteq L^{(1)}$, its first $p+i+1$ elements being sequence $\mu_0\mu_1 \dots \mu_{p-1}\mu_p\lambda_1 \dots \lambda_u$ related to G and the next p elements being the characteristic sequence of $K \subseteq L^{(0)}$: $\nu_i = 1$ if $i \in K$ and $\nu_i = 0$ if $i \notin K$ for $i = 0, 1, \dots, p-1$.

Thus for each subgroup $G \subseteq L^{(1)}\setminus L^{(0)}$ the corresponding sets K are unions of the partition elements induced by its cyclic subgroup maximal of order. So each closed set F and no other one is produced.

$\{x\}$ can take the form of any binary sequence $\nu_0\nu_1 \dots \nu_{p-1}$ and $\nu_\alpha = 1$ in each F_i for the α-preserving group of order g, G_α. Moreover, in the set F_i, $(1+ig)$ elements are equal to 1 while the rest of the elements equal to 0. (Even in the case of $\emptyset$ no more sequence than $00 \dots 0$ is excluded.)

Finally, the sequence $\nu_i = 1$ for $i = 0, 1, \dots, p-1$ belongs to $G \cup L^{(0)}$ if $|G| \geqslant p$ and, in general, $\nu_i = 0$ for $i = 0, 1, \dots, p-1$ belongs to $G \subseteq L^{(1)}\setminus L^{(0)}$.

This construction provides us with a one-to-one correspondence between the sequences in Q and the closed classes in $L^{(1)}$. So it only remains to prove the order-preserving property of this correspondence.

Let $G_2 \cup K_2$ be maximal in the closed class $G_1 \cup K_1$. If $|G_1| \geqslant p$, then $K_1 = L^{(0)}$ and G_2 is maximal in G_1 by Lemma 5. So $\mu_i^{(1)} = 1 = \nu_i^{(1)}$ for all i and $\lambda^{(2)} \leqslant \lambda^{(1)}$ by Lagrange's theorem.

If $|G_1| \leqslant p-1$, then $G_1 = G_2$ implies $K_2 \subset K_1$ and thus $\mu^{(1)}\lambda^{(1)} = \mu^{(2)}\lambda^{(2)}$ and $\nu^{(2)} < \nu^{(1)}$. In the case $G_2 \subset G_1$ we have $\mu^{(2)} \leqslant \mu^{(1)}s(\mu^{(1)}) = 1$ and $\lambda^{(2)} < \lambda^{(1)}$, and $K_2 \subseteq K_1$ implies $\nu^{(2)} \leqslant \nu^{(1)}$. So $\mu^{(2)}\lambda^{(2)}\nu^{(2)} < \mu^{(1)}\lambda^{(1)}\nu^{(1)}$ is true in all cases. ∎

5. Countability, an example and some closing conclusions

From Theorem 13 we can infer the number of closed classes in $L^{(1)}\setminus L^{(0)}$ and in $L^{(1)}$. Let $d(a)$ be the number of positive divisors of a.

THEOREM 14. (A) *The number of subgroups of the group $L^{(1)}\setminus L^{(0)}$ is*

$$|R| = (p+1)d(p-1)+1-p.$$

(B) *The number of subsemigroups of the semigroup $L^{(1)}$ is*

$$|Q| = 2d(p-1)-1-(p-2)2^p+2p\sum_{gh=p-1} 2^g.$$

Proof. (A): One sequence, $\mu\lambda = 00 \dots 0$, belongs to the weight $s(\mu) = 0$. One μ-sequence and $d(p-1)$ λ-sequences belong to the weight $s(\mu) = p$. Finally,

p μ-sequences and $d(p-1)-1$ λ-sequences corresponding to any μ-sequence belong to the weight $s(\mu)=1$.

These facts together yield

$$|R| = 1+1d(p-1)+p\big(d(p-1)-1\big) = (p+1)d(p-1)-p+1.$$

(B): Let us first suppose that $G \neq \emptyset$. The closed classes described in (A) will correspond to the weight $s(\nu)=0$. $d(p-1)$ λ-sequences will correspond to the $s(\mu)=p=s(\nu)$ pair of weights and 2^p-1 sequences will correspond to the configuration $s(\mu)=0\neq s(\nu)$.

New let $s(\mu)=1$, $s(\nu)\neq 0$. The number of sequences associated with weights $s(\mu)=1$ is p, and, with a fixed g, a sequence with weight $1+lg=s(\nu)$ can be chosen in $\sum\limits_{l=0}^{h}\binom{h}{l}$ ways. Likewise we proceed on $\sum\limits_{l=1}^{h}\binom{h}{l}$ ν-sequences having the weight $s(\nu)=lg$ for $l=1,2,\dots,h$. Finally 2^p-1 sequences are related to the case $G=\emptyset$. These all together yield

$$\begin{aligned}
|Q| &= |R|+d(p-1)+2(2^p-1)+p\sum_{\substack{gh=p-1\\ g\neq 1}}\Big(2\sum_{l=0}^{h}\binom{h}{l}-1\Big)\\
&= (p+2)d(p-1)-p-1+2^{\,+1}+p\Big(\sum_{gh=p-1}(2^{h+1}-1)-(2^p-1)\Big)\\
&= (p+2)d(p-1)-(p-2)2^p-1-p\sum_{gh=p-1}1+2p\sum_{gh=p-1}2^h\\
&= 2d(p-1)-(p-2)2^p-1+2p\sum_{gh=p-1}2^h. \qquad\blacksquare
\end{aligned}$$

An immediate consequence of Theorems 6, 7, 8, and 14 is the number of all the closed classes in L. The result concerning the lengths of chains is Theorem 15. By *directed paths* we shall mean the chains of the directed graph corresponding to the lattice of the linear class L. The maximal length of a chain in this graph is clearly its height over the radical vertex L. Let the canonical decomposition of $p-1$ be $p-1=q_1^{\varkappa_1}\dots q_u^{\varkappa_u}$ (as before).

THEOREM 15. (1) *The number of closed classes in the linear class is*

$$p+2-(p-2)2^p+2d(p-1)+2p\sum_{gh=p-1}2^h \sim 2^{p+1}+p2^{(p+1)/2}.$$

(2) *The lengths of the minimal and maximal chains in the linear class L are* 3 *and* $p+2+\sum\limits_{i=1}^{u}\varkappa_i$, *respectively.*

Proof. The first statement needs no proof. It is easily seen that $(L)\to(L_\Delta)\to\to(L_{\Delta 0})\to(\{x\})$ is a minimal chain and that all the maximal ones contain the vertex $(L^{(1)})$. As we descend from $L^{(1)}$, either the sum of exponents $1+\Sigma\varkappa_i$ belonging to the canonical decomposition of $p(p-1)$ or the number of constants belonging

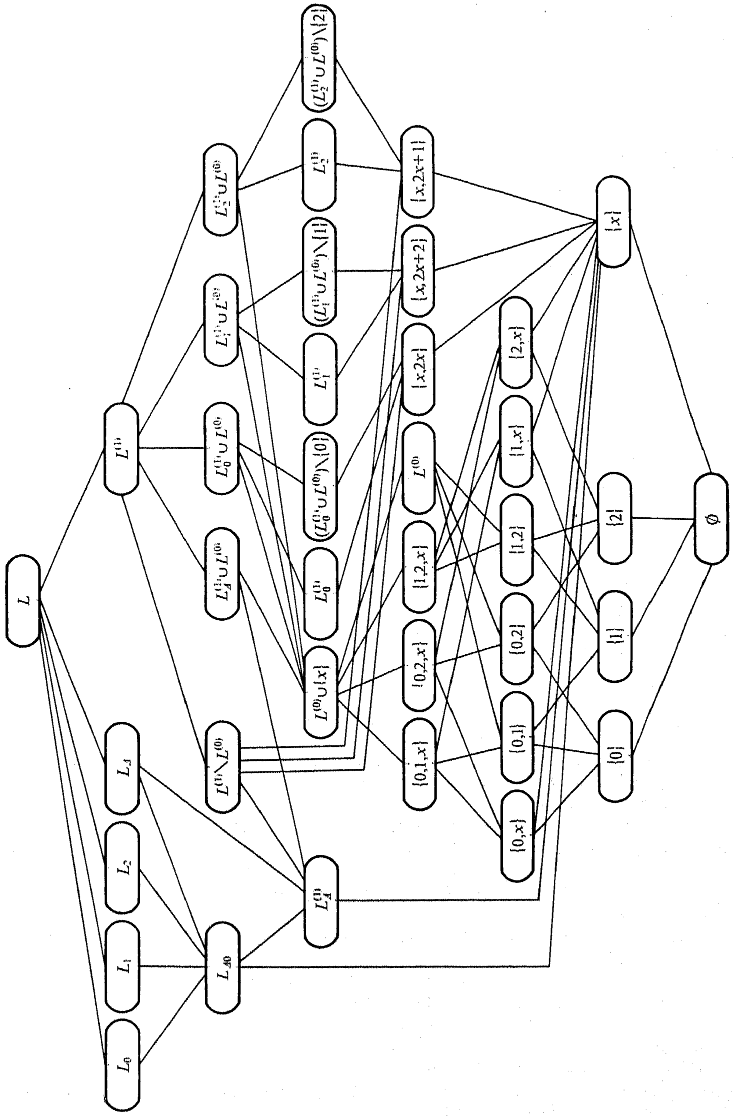

Fig. 3

to the closed classes will decrease. This fact gives the following upper bound for the chain lengths:

$$1+|L^{(0)}|+\left(1+\sum_{i=1}^{u}\varkappa_i\right) = p+2+\sum_{i=1}^{u}\varkappa_i.$$

This bound can be reached by taking the path

$$(L) \to (L^{(1)} \to \ldots \to (G\cup L^{(0)}) \to \ldots \to (L_\Delta^{(1)}\cup L^{(0)}) \to (\{x\}\cup L^{(0)}) \to$$
$$\to (\{x\}\cup(L^{(0)}\setminus\{0\})) \to \ldots \to (\{x\}).$$

The structure of the lattice-diagram can be seen in Fig. 2 and the complete diagram for $p = 3$ in Fig. 3.

Table

Class	Base	Rank
L	$\{x+1, x+y\}$	2
L_α	$\{x+y+(p-\alpha)\}$	2
L_Δ	$\{2x+(p-1)y+1\}$	2
$L_{\Delta 0}$	$\{2x+(p-1)y\}$	2
$L^{(1)}$	$\{0, x+1, ax\}$, $r(a) = p-1$	1
$L^{(1)}\setminus L^{(0)}$	$\{ax, x+1\}$, $r(a) = p-1$	1
$L_\alpha^{(1)}$	$\{\alpha, ax+(\alpha(1-a))\}$, $r(a) = p-1$	1
$L_\Delta^{(1)}$	$\{x+1\}$	1

References

[1] J. Bagyinszki, J. Demetrovics, *The structure of linear classes in prime valued logics*, (Hungarian) MTA SZTAKI Közlemények, 16 (1976), 25–52.

[2] —, —, *The structure of the class of symmetric languages invariant for inner linear transformations*, in: Proc. of Second Hung. Comp. Sci. Conf. 1977, 100–130.

[3] J. Bagyinszki, *The lattice of* SIL-*languages for square-free values of k*, (in preparation).

[4] G. Birkhoff, T. C. Bartee, *Applied modern algebra*, McGraw Hill, 1970.

[5] S. V. Jablonskiĭ, *Functional constructions in k-valued logics*, (Russian) Trudy Mat. Inst. Steklov 51 (1958), 5–142.

[6] S. V. Jablonskiĭ, G. P. Gavrilov, B. V. Kudravchev, *Functions of the algebra of logics and classes of Post*, (in Russian) 1966.

[7] J. I. Janov, A. A. Mučnik, *Existence of k-valued closed classes without a finite basis*, (Russian) Dokl. Akad. Nauk SSSR 127 (1959), 44–46.

[8] E. Post, *The two-valued iterative systems of mathematical logic*, Annals Math. Studies 5 (1941).

[9] L. Rédei, *Algebra*, Vol. I, Pergamon Press, Oxford 1967.

[10] I. Rosenberg, *La structure des fonctions de plusieurs variables sur un ensemble fini*, C. R. Acad. Sci. Paris Sér. A-B 260 (1965), 3817–3819.

[11] A. Salomaa, *On infinitely generated sets of operations in finite algebras*, Ann. Univ. Turku. Ser. AI 74 (1964), 1–13.

[12] —, *On the height of closed sets of operations in finite algebras*, Ann. Acad. Sci. Fenn. Ser. AI 363 (1965), 1–12.

Presented to the Semester
Discrete Mathematics
(February 15–June 16, 1977)