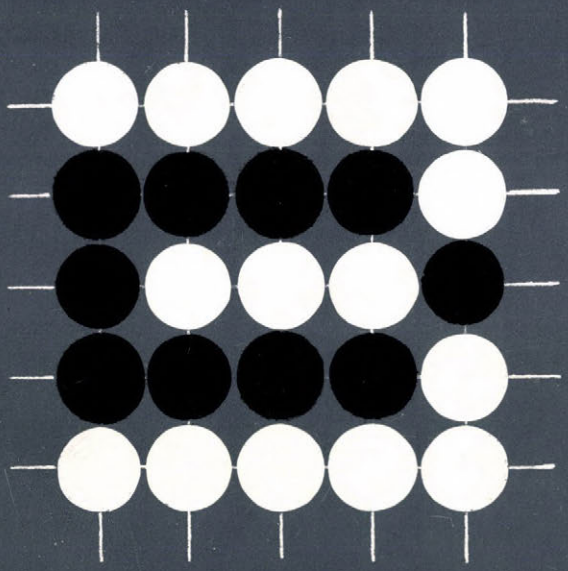
közlemények

MTA Számítástechnikai és Automatizálási Kutató Intézet Budapest



MAGYAR TUDOMÁNYOS AKADÉMIA
SZÁMITÁSTECHNIKAI ÉS AUTOMATIZÁLÁSI KUTATÓ INTÉZETE

KÖZLEMÉNYEK

1982 MÁRCIUS

Felelős kiadó:

DR VÁMOS TIBOR
igazgató

ISBN 963 311 139 0
ISSN 0133-7459

CONTENT

ЛИТЕРАТУРА

MTA Számítástechnikai és Automatizálási Kutató Intézete, **Közlemények 25/1982**

ХРОМАТИЧЕСКИЕ НАБОРЫ И КЛАССЫ МОНОТОННЫХ ФУНКЦИЙ

Густав Бурош, Дитлинде Лау, Эберхард Шмидт

1. ВВЕДЕНИЕ

В данной работе обобщается одна теорема, установленная К. Бензакеном [1]

Бензакен рассматривает биекцию ϕ между множеством всех конечных Шпернеровых гиперграфов H и множеством M_1 всех непостоянных монотонных булевых фнкций f. Его рассмотрения были связаны с интервалом

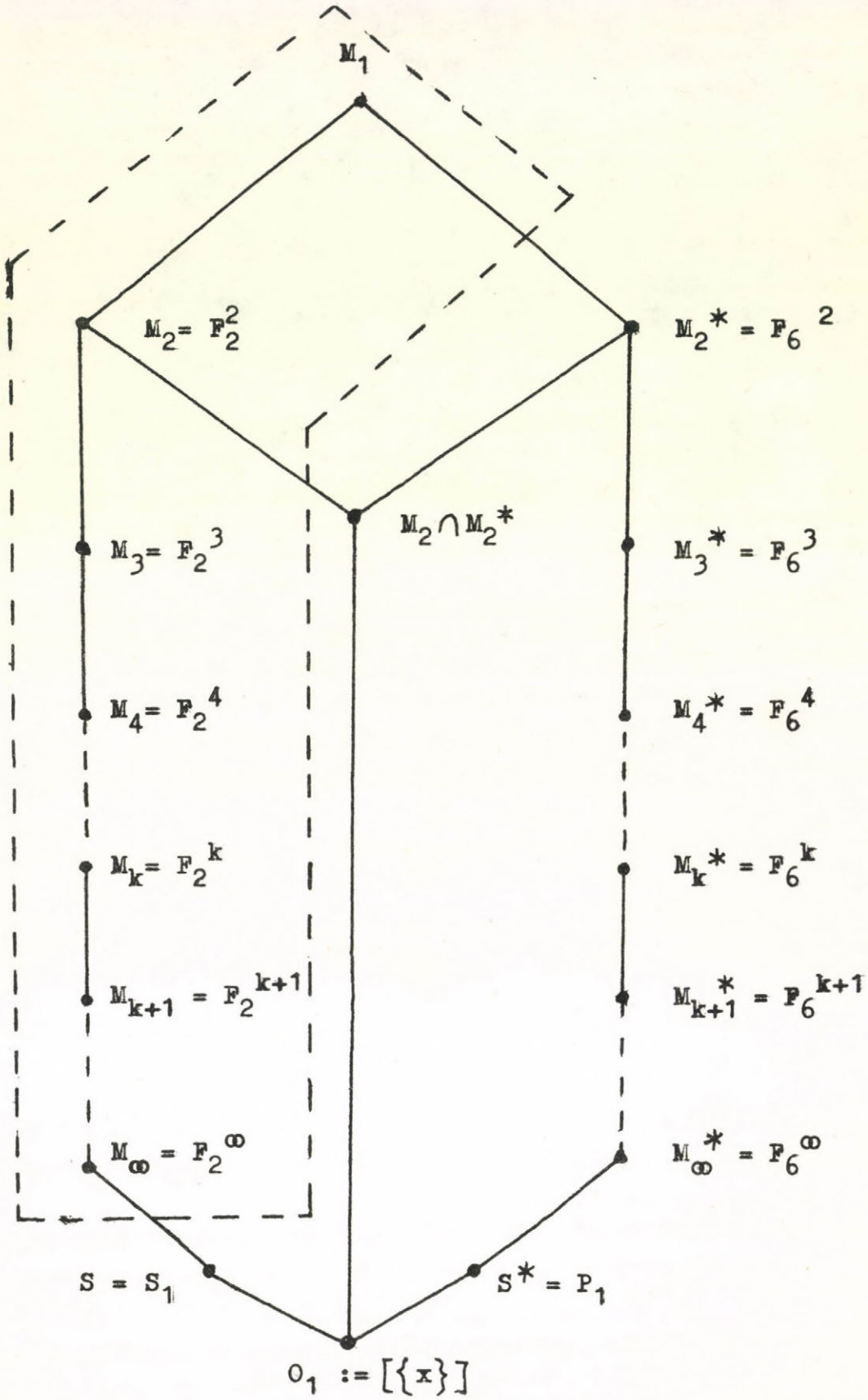
$$[M_\infty, M_1] = \{M_1, M_2, M_3, \ldots, M_\infty\} \qquad \text{где}$$

$$M_1 \supset M_2 \supset M_3 \supset \ldots \quad M_\infty := \bigcap_{i \geq 1} M_i,$$

структуры Поста всех замкнутых множеств булевых функций /см. изобр. 1./.

Теорема /К. Бензакен/ /[1]/. Шпернеров гиперграф обладает слабым хроматическим числом $\chi(H) = k+1$, $1 \leq k < \infty$, тогда и только тогда, когда $f := \phi(H) \in M_k \setminus M_{k+1}$, $1 \leq k < \infty$.

Мы исходим из q-мерного произведения $[M_\infty, M_1]^q$, получая его также в качестве интервала замкнутых множеств некоторой интерактивной алгебры Поста P_{Σ_q}. По теореме Бензакена информация о слабом хроматическом числе гиперграфа равносильна информации о положении функции $f \in M_1$ в интервале $[M_\infty, M_1]$. Сопоставим каждому Шпернеровому гиперграфу H хроматический набор $(k_1, \ldots, k_q)$ и функцию $\phi(H) \in P_{\Sigma_q}$ и покажем, что информация о хроматическом наборе гиперграфа H равносильна информации о положении функции $\rho(H)$ в интервале $[M_\infty, M_1]^q$.



отобр. 1 : интервал $[O_1, M_1]$

Как специальный случай получаем формулировку теоремы Бензакена.

Укажем иную интерпретацию:

Существует q естественных гомоморфизмов P_{Σ_q} на P_2 /P_2 - это алгебра булевых функций/, и интервал $[M_\infty, M_1]$ в P_{Σ_q} определяется с помощью именно таких гомоморфизмов. Поэтому наш результат можно интерпретировать и как вклад, хотя и довольно специальный, в решение вопроса о том, какие свойства одной итеративной алгебры Поста B /здесь такое свойство- теорема Бензакена/ можно переносить на другую итеративную алгебру Поста A при знании естественных гомоморфизмов A на B. Вопросы такого рода рассматривались также в [5]-[9].

В изображении 1 задан интервал $[0_1, M_1]$ из структуры Поста замкнутых множеств из P_2 ([1], [2]) и замаркирован интервал $[M_\infty, M_1]$. Используются обозначения из [1], [2]. В [2] находятся для каждого из этих классов системы образующих. В [1] Бензакен исходит из того, что $f \in P_2$ лежит в M_k, $1 \leq k < \infty$, точно тогда, когда любые k дизъюнкции сокращенной коньюнктивной нормальной формы функции f имеют по меньшей мере одну общую переменную. Классы M_k^*, $1 \leq k < \infty$, определяются двойственным образом, т.е. изоморфно к M_k. Дальше, положим $M_\infty := \bigcap_{i \geq 1} M_i$, $M_\infty^* := \bigcap_{i \geq 1} M_i^*$, $S_1 := [\{x_1 \vee x_2\}]$, $P_1 = [\{x_1 \wedge x_2\}]$.

2. ГИПЕРГРАФЫ И ИХ РАСКРАСКИ

Известно следующее определение гиперграфа: /Конечный/ гиперграф $H=(X; E_1, \ldots, E_t)$ состоит из конечного непустого множества X, называемого множеством вершин, и из множеств E_i ($\emptyset \subset E_i \subseteq X, i = 1, 2, \ldots, t$), называемых ребрами. Мы здесь используем другое определение, трактуемое и как обобщение, и как специальный случай известного понятия гиперграфа.

Определение. Пусть V, W, Z - попарно непересекающиеся мно-

жества, $R \subseteq W \times Z$

$X := V \cup R$

$\emptyset \subset E_i \subseteq X, \quad i=1, 2, \ldots, t.$

$H=(X, E_1, \ldots, E_t)$ называется обобщенным геперграфом, когда имеет место

$$\forall i, w, z, z' : \{(w,z),(w,z')\} \subseteq E_i \quad \Rightarrow \quad z = z' \qquad (1)$$

и $$E_i \cap V \neq \emptyset, \quad i = 1, \ldots, t. \qquad (2)$$

Множества E_i как обычно называем ребрами. Множество Z интерпретируем как множество красок: если $(w,z) \in R$, то говорим, что w раскрашен краской z. Заметим еще, что один и тот же элемент $w \in W$ в различных ребрах может быть раскрашен различными красками.

Пример 1: Пусть $V = \{1, 2, 3\}$, $W = \{1', 2'\}$,

$Z = \{\cdot, +\}$, $R = \{(1',\cdot),(1', +),(2',\cdot)\}$,

$E_1 = \{1,2,(1',\cdot)\}$, $E_2=\{1,2,(1',+)\}$, $E_3 = \{2,3,(1',\cdot), (2',\cdot)\}$

$E_4 = \{1,3, 1',\cdot)\}$, $E_5=\{1,3,(1',+),(2',\cdot)\}$, $E_6=\{2,3,(1',+),(2',\cdot)\}$.

$E_7 = \{1,2,(2',\cdot)\}$, $E_8= \{1,2,3,(1',+)\}$. Тогда

$H_1 = (X;E_1,\ldots,E_7)$ и $H_2=(X;E_1,\ldots,E_8)$ являются гиперграфами.

Гиперграф $H = (X; E_1,\ldots,E_t)$ называется Шпернеровым [1], когда для $i \neq j$ имеет место $E_i \not\subseteq E_j$ $(i,j = 1,2,\ldots,t)$. В примере 1 гиперграф H_1 является Шпернеровым, а H_2 нет.

Дальше мы рассмотрим только Шпернеровы гиперграфы. Каждый гиперграф H однозначно определяет Шпернеров гиперграф, состоящий из всех минимальных ребер гиперграфа H. В 5 пункте данной статьи рассмотрим преобразования графов. Договоримся о том, что возникающий при этих преобразованиях, может быть, не Шпернеров гиперграф автоматически будет заменен соответствующим Шпернеровым гиперграфом.

Шпернеров гиперграф $H = (X;E_1,\ldots,E_t)$, для которого $X = V \cup R$, $R \subseteq W \times Z$, $|Z| = q$, называется $(k_1, \ldots, k_q)$ - раскрашиваемым, когда имеет место:

$$\forall_i \exists \phi_i \quad \forall_j : (1 \leq i \leq q \wedge (\phi_i : V \to \overline{1k_j}) \wedge E_j \subseteq V \cup W \times \{z_i\} \Rightarrow |\phi_i(E_j \cap V)| \geq 2) \qquad (3)$$

Рассматривая элементы $\phi_i(v)$, $v \in V$, как краски, условие (3) можно трактовать следующим образом:

Раскраской точек из V хотим достигать того, чтобы любое ребро E_j гиперграфа или в подребре $E_j \cap V$ или в подребре $E_j \cap R$ было бы раскрашено по меньшей мере двумя различными красками. Эта цель достигнута уже, когда E_j R содержит хотя бы два поразличному раскрашенные элементы. Если этого нет, то для любой краски $z_i \in Z$ должно существовать отображение ϕ_i такое, чтобы пересечение любого ребра с V, пересечение с R которого содержит не больше красок, чем z_i , содержало хотя бы две различные краски.

Определение. Гиперграф H обладает хроматическим набором $(k_1,\ldots,k_q)$, когда он является $(k_1,\ldots,k_q)$ - раскрашиваемым, но для $i=1,\ldots,q$ не является $(k_1,\ldots,k_i-1,\ldots,k_q)$ - раскрашиваемым.

Пример 2: Гиперграф $H = \{X;E_1,\ldots,E_7\}$ из примера 1 является (3, 2,) - раскрашиваемым, но не (3, 1) - или (2, 2) - раскрашиваемым гиперграфом, следовательно, он обладет хроматическим набором (3, 2) .

Если у заданного гиперграфа H для некоторого i условие (3) не выполнимо ни для никакого натурального числа k_i , /это имеет место точно тогда, когда существует ребро $E_j \subseteq V \cup W \times \{z_i\}$, пересечение с V которого пусто или мощности 1/, то на i-тое место хроматического набора гиперграфа H ставим ∞ .

3. АЛГЕБРА P_{Σ_q}

Пусть q - фиксированное натуральное число, $q \geq 1$. Пуст дальше

$$A_2 := \{0,1\}, \quad B_q := \{2, 3,\ldots,q+1\}.$$

Через $P_{\Sigma_q}^{n,m}$ обозначим множество всех $(n+m)$ - местных функций

$$f^{n,m}: A_2^{\,n} \times B_q^{\,m} \to A_2,$$

где $n,m \geq 0$. Дальше $P_{\Sigma_q} = \bigcup_{n,m\geq 0} P_{\Sigma_q}^{n,m}$.

Функции из P_{Σ_q} определяются нами формулами над алфавитами переменных $X := \{x,x_1,x_2,\ldots,\}$ и $Y := \{y,y_1,y_2,\ldots,\}$, причем переменные из X принимают значения только из A_2 и переменные из Y принимают значения только из B_q . Переменная функции $f^{n,m}(\underline{x}, \underline{y})$ называется существенной, когда существуют значения

$a_1, a_2,\ldots,a_n, a_i' \in E_2$ и $b_1,\ldots,b_m \in B_q$ такие, что

$$f(a_1,\ldots,a_i,\ldots,a_n, b_1,\ldots,b_m) \neq f(a_1,\ldots,a_i',\ldots,a_n, b_1,\ldots,b_m).$$

Аналогично определяются существенные переменные из Y . Всякая несущественная переменная некоторой функции называется фиктивной. Функции, отличающиеся только фиктивными переменными, будем считать одинаковыми. Местность функций будем опускать, когда это возможно без недоразумений.

Множество P_{Σ_q} вместе с операциями суперпозиции:

a/ перенумерование переменных из X или из Y между собой;

b/ идентифицирование некоторых переменных из X или из Y друг с другом;

c/ добавление или отпущение фиктивных переменных;

d/ подстановка функции вместо переменной X представляет собой алгебру, обозначаемую также через P_{Σ_q} . Каждому множеству $A \subseteq P_{\Sigma_q}$ сопоставляется его замыкание $[A]$ относительно этих операций. Если $A = [A]$, то множество A называется замкнутым.

Непосредственно видно, что $P_2 \subseteq P_{\Sigma_q}$. Используем привычные для булевых функций обозначения и для функций из P_{Σ_q} , поскольку и те и те имеют одинаковую область значений.

Кроме того определим функцию

$$e_i(y) = \begin{cases} 1 & \text{для } y=i \\ 0 & \text{иначе} \end{cases} \qquad i = 2, 3, \ldots, q+1$$

В дальнейшем воспользуемся обозначениями

$$\underline{i} = (i,i,\ldots,i) \qquad i=2,\ldots,q+1$$

$$\underline{x} = (x_1,x_2,\ldots,x_n)$$

$$\underline{y} = (y_1,y_2,\ldots,y_m)$$

$$\underline{\alpha} = (\alpha_1,\alpha_2,\ldots,\alpha_n)$$

$$\underline{\beta} = (\beta_1,\beta_2,\ldots,\beta_m)$$

$$E_{\underline{\beta}}(\underline{y}) := \bigwedge_{i=1}^{m} e_{\beta_i}(y_i) \qquad \underline{\beta} \in B_q^m .$$

Любая функция из P_{Σ_q} обладает нормальным представлением

$$f(\underline{x},\underline{y}) = \bigvee_{\underline{\beta} \in B_q^m} f_{\underline{\beta}}(\underline{x})\, E_{\underline{\beta}}(\underline{y}). \tag{4}$$

где

$$f_{\underline{\beta}}(\underline{x}) = f(\underline{x}, \underline{\beta}) \quad [5],[6]).$$

Функция $f_{\underline{\beta}}$ называется $\underline{\beta}$- компонентой функции f. Очевидно, что отображение

$$\tau_i : f^{n,m} \to f_{\underline{i}}$$

является гомоморфным отображением

$$P_{\Sigma_q} \quad \text{на} \quad P_2, \quad i=2,\ldots,q+1.$$

Дальше, определим

$$M^* := \bigcup_{n,m \geq 0} \{f^{n,m} \mid \forall \underline{\beta} \in B_q^m : f_{\underline{\beta}} \in M_1\}$$

$$K(M_{i_1},\ldots,M_{i_q}) := \Big(\bigcap_{j=1}^{q} \tau^{-1}(M_{i_j})\Big) \cap M^*, \qquad 1 \leq i_j \leq \infty.$$

Легко видно, что множества M^*, $K(M_{i_1},\ldots,M_{i_q})$ замкнуты. Пусть $(\Phi, \subseteq)$ обозначает структуру всех замкнутых множеств ал-

гебры P_{Σ_q} и положим

$$\Phi_M: \{K(M_{i_1},\ldots,M_{i_q}) \mid 1 \leq i_j \leq \infty, \quad j = 1,\ldots,q\}.$$

Теорема 1: $(\Phi_M, \subseteq)$ является дистрибутивной структурой. Эта структура тождественна интервалу

$$[K(M_\infty,\ldots,M_\infty),\ K(M_1,\ldots,M_1)] \text{ в } (\Phi,\subseteq)$$

и изоморфна $[M_\infty,\ M_1]^q$.

Эта структура именно та упомянутая в п. 1 исходная точка нашего обобщения теоремы Бензакена. Для доказательства нам нужны две леммы.

Лемма 1: Множества $\bar{K}_j := K(M_{i_1},\ldots,M_{i_{j+1}},\ldots,M_{i_q})$, $j=1,\ldots,q$, являются предполными подалгебрами множества

$K := K(M_{i_1},\ldots,M_{i_j},\ldots,M_{i_q})$.

Доказательство: Очевидно, что $\bar{K}_j \subset K$. . Пусть теперь $f^{n,m} \in K \setminus \bar{K}_j$. Тогда $f_j(\underline{x}) \in M_{i_j} \setminus M_{i_j+1}$, следовательно $\tau_i([\bar{K}_j \cup \{f\}]) = M_{i_j}$, поскольку M_{i_j+1} предполный класс в M_{i_j} , см. отобр. 1. Поэтому для произвольной функции $g^{r,s} \in K$ в $[\bar{K}_j \cup \{f\}]$ существует функция $g^{(i)}$, для которой $\tau_i(g^{(i)}) = \tau_i(g)$. Кроме того, в $\bar{K}_j$ содержится по определению функция

$$\ell^{r+q,s}(x_1,\ldots,x_r,\ x_{r+1},\ldots,x_{r+q},\ y_1,\ldots,y_s) ,$$

определенная формулой

$$\ell^{r+q,s}(\underline{x},\underline{y}) := \begin{cases} x_{r+t} & \text{если } \underline{y} = \underline{t+1},\ t = 1,\ldots,q \\ g^{r,s} & \text{иначе} . \end{cases}$$

Подстановкой функций $g^{(i)}$ в функцию ℓ вместо переменных x_{r+i}, $i = 1,\ldots,q$, получаем в $[K_j \cup \{f\}]$ функцию $g^{r,s}$. При образовании суперпозиций надо обратить внимание на следующее: Если функция u возникает подстановкой функции $w \in P_{\Sigma_q}$ в функцию $z \in P_{\Sigma_q}$ вместо некоторой переменной x_j , то функция

$u_{\underline{i}}$ /$\underline{i}$ - компонента функции u/ возникает подстановкой функции $w_{\underline{i}}$ /$\underline{i}$ - компоненты функции w / в функцию $z_{\underline{i}}$ /$\underline{i}$ - компоненту функции z / вместо переменной x_j.

Лемма 2: $\{\bar{K}_1,\ldots,\bar{K}_q\}$ является множеством всех содержащих в себе $K(M_\infty,\ldots,M_\infty)$ предполных подалгебр алгебры $K(M_{i_1},\ldots,M_{i_q})$ и обладает мощностью q.

Доказательство: Очевидно, $\bar{K}_i \neq \bar{K}_j$ для $i \neq j$. Пусть $f_j \in K \setminus \bar{K}_j$, $j = 1,\ldots,q$. Как известно, M_{i_j+1} является единственной содержащей множество M_∞ предполной подалгеброй алгебры M_{i_j} /см. отобр. 1/, поэтому

$$\tau_j[M_\infty \cup \{f_j\}] = M_{i_j}.$$

Теперь заключения идут дальше как в доказательстве леммы 1, обращая внимание на то, что $\ell^{r+q,s}$ лежит и в M_∞.

Из лемм 1 и 2 следует, что множество

$$\{K(M_{i_1},\ldots,M_{i_q}) \mid 1 \leq i_j \leq \infty, \quad j = 1 =\ldots, q\}.,$$

является интервалом $[K(M_\infty,\ldots,M_\infty), K(M_1,\ldots,M_1)]$ в $(\Phi, \subseteq)$, и что этот интервал антиизоморфен к структуре $\{(a_1,\ldots,a_q) \mid a_i \in N \cup \{\infty\}, \quad i=1,\ldots,q\}$ относительно покоординатного отношения $\leq$ /где положим $n \leq \infty$ для всех $n \in N$ /. Следовательно, оно является дистрибутивной структурой /ср. [10]/, изоморфной $[M_\infty, M_1]^q$. Этим доказана теорема 1.

4. ФОРМУЛЫ ДЛЯ МНОЖЕСТВА M^*

В этом участке определим формулы для функций множества M^* и исследуем на основе системы аксиом эквивалентность этих формул. При этом окажется, что множество M^* конечно аксиоматизуемо [3].

Даем определение вспомогательных формул:

1. Любой элемент множества

$$\mathfrak{E} := \{e_2(y_1), e_2(y_2), \ldots, e_3(y_1), e_3(y_2), \ldots, e_{q+1}(y_1), e_{q+1}(y_2), \ldots\}$$

является вспомогательной формулой.

2. Если E и E' - вспомогательные формулы, то и $E \cdot E'$ и $E \vee E'$ - вспомогательные формулы.

3. Вспомогательные формулы образованы только по 1. и 2.

Пусть $\mathfrak{M}$ - множество всех вспомогательных формул и $J(y_j)$ - сокращенный способ записи вспомогательной формулы

$$e_2(y_j) \vee e_3(y_j) \vee \ldots \vee e_{q+1}(y_j)$$

Определение формул:

1. Любой элемент множества

$$X = \{x, x_1, x_2, \ldots\}$$

является формулой.

2. Если F_1, F_2 - формулы и E - вспомогательная формула, то $F_1 \cdot F_2$, $F_1 \cdot E$, $E \cdot F_1$, $F_1 \vee F_2$ - формулы.

3. Формулы образованы только по 1. и 2.

Будем держаться привычным договоренностям о пользовании скобок и о сопоставлении функций формулам [2]. Пусть $\mathfrak{M}^*$ - множество всех формул.

Лемма 3: Любая формула из $\mathfrak{M}^*$ представляет собой функцию из M^* и любая функция из M^* представима формулой из $\mathfrak{M}^*$.

Доказательство предоставляем читателю.

Две формулы F_1 и F_2 называются эквивалентными, когда им соот-

ветствует одна и та же функция из P_{Σ_q} .

Для функции $f^{n,m}(\underline{x},\underline{y}) \in P_{\Sigma_q}$ пусть

$$N_f := \{\underline{\gamma} \in A_2^n \times B_q^m \mid f(\underline{\gamma}) = 1\}.$$

Для функции $\underline{\gamma} \in A_2^n \times B_q^m$ пусть $A_2(\underline{\gamma}) := (\gamma_1, \ldots, \gamma_n)$ и

$B_q(\underline{\gamma}) := (\gamma_{n+1}, \ldots, \gamma_{n+m})$.

Если $f^{n,m}(\underline{x},\underline{y}) \in M^*$ и $\underline{\beta} \in B_q^m$, то $f^{n,m}(\underline{x},\underline{y})$ - монотонная булевая функция, обычная сокращенная днф которой пусть будет обозначена через $\underline{\tilde{f}_\beta}$. Формула

$$\bigvee_{\underline{\gamma} \in N_f} \tilde{f}_{B_q(\underline{\gamma})} \cdot E_{B_q(\underline{\gamma})} \qquad (5)$$

называется кононической нормальной формой /Кнф/ функции

$$f(\underline{x}, \underline{y}) \in M^*$$

Аксиомы для $\mathfrak{M}^*$.

Для любых формул F_1, F_2, F_3 и любых вспомогательных формул E_1, E_2, E_3 и $\mathfrak{I}(y_j)$ имеет место:

(A1) $F_1 \cdot F_2 = F_2 \cdot F_1$

(A2) $F_1 \cdot E_1 = E_1 \cdot F_1$

(A3) $F_1 \cdot (E_1 \cdot E_2) = F_1 \cdot (E_2 \cdot E_1)$

(A4) $F_1 \vee F_2 = F_2 \vee F_1$

(A5) $F_1 \cdot (E_1 \vee E_2) = F_1 (E_2 \vee E_1)$

(A6) $(F_1 \cdot F_2) \cdot F_3 = F_1 \cdot (F_2 \cdot F_3)$

(A7) $(F_1 \cdot E_1) \cdot E_2 = F_1 \cdot (E_1 \cdot E_2)$

(A8) $(F_1 \cdot F_2) \cdot E_1 = F_1 \cdot (F_2 \cdot E_1)$

(A9) $F_1 \cdot [(E_1 \cdot E_2) \cdot E_3] = F_1 \cdot [E_1 \cdot (E_2 \cdot E_3)]$

(A10) $(F_1 \vee F_2) \vee F_3 = F_1 \vee (F_2 \vee F_3)$

(A11) $F_1 [(E_1 \vee E_2) \vee E_3] .= F_1 [E_1 \vee (E_2 \vee E_3)]$

(A13) $F_1 \cdot (E_1 \vee E_2) = F_1 \cdot E_1 \vee F_1 \cdot E_2$

(A14) $(F_1 \vee F_2) \cdot E_1 = F_1 \cdot E_1 \vee F_2 \cdot E_1$

(A15) $F_1 \vee F_1 = F_1$

(A16) $F_1 \cdot (E_1 \vee E_1) = F_1 \cdot E_1$

(A17) $F_1 \cdot F_1 = F_1$

(A18) $F_1 \cdot (E_1 \cdot E_1) = F_1 \cdot E_1$

(A19) $F_1 \cdot (y_j)\mathfrak{I} = F_1$

(A20) $F_1 \vee F_1 \cdot F_2 = F_1$

(A21) $F_1 \vee F_1 \cdot E_1 = F_1$

(A22) $F_1 \vee F_2 \cdot e_i(y_\ell) \cdot e_j(y_\ell) = F_1$ для $i \neq j$.

Для любых формул F_1, F_2 из $\mathfrak{M}^*$ $F_1 = F_2$ называется тождеством над $\mathfrak{M}$.

Правила вывода тождеств /ср. [3]/

1. $\dfrac{\Lambda}{x_1 = x_1}$, где Λ - пустое множество.

2. $\dfrac{F_1(F_2) = F_3, F_2 = F_4}{F_1(F_4) = F_3}$, замена некоторого вхождения формулы F_2 в формулу $F_1(F_2)$ формулой F_4 .

3. $\dfrac{F_1(\ldots, x_i, \ldots) = F_2(\ldots, x_i, \ldots)}{F_1(\ldots, F_3, \ldots) = F_2(\ldots, F_3, \ldots)}$, подстановка любой формулы F_3 во все вхождения переменной x_i в формулах исходного тождества, причем не исключено, что x_i не входит в $F_1(\ldots, x_i, \ldots)$ или $F_2(\ldots, x_i, \ldots)$.

Через $\mathfrak{I}$ пусть обозначено множество всех выводимых из аксиом /схем аксиом/ (A1) - (A22) тождеств над $\mathfrak{M}^*$.

Лемма 4. Для любых формул F_1, $F_2 \in {}^*$ имеет место: F_1 эквивалентно F_2 тогда и только тогда, когда $F_1 = F_2$ является тождеством из $\mathfrak{I}$.

Доказательство: Пусть F_1 эквивалентно F_2 . Легко видно, что

из Кнф $(f_1) \neq$ Кнф (f_2) и следует $f_1 \neq f_2$. От этого каноническая нормальная форма любой функции из M^* определена однозначно. Для доказательства леммы достаточно показать, что любую формулу F, представляющую функцию $f^{n,m}(\underline{x}, \underline{y}) \in M^*$, можно преобразовать с помощью аксиом в $\mathfrak{M} :=$ Кнф(f).

1 шаг: $F \xrightarrow{S_1} F^{(1)} := K_1 \vee K_2 \vee \ldots \vee K_t$, где каждый K_i возникает из элементов из X и Y образованием произведений, причем выступает по меньшей мере один множитель из X. Доказательство о переходе S_1 легко можно вести с использованием (A10),...,(A14), индукцией над числом $\mu_1(F)$ символов $\vee$ в формуле F.

2 шаг: $F^{(1)} \xrightarrow{S_2} F^{(2)} := L_1 \vee L_2 \vee \ldots \vee L_s$, где каждый L_i имеет форму

$$(\bigwedge_{j \in Z_i} x_j) \cdot E_{\underline{\beta}}, \quad \underline{\beta} \in B_q^m \qquad (6)$$

и не является подформулой другого члена дизъюнкции L_j, $j \neq i$.

Для этого сначала от каждого K_i переходим к произведению $K_i' \cdot K_i''$, у которого $K_i'(K_i'')$ является произведением над X(Y). Это возможно по (A1) - (A3), (A6) - (A9), (A17), (A18), (A20),(A21).После этого еще отсутствующие в K_i'' множители добавляются с помощью (A19) и полученные произведения сортируются по растущим индексам переменных из X и Y, в конце сокращаются лишние члены с помощью (A4), (A5), (A15), (A18), (A20) - (A22).

3 шаг: Собрание тех членов дизъюнкции в $F^{(2)}$, у которых один и тот же участок типа $E_{\underline{\beta}}$, в члены вида

$$\mathfrak{M}' \cdot E_{\underline{\beta}}$$

где $\mathfrak{M}'$ - формула из $\vee$, $\cdot$ над X. /Это возможно по (A4) (A10), (A12).) ./ После этого из каждой подформулы типа $\mathfrak{M}'$ привычным образом получаем сокращенную днф представленной формулой $\mathfrak{M}$ монотонной булевой функции. Этим выведена Кнф(5) функции f.

Доказательство обратного утверждения предоставляем читателю. Оно просто.

5. ОБОБЩЕНИЕ ТЕОРЕМЫ БЕНЗАКЕНА

Сначала рассматриваем отображение ρ множества всех Шпернеровых гиперграфов на множество всех функций в M^*. Для любого Шпернерового гиперграфа $H = (V, R; E_1, \ldots, E_t)$ пусть $\rho(H) := f \in M^*$, где f функция, заданная формулой

$$f_H := K_1 \vee K_2 \vee \ldots \vee K_t \qquad (7)$$

причем для каждого E_i вида

$$E_i = v_1, \ldots, v_a, (w_{\ell_{1,1}}, z_1), \ldots, (w_{\ell_{1,p_1}}, z_1), \ldots, (w_{\ell_{q,1}}, z_q), \ldots, (w_{\ell_{q,p_q}}, z_q)\},$$

$$a \geq 1, \quad p_1, \ldots, p_q \geq 0 \qquad (8)$$

поставляем

$$K_i := x_{v_1}, \ldots, x_{v_a} \cdot \bigwedge_{i=2}^{q+1} \bigwedge_{j=1}^{p_{i-1}} e_i(y_{\ell_{i-1,j}}).$$

Это отображение ρ, очевидно, сурьективно на M^*, но в общем не инъективно. Для этого даем два примера:

Пример 3: Пусть $q = 1$, $V = \{1,2\}$, $W = \{1'\}$

$Z = \{z_1\}$, $X = \{1,2,(1',z_1)\}$,

$H_1 = \{E_1, E_2\}$, $H_2 = \{E_3, E_4\}$,

$E_1 = \{1,(1',z_1)\}$, $E_2 = \{2\}$, $E_3 = \{1\}$,

$E_4 = \{2,(1',z_1)\}$.

Пример 4: Пусть $q = 1$, $V = \{1\}$, $W = \{1',2'\}$,

$$X = \{1,(1',z_1),\ (1',z_2),\ (2',z_1),\ (2',z_2)\},$$

$$H_1 = \{E_1,\ E_2\},\quad H_2 = \{E_1,\ E_3\},$$

$$E_1 = \{1,\ (1',z_1)\},\quad E_2 = \{1,(2',z_1)\}\ ,$$

$$E_3 = \{1,\ (1',z_2),\ (2',z_1)\}.$$

В обоих случаях имеет место равенство $\rho(H_1) = \rho(H_2)$, причем значение q существенно для выполнения этого равенства.

Лемма 5. Если для двух Шпернеровых гиперграфов H_1, H_2 имеет место равенство

$$\rho(H_1) = \rho(H_2),$$

то у H_1 и H_2 одинаковые хроматические наборы.

Доказательство: Из-за равенства $\rho(H_1) = \rho(H_2)$ функции f_{H_1} и f_{H_2} эквивалентные, значит по лемме 4 функцию f_{H_2} можно вывести из функции f_{H_1} применением аксиом (A1) - (A22) . Каждому применению аксиомы соответствует переход от одного гиперграфа к другому. Остается показать, что при этих переходах хроматический набор сохраняется неизменным. Легко видеть, что при применении (A1)-(A18), (A20)-(A22) либо сам гиперграф не меняется, либо аксиомы выражают некоторые требования гиперграфам /а именно, (A15) - (A17) выражают требование гиперграфу быть Шпернеровым, (A20) - (A22) соответствуют условиям (1), (2) для гиперграфов/.

Теперь обсуждаем переход от правой стороны формулы (A19) к левой.

Пусть F_1 - произведение над X и Y с по крайней мере одним множителем из X Тогда возможны следующие случаи:

1 случай: F_1 не содержит множителей из Y. Тогда соответствующее F_1 ребро гиперграфа H в (8) в раскраске гиперграфа, соответствующего левой стороне, охватывается каждой краской z_i, $i=1,\ldots,q$; тем самым каждое из q ребер

$$F_1 \cdot e_1(y_j), \ldots, F_1 \cdot e_{q+1}(y_j)$$

охватывается ровно одной из этих q красок. Хроматический набор не меняется.

2 случай: F_1 содержит множитель из Y. Если этот множитель содержит в свою очередь по меньшей мере два множителя, то по (2) как F_1, так и любое из ребер $F_1 \cdot e_i(y_j)$ без влияния на возможность раскраски. Если этот множитель в свою очередь состоит из одного множителя $e_i(y_j)$, то $F_1 \cdot e_2(y_j), \ldots, F_1 \cdot e_{q+1}(y_j)$ опять дают лишь соответствующее F_1 ребро, и гиперграф не меняется. Если же этот множитель состоит из одного множителя $e_i(y_\ell)$, $\ell \neq j$, то соответствующие $F_1 \cdot e_i(y_\ell) \cdot e_p(y_j)$, $p \neq i$, ребра в (8) не охватывается, в то же время, когда соответствующие выражениям $F_1 \cdot e_i(y_\ell)$ и $F_1 \cdot e_i(y_\ell) \cdot e_i(y_j)$ ребра в (8) охватываются одним и тем же образом. Поэтому хроматический набор не меняется.

Случай, где F_1 не является произведением над X и Y, можно вести к только что рассматриваемому случаю.

Теорема 2. Для любого Шпернерового гиперграфа $H = (V, R_i, E_1, \ldots, E_t)$, $R \subseteq W \times Z$, $q: |Z|$, имеет место: Гиперграф H обладает хроматическим набором $(k_1, \ldots, k_q)$, $2 \leq k_1, \ldots, k_1 < \infty$, точно тогда, когда

$$\rho(f) \in K(M_{k_1-1}, \ldots, M_{k_q-1}) \setminus \bigcup_{i=1}^{q} K(M_{k_1-1}, \ldots, M_{k_i}, \ldots, M_{k_q-1}). \tag{9}$$

При ограничении на функции из P_2 и соответствующие им Шпернеровы гиперграфы эта теорема была доказана К. Бензакеном [1]. В этом специальном случае отображение ρ оказывается биекцией.

Доказательство теоремы:

Из леммы 4 и 5 следует, что хроматический набор Шпернеровсго гиперграфа H тот же самый и у Шпернерового гиперграфа $\tilde{H}$, где $f_{\tilde{H}}$ есть каноническая днф функции f_H. Для раскрасов гиперграфа существенны только i-компоненты f_i функции f. Используя теорему Бензакена, сразу видно, что обладает хроматическим набором $(k_1,\ldots,k_q)$ точно тогда, когда $f_i \in M_{k_{i-1}} \setminus M_{k_i}$, $i=1,\ldots,q$, следовательно, когда имеет место (9).

ЛИТЕРАТУРА

[1] C. Benzaken, Posts closed systems and the weak number chromatic number of hypergraphs, Discrete Math. 23 (1978), 77-84.

[2] С.В. Яблонский, Г.П. Гаврилов, В.Б. Кудрявцев: Функции алгебры логики и классы Поста. Изд-во Наука, Москва 1966.

[3] Ю.И. Янов: О системах тождеств для алгебр, Проблемы кибернетики 8 /1962/, 75-90.

[4] G. N. Blochina, G. Burosch, V.B. Kudrjavcev, Vollständigkeitsbedingungen für zwei Algebren vom Postschen Typ, Math. Balkanica 3 (1973), 281-296.

[5] G. Burosch, Über Algebren von Prädikaten, Preprint (1974), Universität Rostock

[6] D. Lau, Prävolsständige Klassen von $P_{(k,1)}$, EIK 11 (1975), 10-12, 624-626.

[7] D. Lau, Kongruenzen aug gewissen Teilklassen von $P_{k,1}$, Rostocker Math. Kolloquium, Heft 3, 37-43.

[8] D. Lau, Basen und Ordnungen der maximalen Klassen zweier mehrsortiger Funktionenalgebren, Rostocker Math. Kolloquium 15 (1980), 81-90.

[9] G. Burosch, J. Dassow, W. Harnau, D. Lau, Über Algebreb von Prädikaten, eingericht EIK

[10] C. Greene, D.J. Kleitman, Proof techniques in the theory of finite sets, Studies in Combinatorics, G.-C. Rota ed., MAA (1978), 22-79.

[11] E. Schmidt, Unteralgebren zweier mehrsortiger Funktionenalgebren (I), Preprint (1980), WPU Rostock, ersch. in Rostocker Math. Kolloquium 17 (1980).

[12] E. Schmidt, Unteralgebren zweier mehrsortiger Funktionenalgebren (II), Preprint (1980), WPU Rostock

Ö S S Z E F O G L A L Á S:

A MONOTON FÜGGVÉNYEK OSZTÁLYAI ÉS KROMATIKUS SZÁMAI

A jelen dolgozatban általánositásra kerül K. B e n z a k e n egy tétele, amely a gráfok és a Post függvények közötti kapcsolatról szól. A dolgozat fő tétele a Sperner hiper gráfokkal kapcsolatos.

A B S T R A C T:

ABOUT CHROMATIC PAIRS AND LASSES OF MONOTON FUNCTIONS

The given article generalizes a theorem by *C. Benzaken*, who found a bijection between sets of graphs with a given chromatic number and closed subsets of the set of monotone functions from Post's lattice P_2 . The theorem of the article states an analogous bijection between sets of generalized Sperner hypergraphs with a given set of chromatic numbers and closed subsets of a set of monotone functions of the algebra P_{Σ_q}, where the algebra P_{Σ_q} contains all functions of the form

$$f : \{0,1\}^n \times \{2,\ldots,q+1\}^m \to \{0,1\}$$

MTA Számítástechnikai és Automatizálási Kutató Intézete, **Közlemények 25/1982**

THE SOLUTION OF HOSSZÚ-EQUATION OVER FINITE FIELDS*

János Bagyinszki

University of Gödöllő

1. PRELIMINARIES

M. Hosszú [H-67] considered the functional equation

$$f(x+y-xy)+f(xy)=f(x)+f(y) \tag{1.1}$$

with real variables x,y,f and solved it under the assumption that $f: \mathbb{R} \to \mathbb{R}$ is a differentiable function on the set $\mathbb{R}$ of real numbers. Several authors investigated equation (1.1). There have been two directions of generalization.

Weakening of the conditions for the function $f: \mathbb{R} \to \mathbb{R}$ was the first direction of generalizations; e.g. requiring the continuity at certain points [S-68.a] or, supposing integrability [D-69], [S-68.b]. Let us consider the well-known Jensen-equation

$$f\left(\frac{x+y}{2}\right)=f(x)+f(y) \tag{1.2}$$

and the Cauchy-equation

$$f(x+y)=f(x)+f(y) \tag{1.3}.$$

The equivalence of equations (1.1) and (1.2), and of equations (1.1) and (1.3) - has been proved for the sets

---

* Presented at the Kolloquium "Diskrete Mathematik und Anvendungen in der Mathematischen Kybernetik", Rostock, 30.3.1981-3.4.1981.

$\{f \mid f: \mathbb{R} \to \mathbb{R}\}$, $\{f \mid f: \mathbb{C} \to \mathbb{C}\}$ in the papers [S-68.b], [B-70], [D-71] and [V-69] ($\mathbb{C}$ denotes the field of complex numbers).

Some generalizations of the equation (1.1) and its solutions have been given in the papers [F-69], [L-72] and [L-74].

The definition and solution of the equation (1.1) over an algebraic structure (different from the field of real or complex numbers) is the second direction of generalizations. By the end of this section F,R,e,G denotes a field, a commutative ring with identity, identity of the field or ring and an Abelian group, respectively. In Świątak's paper [S-71] it has been shown that: if F is a field, whose characteristic is not 2 or 3, G is an Abelian group without 2-torsion and for every fixed $g \in G$ there is a homomorphism $\chi: F^{+} \to G$ such that $\chi(e)=g$, then equation (1.1) is equivalent to equation

$$2f(x+y)=f(2x)+f(2y) \tag{1.2'}$$

for functions $f: F \to G$. Aczél noticed [S-71] that Balnuša's proof for functions $f: \mathbb{C} \to \mathbb{C}$ is also valid for functions $f: F \to F$, if F is a quadratic closed field with certain additional conditions. In Davison's paper [D-74.a] functions of the type $f: R \to G$ have been investigated, where R is one of the three rings Z (rational integers), $Z/_{kZ}$ (integers mod k) and Q (the field of rational numbers). In case of $|F| \geq 5$, the equivalence of equation (1.1) and the equation

$$f(x+y)+f(0)=f(x)+f(y) \tag{1.3'}$$

has been proved in [D-74.b] for functions $f: F \to G$. Finally, if R is additively generated by their units and there exists a unit element $u \in R$ such that $e-u$ and $e-u-u^{-1}$ are units, then the equations (1.1) and (1.3') are equivalent for functions $f: R \to G$ if and only if, the equations (1.1) and (1.3') are equivalent for the functions $f': R/_{2R} \to G$.

2. RESULTS

We prove that, over a finite field, the class of generalized Hosszú-functions and the class of quasi-linear functions of $|F|$-valued logic are the same (in connection to our earlier results [B-D-76], [B-79], see also [R-77]). This fact refute a statement of [D-R-80], which asserts that for $|F|\leq 4$ there exists a Hosszú-function which is not a solution of the equation (1.3'). Our proof is entirely different from the proof of [D-74.b]; it is less complicated but it is valid only for a restricted domain. However, our proof is valid for n-ary functions, too. To the present knowledge of the author, the generalized Hosszú-functions have been introduced first in this paper.

For finite fields we solve a problem of H.Świątak and remark that we can extend the proofs to fields of characteristic p. Some of the proofs can be extended to more general classes of functions, $\{f \mid f:R\to G\}$. However, in this paper, the statement is restricted to finite fields. To formulate our theorems we need some defintions.

Let $R=\langle R;+,\cdot\rangle$ and $R'=\langle R';\oplus,\odot\rangle$ be commutative rings with identity, denote $G=\langle G;\boxplus\rangle$ and N an Abelian group and the set of non-negative integers, respectively. For a function $f:R^n\to G$ $(n\in N)$ we define the Hosszú-operator with the identity

$$H_{\tilde{x},\tilde{y}}\tilde{f}=f(\tilde{x}+\tilde{y}-\tilde{x}\tilde{y}) \boxplus f(\tilde{x}\tilde{y}) \boxminus f(\tilde{x}) \boxminus f(\tilde{y}), \qquad \text{where}$$

$\tilde{x}=(x_1,\ldots,x_n)$, $\tilde{x}+\tilde{y}=(x_1+y_1,\ldots,x_n+y_n)$, $\tilde{x}\cdot\tilde{y}=(x_1y_1,\ldots,x_ny_n)$.
We call the equation

$$H_{\tilde{x}\tilde{y}}\tilde{f}=0 \tag{2.1}$$

and their solutions (generalized) Hosszú-equation, and (generalized) Hosszú-functions, respectively.

It is easy to see that the following two lemmas hold:

Lemma 1: (1) The constant functions are Hosszú-functions.

(2) For every pair of functions (f_1,f_2) of the type $R^n \to G$ and every numbers $n_1,n_2 \in N$, the equality $H(n_1 f_1 \boxplus n_2 f_2)=n_1 \cdot Hf_1 \boxplus n_2 \cdot Hf_2$ is an identity.

Lemma 2: For every pair of functions (f_1,f_2) of the type $R^n \to R'$ and every constants $c_1,c_2 \in R'$, the equality $H(c_1 \odot f_1 \oplus c_2 \odot f_2)=c_1 \odot Hf_1 \oplus c_2 \odot Hf_2$ is an identity.

Further on, let $q=p^\alpha$, where p is a prime, $\alpha \geq 1$ integer, $F_q=GF(q)$.

Theorem 1: The function $f:F_q \to F_q$ is a Hosszú-function if and only if, f is a polynomial function of the form:

$$f(x)=\sum_{i=0}^{\alpha-1} a_i x^{p^i} + a_\alpha . \qquad (2.2)$$

Sketch of the proof: The functions of the form (2.2) are solutions of the equation (2.1) by the lemmas 1. and 2., because the identity $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ holds for rings of characteristic p. We have an indirect proof for the necessity of the condition (2.2) using the automorphism-group of F_q. We mention that this method could also be applied to fields of characteristic p.

Using this theorem and lemmas we have.

Theorem 2: The function $f:F_q^n \to F_q$ is a Hosszú-function if and only if, f is a polynomial function of the form

$$f(\tilde{x})=\sum_{j=1}^{n} \sum_{i=1}^{\alpha-1} a_{ij} x_j^{p^i} + a_\alpha . \qquad (2.3)$$

The next theorem solves a problem of Świątak (P.2. in [S-71]) if f is a function of the type $f:F_q \to F_q$. The theorem is formulated for unary functions and finite fields, but it can be extended to n-ary functions and fields of characteristic p in a similar way as it could be done to theorem 1.

Theorem 3: Let $P_i(x,y)+Q_i(x,y)=T(x,y)$, $i=1,2$ and $P_1 \neq P_2$ be two partitions of a polynom $T(x,y)$ over F_q. Assume that for every elements $u,v \in F_q^*$ the system of equations $P_1(x,y)=u$, $Q_1(x,y)=v$ has a solution (x,y). Then the function f is a solution of the equation

$$f(P_1(x,y))+f(Q_1(x,y))=f(P_2(x,y))+f(Q_2(x,y)) \qquad (2.4)$$

if and only if, f is a polynomial function of the form (2.2).

Remark: The sets A_q of functions $f:F\to F$ with $|F|\leq 4$ which are not a solution of equation (1.3'):

$$A_2=\emptyset,\ A_3=\{f(x)=a_o+a_1x+a_2x^2 \mid a_2\neq 0\} \text{ and}$$

$$A_4=\{f(x)=b_o+b_1x+b_2x^2+x^3\}.$$

It is easy to see that no elements of A_q $(q=3,4)$ are solutions of equation (1.1).

R E F E R E N C E S

A-66 Aczél, J., Lectures on Functional Equations and Their Applications, A.P., 1966.

H-67 Hosszú, M., $f(x+y-xy)+f(xy)=f(x)+f(y)$ (unpublished) Colloquium of Functional Equations, Zakopane, 1967.

S.68.a Świątak, H., On the functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Mat. Vesnik 5 (20), (1968), 177-182.

S-68.b Świątak, H., Remarks on the functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Aequationes Math., 1, (1968), 239-241.

D-69 Daróczy, Z., Über die Funktonalgleichung $f(xy)+f(x+y-xy)=f(x)+f(y)$, Publ. Math. Debrecen, 16, (1969), 129-132.

V-69 Vincze, E., 17. Bemerkung zum Vortrag von Herrn prof. Fenyő. Aequationes Math. 2 (1969), 374.

F-69 Fenyő, I., On the general solution of a functional equations in the domain of distributions, Aequationes Math., 3 (1969), 236-246.

B-70 Blanuša, D., The functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Aequationes Math., 5, (1970), 63-67.

D-71 Daróczy, Z., On the general solution of the functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Aequationes Math., 6, (1971), 130-132.

S-71 Świątak, H., A proof of the equivalence of the equation $f(x+y-xy)+f(xy)=f(x)+f(y)$ and Jensen's equation Aequationes Math., 6, (1971), 24-29.

L-72 Lajkó, K., Über die allgemeinen Lösungen der Funktionalgleihung F(x)+F(y)-F(xy)=H(x+y-xy), Publ. Math. (Debrecen) 19, (1972), 219-223.

L-74 Lajkó, K., Applications of extensions of additive functions, Aequationes Math. 11, (1974), 68-76.

D-74.a Davison, T.M.K., On the functional equation f(m+n-mn)+f(mn)=f(m)+f(n), Aequationes Math., 10, (1974), 206-211.

D-74.b Davison, T.M.K., The complete solution of Hosszú's functional equation over a field, Aequationes Math., 11, (1974), 273-276.

B-D-76 Bagyinszki, J. and Demetrovics, J., The structure of linear classes in prime valued logics (Hungarian) MTA-SzTAKI Közlemények, 16/1976, 25-52.

R-77 Rosenberg, I.G., Completeness properties of multiple--valued logic algebras, in "Computer Science and Multiple-valued Logic" (Ed, D.D. Rine) North Holland, 1977, 144-186.

B-79 Bagyinszki, J., Teh lattice of closed classes of linear functions over a finite ring of square--free order, Dept. of Math. Karl Marx Univ. of Economics, Bp. 1979-2., 1-21.

D-R-80 Davison, T.M.K. and Redlin, L., Hosszú's functional equation over rings generated by their units Aequationes Math., 20, (1980), 318-320.

ÖSSZEFOGLALÁS

Az irodalomban szereplő Hosszú-egyenletet általánositjuk többváltozós függvényekre, s az általánositott Hosszú-egyenletet megoldjuk véges testek fölött értelmezett függvényekre. A megoldásokat általánositott Hosszú-függvényeknek nevezzük.

Megmutatjuk, hogy véges testek fölött az általánositott Hosszú-függvények osztálya azonos a k-értékü logikai kvázi-lineáris függvényeinek osztályával (1. és 2. tétel).

Eredményeink megcáfolják Davison egy állitását.

Véges testek esetére megoldjuk Świątak egy problémáját, más irányba jelentősen általánositva a Hosszú-egyenletet (3. tétel).

Megjegyezzük, hogy a bizonyitások átvihetők p-karakterisztikáju testekre.

Р Е З Ю М Е

Бадински Янош

Уравнение, названное в литературе о М. Госсу, расширяется на функции со многими переменными и решается в случае функций, определенных над конечными полями. Решения называются обобщенными функциями Госсу.

Показывает, что над конечными полями класс обобщенных функций Госсу совпадает с классом квази-линейных функций к-значной логики. /Теоремы 1. и 2./

Эти результаты отрицают одно утверждение Дависона. Решается одна проблема Швиатака в случае конечных полей. При этом дается другое обобщение уравнения Госсу. /Теорема 3./

Заметим, что метод доказательств можно применить и в случае полей характеристикой р.

MTA Számítástechnikai és Automatizálási Kutató Intézete, Közlemények 25/1982

О НЕКОТОРЫХ ИНВАРИАНТНЫХ СВОЙСТВАХ ФУНКЦИЙ

К.Н. Чимев

В работе рассматриваются вопросы об инвариантности выделимых множеств аргументов функций при подстановке аргументов константами.

Используется терминология из [1-15].

Множество существующих переменных функции f будем обозначать R_f.

Определение 1. Пусть $f(x_1,x_2,\ldots x_n)$ функция порядка $n\geq 2$ и

$$R_1 \cup R_2 \subset R_f,\ R_1 \cap R_2 = \emptyset,\ R_1 \neq \emptyset,\ R_2 \neq \emptyset.$$

Множество R_1 называется выделимо для f по отношению R_2, если существуют такие значения для переменных из R_2, что после подстановки переменных этими значениями от f получается функция, которая зависит существенно от всех переменных принадлежащих R_1.

Если $|R_f| \geq 1$ будем считать, что множество R_f выделимо для f по отношению пустого множества.

Определение 2. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 1$ и

$$R \subset R_f,\ R \neq R_f,\ R \neq \emptyset.$$

Множество R называется выделимо для f, если R выделимо для f по отношению $R_f \setminus R$.

Множество R_f считается выделимым для f.

Множество всех выделимых множества аргументов функции $f(R_f \neq \emptyset)$

обозначенися S_f.

Определение 3. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$R\notin S_f,\ R\subset R_f,\ |R|\geq 2.$$

Множество $R_1 (R_1\subset R)$ называется максимально выделемо для f подмножества R, если $R_1\in S_f$ и не существует множество $R_2\in S_f$ для которого

$$R_1\subset R_2\subset R,\ R_2\neq R_1.$$

Отметим, что если

$$R\notin S_f,\ R\subset R_f,\ |R|\geq 2,$$

то существуют хотя бы два максимально выделимых для f подмножеств множества R. Если R_1 максимально выделимо для f подмножество множества R, то

$$|R\setminus R_1|\geq 1.$$

Теорема 1. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$R\notin S_f,\ R\subset R_f,\ |R|\geq 2.$$

Если R_1 максимально выделимо для f подмножество множества R, то для любых переменных

$$x_{i_1},x_{i_2},\ldots,x_{i_m}\in R\setminus R_1,\ 1\leq m\leq |R\setminus R_1|,$$

и для любых для них значений $c_{i_1},c_{i_2},\ldots,c_{i_m}$, функция $f(x_{i_1}=c_{i_1},\ldots,x_{i_m}=c_{i_m})$ зависит существенно хотя бы от одной из переменных $x_i\in R_f\setminus R$ и для нее выделимо множество R_1.

Доказательство. Пусть

$$R=\{x_1,x_2,\ldots,x_{m+p}\}\notin S_f,\ 2\leq m+p\leq n-1,\ p\geq 1,$$

и множество

$$R_1=\{x_1,x_2,\ldots,x_m\}$$

максимально выделимо для f подмножество множества R.

Не ограничивая общности исследования теорема будет доказана

для переменных $x_{m+1},\dots,x_{m+t}$, $1\le t\le p$. Пусть $c'_{m+1},\dots,c'_{m+t}$ произвольно выбраны значения для $x_{m+1},\dots,x_{m+t}$ и пусть

$$f_1=f(x_{m+1}=c'_{m+1},\dots,x_{m+t}=c'_{m+t}).$$

Выберем значения $c'_{m+p+1},\dots,c'_n$ для $x_{m+p+1},\dots,x_n$ таким способом, что $R_1\in S_{f_2}$, где

$$f_2=f(x_{m+p+1}=c'_{m+p+1},\dots,x_n=c'_n).$$

Но

$$R_{f_2}\cap\{x_{m+1},\dots,x_{m+p}\}=\emptyset,$$

и $R_1\subset R_{f_2}$. Следовательно $R_1=R_{f_3}$, где

$$f_3=f_2(x_{m+1}=c'_{m+1},\dots,x_{m+t}=c'_{m+t}).$$

Поэтому $R_1\in S_{f_1}$.

Так как $R_f\in S_f$, $R\notin S_f$ и $R\subset R_f$, то

$$R_f\setminus R\neq\emptyset.$$

Доказывается, что

$$R_{f_1}\cap(R_f\setminus R)\neq\emptyset$$

Действительно, допустим что

$$R_{f_1}\cap(R_f\setminus R)=\emptyset.$$

Тогда какие бы ни были значения $c_{m+p+1},\dots,c_n$ для $x_{m+p+1},\dots,x_n$,

$$R_1\in S_{f_1}(x_{m+p+1}=c_{m+p+1},\dots,x_n=c_n),$$

а следовательно

$$R_1\in S_f(x_{m+p+1}=c_{m+p+1},\dots,x_n=c_n).$$

Пусть $c''_{m+p+1},\dots,c''_n$ такие значения для $x_{m+p+1},\dots,x_n$, что $x_{m+1}\in R_{f_4}$, где

$$f_4=f(x_{m+p+1}=c''_{m+p+1},\dots,x_n=c''_n).$$

Но в соответствии с уже сказанным $R_1\in S_{f_4}$. Следовательно $R_1\subset R_{f_4}$. Тогда

$$R_1\subset R_{f_4}\subset R,\ R_1\neq R_{f_4},\ R_{f_4}=R,$$

и $R_{f_4}\in S_f$.

При сделанном допущении доказали, что R_1 не является макси-

мально выделимым для f подмножество множества R, которое противоречит данным условиям.

Таким образом теорема доказана.

Естественно возникает вопрос: если $f(x_1,x_2,\ldots,x_n)$ произвольная функция порядка $n\geq 3$ и

$$R\in S_f,\ R\subset R_f,\ |R|\geq 2,\ |R_f\setminus R|\geq 2,$$

и R_1 максимально выделимо для f подмножество множества R, то правда ли, что для любых переменных

$$x_{i_1},\ldots,x_{i_m}\in R\setminus R_1,\ 1\leq m\leq |R\setminus R_1|,$$

и для любых для них значений $c_{i_1},\ldots,c_{i_m}$ функция $f(x_{i_1}=c_{i_1},\ldots,x_{i_m}=c_{i_m})$ зависит существенно хотя бы от двух переменных из множества $R_f\setminus R$ и

$$R_1\in S_{f(x_{i_1}=c_{i_1},\ldots,x_{i_m}=c_{i_m})}\ ?$$

Примерно можно показать, что ответ поставленного вопроса отрицателен.

Можно показать, что если R_1 не является максимально выделимым для f подмножество множества R, заключение в теореме 1 в общем случае неверно.

Определение 4. Пусть функция $f(x_1,\ldots,x_n)$ порядка $n\geq 1$ и $R\subset R_f$ $(R\neq\emptyset)$. Будем говорить, что переменная $x_i\in R$ сильно существенная для f по отношению R, если существует такое значение c_i для x_i, что

$$R_{f(x_i=c_i)}\supset R\setminus\{x_i\}.$$

Переменная $x_i\in R$ будем называть сильно существенной для f, если она сильно существенная для f по отношению R_f.

Переменная x_i будем называть сильно существенной для f по отношению x_j, если она сильно существенная для f по отношению $\{x_i,x_j\}$.

Определение 5. Пусть функция $f(x_1,\ldots,x_n)$ порядка $n\geq 1$ и $R\subset R_f$ $(R\neq\emptyset)$. Будем говорить, что переменная $x_i\in R$, с - сильно существенная для f по отношению R, если для каждого значения c_i для x_i

$$R_{f(x_i=c_i)}\supset R\setminus\{x_i\}.$$

Переменная $x_i\in R$ будем называть с - сильно существенной для f, если она с- сильно существенная для f по отношению R_f .

Переменная x_i будем называть с- сильно существенной для f, по отношению x_j , если она с- сильно существенная для f по отношению $\{x_i,x_j\}$.

Следствие 1. Если $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и $R_1\in S_f$, $R_2\notin S_f$, где $R_1\subset R_2\subset R_f$, $R_1\neq\emptyset$, то существует переменная $x_i\in R_2\setminus R_1$, такая, что для каждого значения c_i для x_i,

$$R_{f(x_i=c_i)}\cap(R_f\setminus R_2)\neq\emptyset$$

и

$$R_1\in S_{f(x_i=c_i)}.$$

Следствие 2. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и $R\in S_f$, $1\leq|R|\leq n-2$.

Если существует переменная $x_i\in R_f\setminus R$, такая, что $R\cup\{x_i\}\notin S_f$, то для каждого значения с для x_i, $R_{f(x_i=c_i)}\cap(R_f\setminus(R\cup\{x_i\}))=\emptyset$ и $R\in S_{f(x_i=c_i)}$

Из следствия 2 следует, что x_i с -сильно существенная для f по отношению $R\cup\{x_i\}$.

Следствие 3. Если $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$\{x_i,x_j\}\notin S_f,\ i,j\in\{1,2,\ldots,n\},\ i\neq j,$$

то для каждого значения c_j для x_j,

$$R_{f(x_j=c_j)}\cap(\{x_1,\ldots,x_n\}\setminus\{x_i,x_j\})\neq\emptyset$$

и

$$x_i\in R_{f(x_j=c_j)}.$$

Из следствия 3 следует, что x_j с- сильно существенная для f по отношению x_i.

Следствие 3 является обобщением теоремы 6 от [5].

Следствие 4. Если $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$R\in S_f,\ R\subset R_f,\ 2\leq |R|\leq n-1,$$

то для каждой переменной $x_i\in R$ существует такая переменная $x_j\in R\setminus\{x_i\}$, что для каждого значения c_j для x_j,

$$R_{f(x_j=c_j)}\cap(R_f\setminus R)\neq\emptyset, \quad \text{и} \quad x_i\in R_{f(x_j=c_j)}.$$

Следовательно для каждой переменной $x_i\in R$ существует переменная $x_j\in R\setminus\{x_i\}$, которая c-сильно существенная для f по отношению x_i.

Следствие 5. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и $R\in S_f$, $|R|=n-2$.

Если существует переменная $x_i\in R_f\setminus R$, такая что

$$R\cup\{x_i\}\notin S_f,$$

то x_i является c-сильно существенным для f.

Следствие 6. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и $R\in S_f$, $|R|\leq n-2$.

Если существует переменная $x_i\in R_f\setminus R$, такая что

$$R\cup\{x_i\}\notin S_f \quad \text{и} \quad R_f(R\cup\{x_i\})\in S_f,$$

то x_i сильно существенная для f.

Следствие 7. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 4$ и $R\in S_f$, $|R|=n-3$

Если x_i и x_j такие переменные из $R_f\setminus R$, что

$$R\cup\{x_i,x_j\}\notin S_f,$$

то хотя бы одна из них сильно существенная для f.

Как уже увидели, если $f(x_1,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$\{x_i,x_j\}\in S_f,\ i,j\in\{1,\ldots,n\},\ i\neq j,$$

то каждая из переменных x_i,x_j является c-сильно существенным для f по отношению множества $\{x_i,x_j\}$.

Следствие 8. Если $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 4$ и $R\in S_f$ $|R|=3$, то хотя бы одна из переменных $x_i\in R$ c-сильно существенная для f по отношению R.

Можно показать, что существуют функции $f(x_1,x_2,\ldots,x_n)$ порядка $n\geq 4$ и существуют такие переменные x_i,x_j,x_k, $i,j,k\in\{1,\ldots,n\}$, что $\{x_i,x_j,x_k\}\in S_f$ и только одна из переменных x_i,x_j,x_k c-сильно существенная для f по отношению $\{x_i,x_j,x_k\}$.

При условиях следствия 8, хотя бы две из переменных множества R сильно существенны для f по отношению R.

Можно показать, что существует функция $f(x_1,x_2,\ldots,x_n)$ порядка $n\geq 5$ и существует множество R, такое что

$$R\in S_f,\ |R|=4\ ,\ R\subset R_f,$$

и не существует c-сильно существенная переменная для f по отношению R.

С помощью теоремы 1 можно доказать и другие утверждения.

Теорема 2. Если $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 4$ и $R_1\in S_f$, $R_2\notin S_f$, где

$$R_1\subset R_2\subset R_f,\quad |R_2\setminus R_1|=2,$$

то для каждой переменной $x_i\in R_2\setminus R_1$ и для каждого её значения c_i для которого $R_1\in S_{f(x_i=c_i)}$,

$$R_{f(x_i=c_i)}\cap(R_f\setminus R_2)\neq\emptyset.$$

Доказательство. При условии теоремы пусть

$$R_1=\{x_1,\ldots,x_m\}\in S_f,\ 1\leq m\leq n-3,$$

$$R_2=\{x_1,\ldots,x_m,x_{m+1},x_{m+2}\}\notin S_f.$$

Не ограничивая общности исследования, докажем теоремы, например, для переменной x_{m+1} .

Пусть c'_{m+1} такое значение для x_{m+1} , что

$$R_1 \in S_{f(x_{m+1}=c'_{m+1})}.$$

Допустим, что

$$R_1 \cap \{x_{m+3},\ldots,x_n\}=\emptyset$$

Тогда $R_1 \in S_{f_2}$, где

$$f_2=f(x_{m+3}=c_{m+3},\ldots,x_n=c_n),$$

и $c_{m+3},\ldots,c_n$ произвольные значения для $x_{m+3},\ldots,x_n$.

Пусть $c'_{m+3},\ldots,c'_n$ такие значения для $x_{m+3},\ldots,x_n$, что $x_{m+2} \in R_{f_3}$, где

$$f_3=f(x_{m+3}=c'_{m+3},\ldots,x_n=c'_n).$$

Так как $x_{m+2} \in R_{f_3}$ и $R_1 \in S_{f_3}$, то

$$R_3=\{x_1,\ldots,x_m\} \cup \{x_{m+2}\} \subset R_{f_3}.$$

Но $R_2 \notin S_f$. Поэтому $x_{m+1} \notin R_{f_3}$. Следовательно $R_3 \in S_f$.

Множество

$$R_3 \cup \{x_{m+1}\} \notin S_f,$$

и в соответствии с теоремой 1 для каждого значения c_{m+1} для x_{m+1} ,

$$R_{f(x_{m+1}=c_{m+1})} \cap \{x_{m+3},\ldots,x_n\} \neq \emptyset.$$

Следовательно

$$R_{f_1} \cap \{x_{m+3},\ldots,x_n\} \neq \emptyset,$$

которое приводит к противоречию.

Таким образом теорема доказана.

Можно поставить вопрос о верности заключения теоремы 2, когда

$$|R_2 \setminus R_1| \geq 3.$$

Примером можно показать, что ответ этого вопроса отрицателен.

Теорема 3. Пусть $f(x_1,x_2,\ldots,x_n)$ функция порядка $n\geq 3$ и $R_1\in S_f$, $R_1\neq\emptyset$.

Если $R_2\subset R_f\setminus R_1$, $R_2\neq\emptyset$, то существует пермутация $x_{i_1},x_{i_2},\ldots,x_{i_k}$, $k=|R_2|$, элементов R_2 и существуют такие значения $c_{i_1},c_{i_2},\ldots,c_{i_k}$, для $x_{i_1},\ldots,x_{i_k}$, что для каждого $z\in\{1,\ldots,k\}$,

$$R_1\cup R_2\ \{x_{i_1},\ldots,x_{i_k}\}\subset R_{f_z},$$

и $R_1\in S_{f_2}$, где

$$f_z=f(x_{i_1}=c_{i_1},\ldots,x_{i_z}=c_{i_z})$$

Доказательство. Пусть $f(x_1,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$R_1=\{x_1,\ldots,x_m\}\in S_f,\quad 1\leq m\leq n-1$$

и пусть

$$R_2=\{x_{m+1},\ldots,x_{m+k}\}\ R_f\setminus R_1,\quad m+k\leq n.$$

Тогда можно показать, что существует переменная $x_{i_1}\in R_2$ и существует значение c_{i_1} для x_{i_1} такое, что $R_1\in S_{f_1}$ и

$$R_1\cup R_2\setminus\{x_{i_1}\}\subset R_{f_1},$$

где

$$f_1=f(x_{i_1}=c_{i_1}).$$

Таким образом теорема доказана при $|R_2|=1$.

Если теорема верна, когда $|R_2|=k$, $(k\geq 1)$, то она верна и при $|R_2|=k+1$. Действительно, пусть $f(x_1,\ldots,x_n)$ функция порядка $n\geq 3$ и

$$R_1=\{x_1,\ldots,x_m\}\in S_f,$$

$$R_2=\{x_{m+1},\ldots,x_{m+k+1}\}\subset R_f\setminus R_1,\quad m+k+1\leq n.$$

Тогда существует переменная $x_{i_1}\in R_2$ и существует такое значение c_{i_1} для x_{i_1}, что

$$R_{f(x_{i_1}=c_{i_1})} \supset R_1 \cup R_2 \setminus \{x_{i_1}\}$$

и $R_1 \in S_{f(x_{i_1}=c_{i_1})}$.

Пусть x_{i_1} какая-нибудь переменная вышесказанного вида и c_{i_1} такое значение для x_{i_1}, что

$$R_{f_1} \supset R_1 \cup R_2 \setminus \{x_{i_1}\}$$

и $R_1 \in S_{f_1}$, где

$$f_1 = f(x_{i_1}=c_{i_1}).$$

Так как $R_1 \in S_{f_1}$ и

$$R_5 = R_2 \setminus \{x_{i_1}\} \subset R_{f_1} \setminus R, \quad |R_5| = k,$$

из индуктивного предположения следует, что существует перестановка $x_{i_2}, x_{i_3}, \ldots x_{i_{k+1}}$ элементов множества $R_2 \setminus \{x_{i_1}\}$ и существуют такие значения $c_{i_2}, c_{i_3}, \ldots c_{i_{k+1}}$ для $x_{i_2}, x_{i_3}, \ldots, x_{i_{k+1}}$, что для каждого $z \in \{2,3,\ldots,k+1\}$,

$$R_1 \cup R_2 \setminus \{x_{i_1}, \ldots, x_{i_z}\} \subset R_{f_z}$$

и $R_1 \in S_{f_z}$, где

$$f_z = f(x_{i_1}=c_{i_1}, \ldots, x_{i_z}=c_{i_z}).$$

Таким образом теорема доказана.

Теорема 4. Пусть $f(x_1, x_2, \ldots, x_n)$ функция порядка $n \geq 3$. Если

$$R_1 \notin S_f \qquad R_2 \in S_f$$

где

$$R_1 \subset R_2 \subset R_f, \qquad R_1 \neq \emptyset, \; R_1 \neq R_2,$$

то для каждой переменной $x_i \in R_2 \setminus R_1$ существует переменная $x_j \in R_1$, которая с-сильно существенная для f по отношению x_i.

Доказательство. Если $R_2 = R_f$ теорема доказывается индуктивным способом.

Рассмотрим случай, когда $R_2 \neq R_f$. Например, пусть

$$R_1 = \{x_1, \ldots, x_m\},$$

$$R_2=\{x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+p}\},\ 3\le m+p\le n-1.$$

Так как $R_2\in S_f$, то существуют такие значения $c_{m+p+1},\ldots,c_n$ для $x_{m+p+1},\ldots,x_n$, что

где $R_{f_1}=\{x_1,x_2,\ldots,x_m,\ldots,x_{m+p}\}$,

$$f_1=f(x_{m+p+1}=c_{m+p+1},\ldots,x_n=c_n).$$

Но

$$R_1\notin S_{f_1},\ R_2=R_{f_1},\ R_1\subset R_2,\ R_1\neq\emptyset,\ R_1\neq R_2.$$

Тогда, в соответствие с уже рассмотренным случаем для каждой переменной $x_i\in R_2\setminus R_1$ существует переменная $x_j\in R_1$, которая c-сильно существенная для f_1 по отношению x_i.

Следовательно для каждой переменной $x_i\in R_2\setminus R_1$ существует переменная $x_j\in R_1$, которая c-сильно существенная для f по отношению x_i.

Л И Т Е Р А Т У Р А

1. Яблонский С.В.: Функциональные построения в к-значной логике. Труды математического института им. В.А. Стеклова, т. 51, 1958, 5-142.

2. Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б.: Функции алгебры логики и классы Поста, Москва, 1966.

3. **Schwartz R.E.: Existence and uniqueness properties of Boolean functions. SIAM Journal on applied matematics, 1970, 18, 2, 454-461.**

4. Тоом А.Л.: О сложности реализации двоичных функций, имеющих мало "подфункций". Пробл. кибернетики, вып. 18, 1967, 83-90.

5. Чимев К.Н.: Върху някои свойства на функциите, Год. на ВТУЗ. Математика, т. **VII**, кн. 1, 1971, 23-32.

6. Чимев К.Н.: Върху инвариантността на отделимите двойки на функциите. Год. на ВТУЗ. Математика, т. **VIII**, кн. 1, 1972, 129-136.

7. Чимев К.Н.: Върху подфункциите и силно съществените променливи на функциите. Год. на ВТУЗ. Математика, т. **IX**, кн. 4, 1973, 43-55.

8. Чимев К.Н.: Върху отделимите двойки на функциите. Год. на ВТУЗ, Математика, т. **VII**, кн. 3, 1971, 7-12.

9. Лупанов О.Б.: Об одном классе схем из функциональных элементов. Сб. "Проблемы кибернетики", вып. 7, 1962, 61-114.

10. Соловьев Н.А.: К вопросу о существенной зависимости функции алгебры логики. Сб. "Проблемы кибернетики", вып. 9, 1963, 333-335.

11. Брейтбарт Ю.Я.: О существенных переменных функции алгебры логики. ДАН СССР, 1967, т. 172, № 1, 9-10.

12. Solomaa A.: On essential variables of functions, especially in the algebra of logic. Annales academiae scientiarum fennicae, ser.A, 339 /1963/, 1-11.

13. Чимев К.Н.: Върху силно съществените променливи на функциите от P_K. Год. на ВТУЗ. Математика, т. V, кн. 2, 1968/69, 155-162.

14. Чимев К.Н.: Върху зависимостта на функциите от P_K от аргументите им. Год. на ВТУЗ. Математика, т. IV, кн. 3, 1967, 5-13.

15. Чимев К.Н.: Върху отделимите подмножества и силно съществените променливи на функциите. Год. на ВТУЗ. Приложна математика, т. X, кн. 4, 1974, 7-13.

16. Csimev K.N.: Függvény argumentumai halmazának leválasztásáról. MTA SzTAKI Közlemények, 24, 1980, 19-25.

Összefoglaló

Függvények invariáns tulajdonságairól

A cikkben függvények bizonyos argumentumhalmazainak az argumentumok rögzítésére vonatkozó invarianciájával kapcsolatos kérdéseket tárgyal a szerző.

Summary

On some invariant properties of functions

In the paper the author looks over some problems of the invariancy of certain sets of arguments of functions with respect to replacement of arguments by constants.

MTA Számítástechnikai és Automatizálási Kutató Intézete, **Közlemények 25/1982**

HOW TO CONSTRUCT A LARGE SET OF NON-EQUIVALENT FUNCTIONALLY CAMPY LATE ALGEBRAS

J. Demetrovics - L. Hannák

Many authors have investigated certain classes of functionally complete algebras. The finite algebras $\langle A,t\rangle$ and $\langle A,d\rangle$ with the discriminator t and the dual discriminator d, respectively, all but 6 homogeneous algebras and other types of algebras having a 'large' automorphism-group were proved to be functionally complete. See Werner [6], Fried-Pixely [2], Csákány [1], Pálfy-Szabó-Szendrei [4]. In the present paper we are going to determine the number of non-equivalent functionally complete algebras. We call the algebras $\langle A,F\rangle$ and $\langle A,B\rangle$ equivalent if $[F]=[B]$ where $[F]$ denotes the set of all polynomials of $\langle A,F\rangle$. We denote the set of all functions on A by O_A. In the following $E_\ell=\{0,1,\dots k-1\}$ will present the base set of the investigated algebras and $\mathfrak{C}$ denotes the cardinality of the continuum.

In the case $|A|=2$ we have a complete description of all algebras (See E. Post [5]), and so we know, that there are only finitely many non-equvalent functionally complete algebras with a two-element base set. In the case $|A|=3$ we shall prove the existence of many functionally complete algebras. In the case $|A|=3$ we cannot prove any equality, but we can easily construct a nonfinite set of functionally complete algebras.

Proofs of our theorems are based on the well-known constructions of Janov and Mucnik, and on the fact that for every k there is a function $s(x,y)$ with $[s]=O_{E_k}$.

Let us define for $n>3$ $g_n(x_1,\dots x_n)$ as follows:

$$g_n(x_1,..,x_n)=\begin{cases}1 \text{ if, } x_j=1 \text{ and for } i\neq y\ x_i=z\\ s(x_1,x_2) \text{ if for } i>2\ x_i=3\\ 0 \text{ otherwise.}\end{cases}$$

Since $g_n(x_1,x_2,3,3,\circ,3)=s(x_1,x_2)$ and $[s]=0_{E_k}$, all the g_n-s are functionally complete. Let $\mathcal{G} = \bigcup_{n>3} g_n$. We shall prove that $g_n \notin [G \setminus g_n]$:

Let $\mathfrak{A}$ $(x_1,\ldots x_n)$ be a polynomial of $\langle E_k, G\setminus g_n\rangle$.

Let $g_m(x_{i1},..,x_{im})$ be any subformula of $\mathfrak{A}$ so, that all the s_{ij}-s are variables. Since $m\neq n$ we have two cases:

1. $|\{i_1,..,i_m\}|<n$. Then let $g_e=1$ for a fixed $\ell \notin \{i_1,\ldots i_m\}$ and $y_i=z$ for $\ell\neq i$. Then we have $\mathfrak{A}$ $(y_1,..,y_m)=0$ and - by definition - $g_n(g_1,\ldots y_n)=1$.

2. $|\{i_1,\ldots i_m\}|=n$. Then there are at least two indices i_{ℓ_1}, i_{ℓ_2} so, that $i_{\ell_1}=i_{\ell_2}=t$; we can choose $y_t=1$ and $y_j=1$ for $j\neq t$, and so we also obtain $\mathfrak{A}$ $(y_1,\circ\circ y_n)=0$ and $g_n(y_1,..,y_n)=1$.

Theorem 1: Let $|A|>3$. Then the cardinality of non-equivalent functionally complete algebras is $\mathfrak{C}$. In the case $k=3$ let us define g_n as follows:

$$g_n(x_1,..,x_n)= \begin{cases} 2 \text{ if } |\{i/k_i=2\}|\geq n-1 \text{ and} \\ \qquad |\{i/k_i=0\}|=0. \\ s(x_1,x_2) \text{ if for } j\geq 3\ x_j=0, \\ 1 \text{ otherwise.} \end{cases}$$

In this case all g_n are also functionally complete. Let $\mathcal{G}^n = \bigcup_{i>n} g_i$. We shall prove $g_n \notin [\mathcal{G}^n]$, and so we obtain, that

$$\mathcal{G}^m \supsetneq \mathcal{G}^{m+1} \supsetneq \ldots \supsetneq \mathcal{G}^{m+k} \supsetneq \ldots$$

If $g_n \in [\mathcal{G}^n]$, then there is a polynomial of $\langle E_k, \mathcal{G}^n\rangle$, $\mathfrak{A}(x_1,..,x_n)$, so that $\mathfrak{A}$ $(x_1,\circ\circ,x_n)=g_n(x_1,..,x_n)$. Let us consider the set $Y\ (E_k)^n$, where

$$Y=\{(y_1,..,y_n)\,|\,(y_1,..,y_n)\in\{1,2\}^n \text{ and } |\{y|y_j=1\}|=1\}.$$

Since $\mathfrak{A}$ $(x_1,\ldots x_n)=g_n(x_1,..,x_n)$ holds, we can choose a "minimal" polynomial $\mathfrak{A}^*\in[\mathcal{G}^n]$ so that

$$\mathfrak{A}^*|_Y = g_n|_Y \quad \text{and,}$$

if $\mathfrak{A}^*$ is written in the form $\mathfrak{A}^* = g_q(\mathcal{L}_1,..,\mathcal{L}_q)$ then there is no $\mathcal{L}_i$ with $\mathcal{L}_i|_Y = g_n|_Y$.

By $\mathfrak{A}^* \in [G^n]$ we have $q>n$. The set Y has exactly n elements and so $\mathcal{L}_i|_Y \neq g_n|_Y$ implies that there is at least one $y \in Y$ and j_1, j_2 such, that $\mathcal{L}_{j_1}(y) = \mathcal{L}_{j_2}(y) = 1$, and hence $\mathfrak{A}^*|_Y \neq g_n|_Y$.

This contradiction proves our

Theorem 2. For all $k>2$ there are at least countable many non-equivalent functionally complete algebras.

REFERENCES

1 B. Csákány: HOmogeneous algebras are functionally complete, Algebra Universalis, 11 (1980), 149-158.

2 E. Fried - A. Pixely: The dual discriminator function in universal algebra, Acta Sci. Math, 41 (1979), 83-100.

3 Ju. I. Janov - A.A. Mucnik: Existence of k- valued closed classes without finite basis. Dokl. Akad. Nauk. USSR. 127 (1959) 44-46.

4 P.P. Pálfy — L.Szabó - Á. Szendrei: Algebras with doubly transitive automorphism groups. Coll. Math. Soc. J. Bolyai 28. Finite Algebra and Multiple-Valued Logic Szeged Hungary 1979.

5 E. Post: Introduction to general theory of elementary propositions. Amer. J. Math. 93 (1921) 183-185.

6 H. Werner: Eine Characterisisierung functional vollständiger Algeberen, Archive der Math., 21 (1970), 381-385

Összefoglaló

Hogyan konstruáljunk sok nem-ekvivalens funkcionálisan teljes algebrát

Jelen dolgozatban a szerzők a következő kérdésre keresik a választ: mi a nem-ekvivalens funkcionálisan teljes algebrák száma egy rögzített véges alaphalmazon. Az $\langle A, F \rangle$ és $\langle A,B \rangle$ algebrákat ekvivalensnek nevezzük, ha az általuk generált klonok egyenlőek ($[F] = [B]$). Konstruálnak kontinuum sok nem ekvivalens funkcionálisan teljes algebrát legalább 4 elemű alaphalmaz fölött.

Резюме

Как надо построить много неэквивалентных функционально полных алгебр

В настоящей работе авторы изучают следующий вопрос: сколько неэквивалентных функционально-полных алгебр существует. Алгебры $\langle A,F \rangle$ и $\langle A,B \rangle$ эквивалентные, если $F = B$. В настоящей работе авторы построят континуум неэквивалентных функционально полных алгебр, если $|A| \geq 4$.

MTA Számítástechnikai és Automatizálási Kutató Intézete, **Közlemények 25/1982**

ON FUNCTIONALLY COMPLETENESS OF PRIME-ELEMENT ALGEBRAS

J. Demetrovics - L. Hannák - L. Rónyai

Several authors have discussed the question of giving conditions for the functional completeness of a finite algebra. A major part of these theorems is concerned with the fact that if the automorphism-group of the algebra is a sufficiently large subgroup in the permutations of the base set, then the algebra is functionally complete, if we disregard some exceptions. For example for every finite algebra $\langle A,t\rangle$ or $\langle A,d\rangle$, $|A|>2$ where t,d are the discriminator function and dual discriminator function respectively, it was known, that they are functionally complete. (See H. Werner [12] and E. Fried, A. Pixley [4].) In this case Aut $(\mathfrak{A})$ is the full symmetric group on . A generalization of this result was given by B. Csákány [2] who proved that all but six homogeneous algebras (algebras for which Aut $(\mathfrak{A})=S_A$ where A is the base set of $\mathfrak{A}$) are functionally complete. Analogous results were showed by Á. Szendrei - L. Szabó [10] and P.P. Pálfy - Á. Szendrei - L. Szabó [6]. These theorems are the following:

[10]: A finite algebra $\mathfrak{A}=\langle A,F\rangle$ with triply transitive automorphism group is either functionally complete or equivalent to an affine space over the $GF(2)$.

[6]: A finite algebra $\mathfrak{A}=\langle A,F\rangle$, with doubly transitive automorphism group is either functionally complete or equivalent to an affine space over a finite field.

The structure of affine spaces (or in terms of k-valued logics: linear closed classes) is well known. (See J. Bagyinszki - - J. Demetrovics [1] and Á. Szendrei [11].) According to the above results, these exceptional algebras are sufficiently

described. The authors give a similar result for special algebras with transitive automorphism groups. Other notions and notations are to be found in G. Grätzer [5] and R. Pöschel, L.A. Kaluznin [7].

THEOREM.

Let $\mathfrak{A} = \langle A, F \rangle$ be an algebra where $|A| = p$ and $p \geq 3$ is a prime number. Suppose that Aut $(\mathfrak{A})$ is a transitive subgroup of S_A. Then $\mathfrak{A}$ is either functionally complete or polynomially equivalent to an affine algebra over the $GF(p)$.

In the two element lattice the dual discriminator is an algebraic function (this is the median) but this structure is not functionally complete - since all algebraic functions are isotone. On the other hand d is a homogeneous function, hence the restriction $p \geq 3$ is essential.

It is easily seen that in our case the transitivity of Aut $(\mathfrak{A})$ means that Aut $(\mathfrak{A})$ contains a cycle of length p, which we shall denote by φ. Of course, the subgroup $\langle \varphi \rangle$ itself acts transitively on the set A. To simplify notations, we can suppose $A = \{0, 1, \ldots, p-1\}$ and $\varphi : x \to x+1$ for all $x \in A$ where + denotes the addition mod p.

The proof uses Rosenberg's completeness theorem. (I.G. Rosenberg [9], R.W. Quackenbush [8].) The authors show that whenever F preserves none of the linear relations of A, then it will preserve none of the six types in Rosenberg's classification. The main problem was to show that in the above case $\mathfrak{A}$ is simple.

It is well known that for an arbitrary algebra $\mathrm{Con}(\mathfrak{A}) = \mathrm{Con}(\langle A, F_1 \rangle)$ with F_1 denoting the set of all unary algebraic functions of $\mathfrak{A}$. This simple fact suggests to investigate the unary algebraic functions of $\mathfrak{A}$. A basic tool in the proof was the following

LEMMA 1.

Let $\mathfrak{A} = \langle A, F \rangle$ be a non-trivial algebra with $|A| = p, p \geq 3$ prime with its operations being not all projections and with $\varphi \in \mathrm{Aut}(\mathfrak{A})$.

Then at least one of the following cases holds

a) $F_1 \cap S_A \neq \langle id_A \rangle_T$

b) There is a $k \not\equiv 0 \pmod{p}$ and there are f, g elements of F_1 for which $1 < |imf| < p$ and for all $y \in imf$ $g(y) = y + k$ hold.

An easy consequence of Lemma 1 is

LEMMA 2.

In the case b.) in Lemma 1 there is a $h \in F_1$ for an arbitrary $k \in A$ with $h(y) = y + k$ for all $y \in imf$.

For all $f \in F_1$ $\varphi^{-1} f \varphi \in F_1$ holds, and in the case a.) of Lemma 1 it means that $F_1 \cap S_A$ is a transitive subgroup of S_A. So in each of the above two cases we have a "large" set of unary algebraic functions.
The following two lemmas facilitate handling central and k-regular relations. (See [7], [8]). Let O_A denote the set of all operations on A with finite arites.

LEMMA 3.

Let $\rho \subseteq A^k$ be a k-ary totally reflexive relation and $k \geq 3$. If $H \subseteq O_A$ such that all operations in H are surjective (or constant) then $\rho \in Inv H$ implies $\rho' \in Inv H$ where

$$\rho' = \{(x, y) \mid (x, y, a_1, \ldots, a_{k-2}) \in \rho \quad \text{for all} \quad a_1, \ldots, a_{k-2} \in A\}.$$

LEMMA 4.

Let H, ρ, ρ' be as defined in Lemma 3.

i) If ρ is a non-trivial central relation then ρ' is also central with the same center.

ii) If ρ is a k-regular relation defined by the equivalence relations $\Theta_1, \ldots, \Theta_m$ then

$$\rho' = \bigcap_{i=1}^{m} \Theta_i$$

In the possession of the above media Theorem is easy to prove. Its statement underlines the technical character of Lemma 1. J. Bagyinszki and J. Demetrovics proved that every linear closed class properly containing constant functions and projections will contain a permutation different from the identity. So, if $\mathfrak{A} = \langle A, F \rangle$ is a non-trivial affine algebra then $S_A \cap F_1 \neq \langle id_A \rangle$. This fact and the Theorem show that in all cases the statement a.) of Lemma 1 holds. At last we mention two consequences of the Theorem.
A subset H of O_A is called basic if for all Slupecki functions $f, [\{f\} \cup H] = O_A$ holds. (Then for arbitrary $X \subseteq O_A$ $[X]$ denotes the closed class generated by X.) A group $G \leq S_A$ is a basic group if G is a basic subset in O_A. L. Szabó has conjectured (personal communication) the following:

Let $\mathfrak{A} = \langle A, F \rangle$ be a nontrivial finite algebra and assume that $\mathrm{Aut}(\mathfrak{A})$ is a basic group. Then $\mathfrak{A}$ is functionally complete. From our theorem follows:

COROLLARY 1.

If $\mathfrak{A} = \langle A, F \rangle$, $|A| = p$ and p is a prime number then Szabó's conjecture holds.

Let A be a nonempty set and $\pi \in S_A$. The graph ρ_π of π can be defined as follows:

$$\rho_\pi = \{(x_1 \pi(x)) \mid x \in A\}$$

That is, $\rho_\pi \subseteq A^2$ is binary relation on A. J. Demetrovics and L. Hannák in [3] have proved the following: if $|A| \geq 5$ then for arbitrary $\pi \in S_A$, $Pol\ \rho_\pi$ contains a continuum cardinality set of closed classes. In other words in this case there is a continuum cardinality set of polynomially non-equivalent algebras $\mathfrak{A}_\beta = \langle A, F_\beta \rangle$ $(\beta < \mathfrak{c})$ for which $\pi \in Aut(\mathfrak{A}_\beta)$ $(\beta < \mathfrak{c})$. This result and our Theorem imply:

CORALLY 2:

If A is a prime element set and $|A| \geq 5$ then there is a continuum cardinality set of pairwise polynomially non-equivalent functionally complete algebras $\mathfrak{A}_\beta = \langle A, F_\beta \rangle (\beta < \mathfrak{c})$.

In the case $|A| = 3$ the authors cannot tell even the number of different algebras with $\varphi \in Aut(\mathfrak{A})$.

REFERENCES

[1] *Bagyinszki, J., Demetrovics, J.,* Lineáris osztályok szerkezete primszámértékü logikában, *MTA SZTAKI Közlemények,* 16 (1976) 25-52.

[2] *Csákány, B.,* Homogeneous algebras are functionally complete, *Algebra Universalis,* to appear.

[3] *Demetrovics, J., Hannák, L.,* On the cardinality of self-dual classes in k-valued logics, *MTA SZTAKI Közlemények* 23(1979) 8-17.

[4] *Fried, E., Pixley, A.,* The dual discriminator function in universal algebra. *Acta Sci. Math.* 41 (1979), 83-100.

[5] *Grätzer, Gy., Universal algebra.* D. van Nostrand, Princeton N.J. (1968).

[6] *Pálfy, P. P., Szendrei, Á., Szabó, L.,* Algebras with transitive automorphism groups. *Coll. Soc. J. Bolyai* 28 (1979), Szeged.

[7] *Pöschel, R., Kaluzin, L.A., Funktionen- und Relationen-algebren,* VEB Deutscher Verlag der Wissenschaften, Berlin (1979).

[8] *Quackenbush, R.W.,* A new proof of Rosenberg's primal algebra characterisation theorem. To appear.

[9] *Rosenberg, I.G.,* Über die funktionale Vollständigkeit in den mehrwertigen Logiken, *Rozpr. CSAV. Rada Mat. Prir. Ved.,* Praha 80, 4 (1970), 3-93.

[10] *Szendrei, Á., Szabó, L.,* Almost all algebras with triply transitive automorphism groups are functionally complete. *Acta Sci. Math.* 41 (1979), 391-402

[11] *Szendrei, Á.,* On closed sets of linear operations over a finite set of square-free cardinality. *Elektron. Informationsverarb. Kybernet.,* v. 14 (1978) 547-559.

[12] *Werner, H., Discriminator-algebras.* Akademie-Verlag, Berlin (1978).

AUTHORS' ADDRESS:

J. DEMETROVICS, L. HANNÁK, L. RÓNYAI:

Computer and Automation Institute Hungarian Academy of Sciences
H 1502 Budapest XI. Kende u. 13-17.
Phone 297-861

Összefoglaló

Prímszám elemű algebrák függvény-teljességéről

A jelen dolgozatban a szerzők a tranzitív automorfizmus csoporttal rendelkező algebrákkal foglalkoznak. A fő eredmény szerint ezen algebrák vagy függvényteljesek, vagy lineárisok. Az eredmények bizonyítás nélkül szerepelnek.

Р е з ю м е

О функциональной полноте алгебр с простыми числами элементов

В настоящей работе занимаемся функциональной полнотой некоторых алгебр. Главный результат настоящей работы заключается в том, что изучаемые алгебры либо функционально полные , либо линейные.

MTA Számítástechnikai és Automatizálási Kutató Intézete, **Közlemények 25/1982**

GENERALIZATION OF THE SELFDUALISM IN THE LIMIT-LOGIC M

É. Gárdos

1. INTRODACTION

The notion of the limit-logic was introduced by S.V. Yablionski [16] in 1958. The necessity of this notion arose in the study of finite-valued logics [15] and infinite logics [17]. In partucular, the infinite-valued logics contain as many as continuum functions, thus, working with this logics is very difficult. Therefore the necessity of such a logic was recognized that contains countably many functions and can be regarded, from a certain point of view, as the model of all k-valued logics. It was prooved, that they are continuum, pairwise non-isomorphic limit-logics [1].

The partial ordering introduced in [1, 14], in a logical way, also decomposes the set of limit-logics into equivalence classes, and under such a partial ordering there are already maximum and minimum limit-logics. Such a logic is maximal to the extent that it contains every other limit-logic, and is minimal if it is contained in every limit-logic.

In this work we examine limit-logic M, which is a representation of the - in previouse sense - maximal limit-logic. In this, we give the generalization of the notion of the selfdualism in the limit-logic M.

2. ELEMENTS

Definition 2.1

Let E_k be an arbitrary aset of k elements. Denote by P_k^n $(n=0,1,2,\ldots)$ the set of functions with n variables, with the variables and values taken from the set E_k. The function

set $P_k = \bigcup_{n=0}^{\infty} P_k^n$ will be called k-valued logic. Without loss of generality we suppose $E_k=\{0,1,\ldots,k-1\}, k\geq 2$.

Definition 2.2

If the finite set E_k in Definition 2.1 is replaced by the countably infinite set $E_{\aleph_o}$, the function set $P_{\aleph_o}$ will be called the infinite-valued logic. In this paper, $E_{\aleph_o}$ will always be the non-negative integers, that is $E_{\aleph_o}=\{0,1,\ldots,n,n+1,\ldots\}$.

Definition 2.3

We say the subset P of $P_{\aleph_o}$ infinite-valued logic is a limit-logic, if it is performed the next conditions:

a/ in the function set P contains countably many functions.

b/ for every natural number k ($k\geq 2$) exits such a function set $A_k \subseteq P$, wich is constitutable in a homomorphic way to the k-valued logic.

The notions of maximum, superposition, closure, pre-completness are defined as in [15] and in [4].

We shall define a representation M of the maximal limit-logics, which we are going toexamine in detail:

Definition 2.4 [2].

Define the function $\mu_k(x_1,x_2)\in P_{\aleph_o}$ ($k>2$) as follows:

$$\mu_k(x_1,x_2)=\begin{cases} e, & \text{if } (x_1,x_2)\in E_k \times E_k \text{ and } \max(x_1,x_2)=e-1, \\ & \text{where } 1\leq e-1\leq k-1; \\ 1, & \text{if } (x_1,x_2)\in E_k \times E_k \text{ and } \max(x_1,x_2)=k; \\ 0, & \text{otherwise.} \end{cases}$$

Let M_k denote the closure of the function-set $\{\mu_k(x_1,x_2)\}$, i.e. $M_k=[\{\mu_k(x_1,x_2)\}]$ and $M=[\bigcup_{k=2}^{\infty} M_k]$.

Remark 2.1

It is easy to see that M is isomorphic with P_k and M is a limit-logic.

Remark 2.2

The functions of the limit-logic M have the property

$$f(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n)=0.$$

Definition 2.5

Let be $\varepsilon_o,\varepsilon_1,\ldots,\varepsilon_t$ a disintegration D of the $E_{\aleph_o}$, with are pairwise disjunktive and non-empty subsets. Then, let be note $U_{\varepsilon_o,\varepsilon_1,\ldots,\varepsilon_t}$ the set of the all functions $f(x_1,\ldots,x_n)\in P_{\aleph_o}$, which satisfy: if

$$(a_1,\ldots,a_n)\sim(b_1,\ldots,b_n) \pmod D, \text{ then}$$
$$f(a_1,\ldots,a_n)\sim f(b_1,\ldots,b_n) \pmod D.$$

Definition 2.6

We say that the function $f(x_1,\ldots,x_n)\in P_{\aleph_o}$ preserves the set $R\subset E_{\aleph_o}$ (i.e. type of $T_{R,0}$) if $f(R,R,\ldots,R)\subseteq R$.

3. THE SELFDUAL FUNCTION CLASSES OF THE LIMIT-LOGIC M

In this paragraph we examine the selfdual function classes of the limit-logic M. We prove that the selfdual function classes of M are closed and we give necessery condition for the pre-completness.

Definition 3.1

Let be P a limit-logic, E a subset of the $E_{\aleph_o}$ and $g(x_1,\ldots,x_n)\in P$. Let $g_E(x_1,\ldots,x_n)$ denote the function, which is interpreted on the set $\underbrace{ExEx\ldots xE}_{n \text{ time}}$ and there it is equal $g(x_1,\ldots,x_n)$, otherwise it is 0. I.e.:

$$g_E(x_1,\ldots,x_n)=\begin{cases} g(x_1,\ldots,x_n), & \text{if } x_1,\ldots,x_n\in E^n \\ 0 & \text{otherwise.}\end{cases}$$

The function $g_E(x_1,\ldots,x_n)$ will be called the restriction of $g(x_1,\ldots,x_n)$ to E.

Remark 3.1

Of course we shall speak about the elementwise restriction of the function class M_{ε_γ} to E_γ. This means no restriction to the validity of the theorems. We define the set ε_γ, starting from a function $f(x_1,\ldots,x_n)\in M$ as follows:

1. Let α denote the maximum in the range of $f(x_1,\ldots,x_n)$,
2. Let β be the largest value in some n-tuple, on which the functions isn't equal to 0. $(f(\ldots,\beta,\ldots)\neq 0)$.
3. Let $\gamma=\max(\alpha,\beta)$, $\varepsilon_\gamma=\{1,2,\ldots,\gamma\}$ $(\gamma\leq k)$.

Let be $g(x)\in P^1_{\aleph_o}$ a permutation. Denote by $g_{E_k}(x)$ the restriction of the function g(x) to the set. (Similary $f_{E_k}(x_1,\ldots,x_n)$).

Definition 3.3

We say that the function $f(x_1,\ldots,x_n)\in M_k$ is selfdual with respect to the function $g(x)\in P_{\aleph_o}$ for arbitrary $x_i\in E_k$, if it is equal with the dual of the function $f(x_1,\ldots,x_n)$ respect to g(x), (denote with $f^{g(x)}(x_1,\ldots,x_n)$). That is $f(x_1,\ldots,x_n)\equiv f^{g(x)}(x_1,\ldots,x_n)$ or

$$g(f(x_1,\ldots,x_n))=f(g(x_1),\ldots,g(x_n)) \quad \text{for } \forall x_i \in E_k,$$

where $k \geq \gamma$ (see Remark 3.1.).

Theorem 3.1.

If the function $g(x) \in P^1_{\aleph_o}$ a finite permutation, than the set of the selfdual functions with respect to this function $g(x)$ (denote $S^k_{g(x)}$):

1/ closed

2/ $S^k_{g(x)}=M_k$, if $g_{E_k}(x)=x$

3/ the function class $S^k_{g(x)}$ is pre-complete, if the function $g(x)$ factorisable to composition of equal, cardinal number r long cycle.

Proof [19].

4. NOTION OF THE COMMUTABLE IN THE LIMIT-LOGIC M

Let be $g(x) \in P^1_{\aleph_o}$ an one variable function. Then $g(x)$ or

a/ finite permutation

b/ non permutation

c/ infinite permutation.

Definition 4.1

We say that the function $f(x_1,\ldots,x_n) \in M_k$ is commutable with $g(x) \in P^1_{\aleph_o}$ if $g(f(x_1,\ldots,x_n))=f(g(x_1),\ldots g(x_n))$. (Note this function set with V_g).

Remark 4.1

a/ If $g(x)$ is a finite permutation, than the notion of the commutable is same with the notion of selfdualism.

b/ Let we examine the second case, when the function $g(x)$ isn't permutation.

Definition 4.2

We say that $f(x)\in P^1_{\aleph_o}$ is maximal, if $f(x)\neq x$ and ins't other $g(x)\neq x$, that the set of the commutable functions respect to $g(x)$ will before detailed than the set of the commutable functions rexpect to $f(x)$.
(I.e. $\not\forall g(x)\in P^1_{\aleph_o}$ that $V_g \supset V_f$).

Let be $g(x)\in P_{\aleph_o}$ a non permutation. Then easy to see that the next lemmas are true, which are simple generalization of the finite case. These lemmas and proofs of the finite case can be read (6,7,8).

Lemma 4.1

$g(x)\in P^1_{\aleph_o}$ $(g(0)=0)\cdot g^2(x)=g(x)$ iff $A_{g(x)} \cup F_{g(x)}=E_{\aleph_o}\setminus 0$, when

$A_{g(x)}=\{a \mid a\in E_{\aleph_o}\setminus 0$ and $\not\exists b\in E_{\aleph_o}\setminus 0,\ g(b)=a\}$,

$F_{g(x)}=\{a \mid a\in E_{\aleph_o}\setminus 0, g(a)=a\}$.

Lemma 4.2

Let be $f(x)\in P_{\aleph_o}$ $(f(0)=0)$ non permutation. Then $f(x)$ is maximal exactly then, when $f^2(x)=f(x)$.

By reason of Lemma 4.1 and 4.2, we must be examine two cases for the maximal non permutation $g(x)\in P_{\aleph_o}$.

1/ The number of fixed points of $g(x)$ is finite
$(|F_g|=n,\ F_g=\{a_1,a_2,\ldots,a_n\})$

2/ the number of fixed points of $g(x)$ is infinite
$(|F_g|=\aleph_o,\ F_g=\{a_1,a_2,\ldots\})$

1/ Let be $g(x)\in P_{\aleph_o}$ $(g(0)=0)$, $F_g=\{a_1,\ldots,a_n\}$, $\ell=\max\{a_i\}, i=1,\ldots,n$.

Then easy to see that the next theorems are true

Theorem 4.1

The function $f(x_1,\ldots,x_n)\in M$ iff is commutable with the maximal non permutation $g(x)\in P_{\aleph_o}$ for $\forall x_i\in E_k$, when

$f(x_1,\ldots,x_n)\in T_{F_{g_o}\cap U S_1\ldots S_n | E_k}$ where

$F_g=\{a \mid g(a)=a \text{ and } a\in E_k\}$, $S_i=\{b \mid b\in E_{\aleph_o}\setminus 0 \text{ and } g(b)=a_i\}$ $i=1,2,\ldots,n$

$$S_i=|_{E_k}=\{b \mid b\in S_i \text{ and } b\in E_k\}$$

2/ $g(x)\in P_o$ $(g(0)=0)$ is a maximal non permutation with infinite number fixed points.

Then $F_g=\{a_1,a_2,\ldots\}$, $|F_g|=\aleph_o$,

$S_i=\{b \mid b\in E_{\aleph_o}\setminus 0 \text{ and } g(b)=a_i\}$ $i=1,2,\ldots$

Theorem 4.2

A function $f(x_1,\ldots,x_n)\in M$ is commutable with a maximal non permutation $g(x)\in P^1_{\aleph}$ $(g(0)=0)$ with infinite number fixed-point, if $g(x)$ a map E_k onto E_k i.e. $g(x)\in E_k$, $\forall x\in E_k$).

Theorem 4.3

If $g(x)\in P^1_{\aleph_o}$ $(g(0)=0)$ is a maximal non permutation with infinite number fixed point, for wich exists such a $E_k\subseteq E_{\aleph_o}\setminus 0$, that $g(x)$ preserves E_k, than exists such a $f_{E_k}(x_1,\ldots,x_n)\in M$ that

$$f_{E_k}(x_1,\ldots,x_n)\in T_{F_{g_{E_k},0}\cap U S_1,\ldots S_i | E_k}=V_g$$

where

$$F_{g_{E_k}}=\{a \mid a\in E_k \text{ and } g(a)=a\}$$

$$S_{i_{E_k}}=\{b \mid b\in E_k \text{ and } g(b)=a_i\} \quad 1\leq i\leq k.$$

Remark 4.2.

There exists such a maximal non permutation $g(x) \in P_{\aleph_o}$ $(g(0)=0)$, for which doesn't exist set $E_k \subset E_{\aleph_o} \setminus 0$ so, that for every $x \in E_k$ is true that $g(x) \in Ek$.

Example:

x	0	1	2	3	4	5	6	7	8	...
g(x)	0	4	2	6	4	8	6	10	8	....

c.)

Theorem 4.4.

Let be $s(x) \in P_{\aleph_o}$ a infinite permutation. Than doesn't exist such function $f(x) \in M$, that $f(x)$ is commutable with $s(x)$.

LITERATURE

1 J.Demetrovics: A határérték-logikák homomorfizmusairól Alk.Mat.1./1975/. 125-138.

2 J.Demetrovics: Az M maximális határérték-logikákról Alk.Mat.2./1976/. 57-66.

3 S.L.Lec. E.T.Lee: On multivalued Symmetric Functions, IEEE. Trans. on Computers C-21. /1972/. 312-317

4 I.Rosenberg: Uber die Verschi den keit maximaler Klassen Rev. Roum.math jures et appl. 14, /1969/ 413-438

5 D.L.Webb: Generation of any n-valued logic by one binary operator. Proc. Mat. Acad. Sci 21. /1953/ 252-254.

6 W.Harnau: Die definition von Vertauschbarkeitsmengen in die der k-vertigen Logik und das Maximalitätsproblem Zeitschr. f. math. Logik und Grundlagend.Math. 20/1974/ 339-352.

7 W.Harnan: Die Vertauschbaren Funktionen der k-werigen Logik und ein Basisproblem Zeitschr. f. math. Logik und Grundlagen d. Math. 20 /1974/

8 W.Harnau: Die teilweise geordnete Menge P_k der Vertauschbarkeitsmengen der k-wetigen Logik Zeitschr. f. math. Logik und Grundlagen d.Math. 22. /1976/ 19-28.

9 Г.П. Гаврилов: О мощности множества предельных логик, обладаюших конечным базисом. Сб. "Проблемы кибернетики" вып. 21, М., "Наука" /1969/, /113-126/.

10 В.М. Гниденко: Нахождение порядков предельных классов в трехзначной логике. Сб. "Проблемы кибернетики", вып. 8., М., /1962/, /341-346/.

11 Я. Деметрович: О числе попарно неизоморфных предельных логик. Сб. "Дискретный анализ", вып. 24, Новосибирск, "Наука", /1974/, /21-29/.

12 Я. Деметрович: О сравнении предельных логик при моделировании в них конечнозначных логик. Акта Кибернетики, /1974/, /2/.

13 Я. Деметрович: О свойствах минимальной предельной логики. Штудиа Мат. Акад. Шси. Нунг. 9., /1974/, /1-2/.

14 Я. Деметрович: О некоторых гомоморфизах и отношениях для предельных логик. Сб. "Проблемы кибернетики" 30., Москва, /1975/, /5-42/.

15 С.В. Яблонский: Функциональные построения в к-значной логике, Труды Мат. АН СССР, 51., /1958/, /5-142/.

16 С.В. Яблонский: О предельных логиках, Докл. АН СССР 118.4. /1958/, /657-660/.

17 С.В. Яблонский: О некоторых свойствах счетных замкнутых классов из . Докл. АН СССР 124.5., /1959/, /990-993/.

18 С.В. Яблонский, Г.П. Гаврилов, В.Б. Кудрявцев: Функции алгебры логики и классы Поста. "Наука", Москва, /1966/.

Z U S A M M E N F A S S U N G

DER VERALLGEMEINER DER VERTAUSCHBARKEIT VON FUNKTIONEN AUS DEN GRENZE-LOGIK M.

In diesem Aufsatz wir erhielten folgende Ergebnisse:

1, Wenn $g(x) \in P_{\chi_o}$ ist eine endliche Permutationen, dann der Begriff der Selstdualismum ist derselbe wie der Begriff der Vertauschbarkeit.

2, Wenn $g(x) \in P_{\chi_o}$ ist nicht eine Permutationen, dann $f(x_1,\ldots,x_n) \in T_{F_{g,o}} \cap U_{S_1 \ldots S_n} \mid E_k$.

3, Wenn $g(x) \in P_{\chi_o}$ ist eine unendliche Permutationen, dann ist keine $f(x) \in M$, dass die Funktionen $f(x)$ ist vertauschbar mit $g(x)$.

Ö S S Z E F O G L A L Á S

A FELCSERÉLHETŐSÉG FOGALMÁNAK ÁLTALÁNOSITÁSA AZ M HATÁRÉRTÉK-LOGIKÁBAN

Ebben a dolgozatban a felcserélhetőség fogalmát vizsgáltuk az M határérték-logikában.

A következő eredményekre jutottunk:

1, Ha $g(x) \in P_{\chi_o}$ egy véges permutáció, akkor az öndualitás fogalmával teljesen azonos a felcserélhetőség fogalma.

2, Ha $g(x) \in P_{\chi_o}$ nem permutáció, akkor $f(x_1,\ldots,x_n) \in M$ függvény akkor és csak akkor felcserélhető $g(x)$-vel, ha

$$f(x_1,\ldots,x_n) \in T_{F_{g,o}} \cap U_{S_1 \ldots S_n} \mid E_k.$$

3, Ha $g(x) \in P_o$ végtelen permutáció, akkor nem létezik olyan $f(x) \in M$ függvény, amely felcserélhető $g(x)$-vel.

MTA Számítástechnikai és Automatizálási Kutató Intézete, Közlemények 25/1982

ИССЛЕДОВАНИЕ ОДНОГО КЛАССА АБЕЛЕВЫХ КОДОВ С ИСПОЛЬЗОВАНИЕМ ЭВМ

П. Лакатош, А. Пете

В теории кодирования важное место занимает вопрос оптимизации связи между расстоянием кода и длинной кодовых слов, т.к. последняя непосредственно влияет на затраты связанные с передачей и исправимостью кодированной информации.

В настоящей статье обсуждается один класс, так называемых абелевых кодов, и попутно наши решаются некоторые интересные сами по себе проблемы, касающиеся векторного пространства над двухэлементным полем.

Пусть G -абелева группа и K поле. Произвольный I идеал групповой алгебры KG будем называть абелевым кодом. Ясно, что если G -конечна, то KG -векторное пространство конечной размерности над K .

Если обозначим через $w(x)$, $x \in I$ вес кодового слова, т.е. число компонентов его отличных от нуля, то вес кода I может быть выражен как

$$d(I) = \text{мин}\ w(x)$$
$$0 \neq x \in I$$

Пусть $G=(a_1)x\ldots x(a_n)$; $a_i^2=1$; $i=1,2,\ldots,n$; и K

поле характеристики отличной от 2. Тогда абелевый код бинарен, и известно что KG -полупростая алгебра, и т.о. для произвольного идеала I представления:

$$KG = I \oplus \bar{I}$$
$$I = I_1 \oplus \ldots \oplus I_s$$
$$\bar{I} = I_{s+1} \oplus \ldots \oplus I_{2^n}$$

($\bar{I}$-дополнительный идеал идеала I)

где I_j -минимальный идеал генерируемый идемпотентом e_j $(j = 1,2,\ldots,2^n)$ однозначны.

Следующая теорема была доказана в [1]:

<u>Теорема:</u> Пусть $\mathcal{H}^* = \{X_{s+1},\ldots,X_{2^n}\}$ множества характеров неизоморфных неприводимых представлений соответствующих $e_{s+1},\ldots, e_{2^n}$ идемпотентам $\bar{I}$. Если X характер некоторой подгруппы $H \subseteq G$ порядка 2^k не может быть получен ограничением системы $\mathcal{H}^*$ на H то

$$X = \sum_{a \in H} X(a^{-1})a \in I$$

По утверждению теоремы в I существует элемент с весом 2^k и т.о. $d(I) \leqslant 2^k$.

В дальнейшем подгруппу H со свойствами условий теоремы будем называть подгруппой ассоцированной с системой характеров $\mathcal{H}^*$.

Обозначим при заданных n и k через

- $t(n,k)$ - наибольшее число для которого существует такое множество характеров с количеством элементов $t(n,k)$ для которого может быть определена ассоцированная подгруппа порядка 2^k.
- $l(n,k)$ - наибольшее число, такое что для любого множества

группы характеров G с числом элементов $l(n,k)$ существует ассоцированная группа порядка 2^k.

- $p(n,k)$ - наименьшее число, для которого существует множество характеров с числом, элементов $p(n,k)$, такое что у него нет ассоцированной подгруппы порядка 2^k.

Ясно что $p(n,k) = l(n,k)+1$; $t(n,k) \geqslant l(n,k)$. В [1] доказываются также следующие утверждения. Пусть

$q(n,k) = \sum_{i=0}^{k} C_n^i$ (C_n^i-комбинаторный коеффициент), тогда:

(1) $d(n,k) < q(n,k)$ если $1 < k < n-1$

$l(n,k) = q(n,k)$ если $k=1$ или $k=n-1$

(2) $p(n,k) \leqslant q(n,k)$ если $1 < k < n-1$

(3) $p(n,k) \leqslant q(n,k) - \sum_{i=1}^{} \sum_{j=i-1}^{} ([\frac{n+j}{2i}]-1)$, $n \geqslant 4$

([a] - обозначает целую часть числа a)

В настоящей статье приводится алгоритм определения вышеупомянутых границ, описанный на языке PL /1, при помощи которого были выполнены конкретные вычисления.

Проблема представляет интерес и с точки зрения комбинаторики т.к. $p(n,k)$ - мощность наименьшего состоящего из векторов длинной 2^k множества, такого, что для любый k x 2^n бинарной матрицы могут быть выбраны k векторов, так что составленная из них матрица размерности 2^n x k, умноженная на предидущую матрицу даёт в результате обратимую бинарную матрицу.

1.

Прежде чем перейти к обсуждению алгоритма остановимся на нескольких результатах, которые ведут к сокращению времени вычисления. Будем говорить, что множество характеров $\mathcal{H}^*$ k-реализуемо на G , если ни одна из подгруппы группы G порядка 2^n не ассоциируема с $\mathcal{H}^*$.

Пусть $\mathcal{H} = (X_1)X\ldots X(X_n)$, где характеры X_i $(i = 1,2,\ldots,n)$ составляют базис $\mathcal{H}$ группы характеров для G . В [1] указывается что для этого базиса всегда может быть выбран такой $a_1, a_2, \ldots, a_n$ базис G , что

$$(4) \qquad X_i(a_j) = \begin{cases} -1 & \text{если } i = j \\ 1 & \text{если } i \neq j \end{cases}$$

Базис G обладающий этим свойством мы будем называть дуальным по отношению к $X_1,\ldots,X_n$ базису.

Лемма 1: Если $\mathcal{H}^1 \subseteq \mathcal{H}$ (H-группа характеров для G) такое множество характеров, что для любого $e \neq g \in G$ существует такой $X \in \mathcal{H}^1$, что $X(g) = -1$, тогда $\mathcal{H}^1$ порождаёт $\mathcal{H}$.

Доказательство: Пусть для $\mathcal{H}^1$ -с заданным свойством $\{\mathcal{H}^1\} = \mathcal{H}^2 \subset \mathcal{H}$, и пусть $\mathcal{H}^2 = (X^{i_1})X\ldots X(X^{i_e})$, тогда $e < n$ и так базис может быть дополнен элементами $X^{i_{e+1}},\ldots X^{i_n}$ до базиса $\mathcal{H}$. Пусть дуальным базисом базиса $X^{i_1},\ldots,X^{i_n}$ будет $b_1 b_2,\ldots b_n$:
Из-за (4) $X^{i_e}(b_n) = 1$ для всех элементов X из $\mathcal{H}^1$. Получая противоречие $\mathcal{H}^2 = \{\mathcal{H}^1\} = \mathcal{H}$, мы приходим к выводу что $\mathcal{H}^1$ со свойствами теоремы и очевидно любое к-реализуемое множество характеров содержит некоторый базис $\mathcal{H}$.

Будем говорить, что в индексе элемента X присутствует i, если в базисном разбиении приводимом в (4) присутствует X_i и обозначим через $X_{i_1 i_2 \ldots i_j}$ характер $X_{i_1}X_{i_2}\ldots X_{i_j}$ $(1 \leqslant i_k \leqslant n;$ $k = 1,2,\ldots,j)$.

Замечание: По лемме 1 любое к-реализуемое $\mathcal{H}^*$-множество характеров содержит один из базисов $\mathcal{H}$-группы характеров G , и т.о. всегда достижимо что $\mathcal{H}^*$ содержит характеры с одним индексом.

Действительно, достаточно переиндексировать дуальный базис в соответствии с (4).

Теорема 1: Пусть $\mathcal{H}^*$ 2-реализуемое подмножество группы $\mathcal{H}$ и $1 \leqslant i \leqslant n$, тогда если $\mathcal{H}^*$ содержит одноиндексные характеры, то в индексах элементов $\mathcal{H}^*$ индекс i появляется по крайней мере n-раз.

Доказательство: Достаточно доказать теорему для случая i=1. Рассмотрим $\{a_1, b\}$ $b \neq a_1 c, e$; $c, b \in G$ - подгруппу четвёртого порядка. Характер $X \in \mathcal{H}^*$ тогда принимает значение $(-1, \pm 1)$ на генерирующей паре, если $X = X_1 \cdot X'$ и в индексе X' 1 не присутствует.

Пусть $\mathcal{H}^1 = \{X \mid X \in \mathcal{H}^*, \quad X = X_1 \cdot X'\}$. По предположению теоремы $X_1 \in \mathcal{H}^1$. Пусть $\bar{\mathcal{H}}^1 = \{X \mid X \in \mathcal{H}^1, \quad X \neq X_1\}$, очевидно что элементы $\bar{\mathcal{H}}^1$ характеры подгруппы $G^1 = (a_1) X \ldots X (a_n)$. Так как по предположению $\mathcal{H}^*$ реализуемо для любой подгруппы G четвёртого порядка, в том числе реализуемо и для подгруппы генерируемой парой (a_1, b), для произвольного $b \in G^1$ существует такой $X' \in \bar{\mathcal{H}}^1$, для которого $X'(b) = -1$ поэтому по лемме 1 $\bar{\mathcal{H}}^1$ генерирует подгруппу $\mathcal{H}$ порядка 2^{n-1}. Из-за $\mathcal{H}^1 = \bar{\mathcal{H}}^1 \cup \{X_1\}$ и тем самым теорема доказана.

Результаты приводимые в дальнейшем непосредственно направлены на упрощение определения границ для $p(n,к)$ и $l(n,к)$.

Лемма 2: Для n=5 и $\mathcal{H}^*$ - 13 элементная 2-реализуемся система, то при помощи трансформации базиса может быть достигнуто что $\mathcal{H}^{1'} = \{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^*$ и $\mathcal{H}^*$ со-

держит по крайней мере один характер с индексом 1 не принадлежащий $\mathcal{H}^{1)}$.

Доказательство: Если $n=5$ то по теореме 1 если существует 13-элементная 2-реализуемая система, то есть и такая $\mathcal{H}^*$ для которой в индексах элементов $\mathcal{H}^*$ каждый индекс появляется по крайнер мере 5-раз и эта система $\mathcal{H}^*$ содержит и одноиндексные элементы. Предположим теперь, что в индексах элементов системы $\mathcal{H}^*$ каждый из них повтаряется по крайнер мере семь раз. Это возможно лишь тогда если сумма числа индексов равна по крайнер мере 35. Так как индекс главного характера равен нулю вышеупомянутая ситуация возможна лишь если в $\mathcal{H}^*$ кроме X_1, X_2, X_3, X_4, X_5 одноиндексных характеров:

Число различных индексов элементов	Число характеров в $\mathcal{H}^*$ исключая одноиндексные		
5	1	1	1
4	5	5	4
3	2	1	3
2	-	1	-
0	-	-	-

В каждом из трёх случаев X_{1234} принадлежит $\mathcal{H}^*$ и X_{15} не принадлежит $\mathcal{H}^*$.

Выполняя трансформацию $X_1 \to X_{1234}$, $X_i \to X_i$ $(i = 2,3,4,5)$ на $\mathcal{H}^*$ (и соответственно на G) получим что $\mathcal{H}^*$ не содержит X_{1235} и поэтому сумма числа индексов (учитывая и одноиндексные) элементов не достигает 30-ти.

Таким образом можем предположить что существует такой индекс, который в $\mathcal{H}^*$ повторяется по крайнер мере 5 раз, но не более

6-ти раз. Пусть $\mathcal{H}^1$ -множество состоящее из таких $X \in \mathcal{H}^*$ в индексе которых присутствует 1. В теореме 1 мы уже видели, что для множества состоящего из X' для которого $X_1 X' \in \mathcal{H}^1$ реализуема любая $G^1 = (a_2) X \ldots X (a_5)$ группа четвёртого порядка и поэтому по лемме 1 группа характеров G^1 содержит один из её базисов.

Подобным образом переиндексированием элементов G и соответственно элементов $\mathcal{H}$ получим

$$\{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^1$$

Так как 5 характеров содержащих 1-й индекс нами даны, то осталось найти восемь или семь характеров не содержащих 1-ого индекса, в зависимости от того, что число характеров содержащих 1 было 5 или 6. Т.о. в нашей программе нужно проверить лишь $C_{16}^8 + 11 \cdot C_{16}^7 = 138710$ число комбинаций для нахождения реализуемой системы из 13 элементов.

Подобные, ускоряющие поиск предположения могут быть приняты и для случая $n > 5$, при условии принадлежности множеств вида $\mathcal{H}^{1'}$ реализуемой системе.

Лемма 3: Пусть $N = 5$ и $\mathcal{H}^*$ - 24 элементная 3-реализуемая система, тогда при помощи трансформации базиса можем достигнуть что $\mathcal{H}^{1'} = \{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^*$ и $\mathcal{H}$ содержит 6 или 7 элементов с индексом 1 не принадлежащих $\mathcal{H}^{1'}$.

Доказательство: Следуя ходу доказательства леммы 1 и используя $p(4,2) = 10$, получим что в реализуемой системе каждый из индексов повторяется 10-ть раз. По доказанным в [1] $p(5,3) \leqslant 25$. Если $p(5,3) = 24$, то так как достижимо что

все характеры с одним индексом содертатся в реализуемом $\mathcal{H}^*$, то максимальная сумма индексов достижима в случае если $\mathcal{H}^*$ содержит

5	шт.	1	индексных характеров
1	шт.	5	"
5	шт.	4	"
10	шт.	3	"
3	шт.	2	"

Т.о. в общей сложности 24 характера имеют максимально 66 индексов и поэтому существует такой индекс который встречается 13 раз. Если система не содержит характера с 5-ю или 4-мя индексами, то элементы этой системы содержат самое больше 64 индекса, и т.о. существует индекс который встречается 12 раз. Если все характеры с 5-ю и 4-мя индексами находятся в $\mathcal{H}^*$, то может быть предположено, что существует такой 2-х индексный характер, каторый не принадлежит системе, ибо в противном случае максимальная сумма индексов составляла бы 59, что противоречиво. Пусть т.о. $X_{12} \in \mathcal{H}^*$, тогда выполняя трансформацию $X_1 \longrightarrow X_{1345}$, $X_i \longrightarrow X_i$ $(i = 2,3,4,5)$ получим систему в которой нет характера с пятью индексами. На основании вышесказанного, можем предположить, что существует такой индекс, который по крайнер мере 10 раз и по меньшей мере 12 раз повторяется.

Следуя обозначениям и ходу рассуждений леммы 2 получим $\{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^1$, $10 \leqslant |\mathcal{H}^1| \leqslant 12$.

Если каждый индекс повторяется точно 10-раз, то либо 0,0,9,9 ,5,1 соответственно 0,1,7,10,5,1 характеры, соответ-

ственно, с числом индексов 5,4,3,2,1,0 содержатся в $\mathcal{H}^*$. В первом случае можно предположить что $X_{123} \notin \mathcal{H}^*$, и на подгруппе (a_1,a_2,a_3), а во втором случае X_{123} и $X_{124} \notin \mathcal{H}^*$ и на подгруппе (a_1,a_2,a_3,a_4) не может быть получен ограничением системы $\mathcal{H}^*$ характер $(-1,-1,-1)$. Лемма доказана.

2.

В программе принимаются следующие обозначения:

- Переменные которые не декларируются явно имеют тип соответствующий неявной декларации.
- N обозначается число элементов базиса группы G, а K число элементов базиса рассматриваемых подгрупп.
- Характеры и элементы группы представляются как строки битов длинной N (расположенных в переменных с декларацией FIXED BINARY), так что последние N-битов определяют значения характеров на элементах базиса группы $a_1,\ldots,a_N$ следующим образом: значение бита равно 1, если значение характера -1 и ∅ в противном случае.

В массиве KA состоящем из $KO=2^N$ - элементов первые $KH=2^N - N$ - элементы содержат характеры которые не были нами ещё выбраны, т.е. не принадлежат $\mathcal{H}^1$. Заполнение этого массива выполняет:

```
KA(1)=0;
DO I=2 TO KO;
  KA(I)=I-1;
END;
DO I=1 TO KO;
  C1:IF KA(I)=2**(N-1) THEN GOTO C2;
  DO L=1 TO N-1;
```

```
      IF KA(I)=2**(L-1)+2**(N-1) THEN GOTO C2;
    END;
    GOTO C3;
    C2:DO J1=I+1 TO KO;
         KA(J1-1)=KA(J1);
       END;
    GOTO C1;
  C3:END;
```

b)

Располагая в массиве NC элементы группы отличные от единичного, можем определить значение характеров на этих елементах. Значение принимаемые характерами однозначно определяется чётностью суммы общих единиц характеров и элементов группы. Характер принимает значение 1 на элементе группы если сумма чётна и-1 противном случае.

B - двухмерный (KO-1) x (KO-1) массив и B1, B2 - переменные с общим типом BIT(1).

```
    DO I=1 TO KO-1;
      NC(I)=I;
    END;
    DO I=1 TO KO-1;
      DO L=1 TO KH;
        B1='0'B;
        N1=NC(I)&KA(L);
        DO J1=1 TO N;
          IF MOD(N1,2)=1 THEN B3='1'B;
```

```
                ELSE B3='0'B;
        B1=(B1&¬B3)|(¬B1&B3);
        N1=N1/2;
      END;
    B(I,L)=B1;
    END;
  END;
```

c)

Далее, определяясь от элементов K1=1 и K2=2 перечислим в лексиграфическом порядке все пары элементов группы, и для предупреждения совпадения порожденных или подгруппе, рассмотрим лищ те пары у которых компонента наименьшего индекса, т.е. бинарно единица с наибольшим позиционным весом, общая. Легко проверить что таким образом могут быть получены (и лищ единожды) все группы четвёртого порядка числа $C^2_{ко-1} : C^2_3$.

Каждой подгруппе H будут сопоставлены наибольшее 4 строки имеющей KH столбцов матрицы B2 типа BIT (1) следующим образом: если некоторый характер H не может быть задан ограничениями элементов включенных в систему характеров $\mathcal{H}^{1)}$ на H, тогда дополним B2 следующей J-той строкой характеризующей подгруппу и характер исследуемой подгруппы так, что B2(J,L)= = '1'B, если L-тый характер из $\mathcal{H}$ редуцируемый к H, даст исследуемый характер H, в противном случае B2(J,L) = '0'B.

```
K1=1;K2=2;J=1;
C4:DO L=N TO 1 BY -1;
     IF K2>=2**L THEN DO; LL=L;GOTO Q1; END;
   END;
GOTO C5;
Q1:IF K1<2**LL THEN GOTO C5;
```

```
      IF K1<2**(N-1) THEN GOTO Q3;
      IF (K1&K2-2**(N-1))¬=0 THEN GOTO Q2;
    DO J1=1 TO KH;
      IF B(K1,J1)¬='0'B|B(K2,J1)¬='0'B THEN B2(J,J1)='0'B;
    END;
    J=J+1;
    Q2:IF (K1&¬K2)¬=0 THEN GOTO C5;
    DO J1=1 TO KH;
      IF B(K1,J1)¬='0'B|B(K2,J1)¬='1'B THEN B2(J,J1)='0'B;
    END;
    J=J+1;
    Q3:IF (K1&¬K2)¬=0 THEN GOTO C5;
    DO J1=1 TO KH;
      IF B(K1,J1)¬='1'B|B(K2,J1)¬='0'B THEN B2(J,J1)='0'B;
    END;
    J=J+1;
    C5:IF K2<KO-1 THEN DO;K2=K2+1;GOTO C4;END;
       IF K1<KO-2 THEN DO;K1=K1+1;K2=K1+1;GOTO C4;END;
```

d)

В целях экономии помяти и ускорочения времени вычислений каждые 31 строки B2 помести в одну строку массива M-типа FIXED BINARY (31):

```
    J=J-1;
    V8:M1=J/31*31+31;
    J2=M1/31;
    DO I=1 TO J2;
      DO L=1 TO KH;
        DO L1=1 TO 31;
          M(I,L)=B2((I-1)*31+L1,L)+M(I,L)*2;
        END;
```

```
    END;
END;
```

Последние, ранее не получившие значений, M1-J элэменты массива M содержат '1'B и т.о. размер M не влияет на дальнейшие вычисления.

е)

Из числа характеров не содержащих 1-го индекса, исходя из 2 и 3 леммы, можно выбрать и добавить определённое каличество к N элементному $\mathcal{H}^{1)}$.

Предположим, что в реализуемой системе содержащей КК-элементов содержится L1-L2 характеров без индекса 1. Нужно проверить, что добавляя к $\mathcal{H}^{1)}$.

КА(1),...,КА(КJ) где КJ=КК-N получим ли полную систему характеров, ограничая вышеупомнутую на произвольные подгруппы порядка $2^{к}$, т.е найдём ли 1 в каждой строке при подходящем выборе КJ столбцов матрицы B2. Проверку произведём т.о, что беря дизъюнкцию выбранных столбцов, посмотрим, что из строк M получим ли строку битов представляющую значение $2^{31}-1$.

Так как выбор множества характеров производился в лексикографическом порядке, множество состоящее из первых L1 характеров изменяется лишь тогда, когда следующие после них элементы пробежали по всем выбираемым и содержащим индекс 1 характерам. Целесообразно, т.о., столбцы M разделять на две части, отдельно проверяя ко/2 столбцов относящихся к характерам без индекса 1.

Элемент MS(I ,1) может быть получен дизъюнкцией элементов лежащих на пересечении выбранных по характерам L1 столбцов с I-той строкой матрицы M. MS(I ,2) получаем по-

добной дизъюнкцией с участием KJ-L1 столбцов.

```
M5=2**31-1;
DO L1=L1 TO L2 BY -1;
  DO L=1 TO L1;
    IN(L)=L;
  END;
  Z1;DO L=L1+1 TO KJ;
    IN(L)=KO/2+L-L1;
    END;
  Z2;DO I=1 TO J2;
       MS(I,1)=0;
       DO J1=1 TO L1;
         MS(I,1)=MS(I,1)!M(I,IN(J1));
       END;
     END;
  Z3;DO I=1 TO J2;
       IF MS(I,1)=K5 THEN GOTO Z7;
       MS(I,2)=0;
       DO J1=L1+1 TO KJ;
         MS(I,2)=MS(I,2)!M(I,IN(J1));
       END;
       IF (MS(I,1)!MS(I,2))=M5 THEN GOTO Z7;
       DO L=KJ TO L1+1 BY -1;
         IF IN(L)<L+KH-KJ THEN GOTO Z4;
```

```
            END;
            GOTO Z5;
            Z4:IN(L)=IN(L)+1;
            DO L=L+1 TO KJ;
              IN(L)=IN(L-1)+1;
            END;
            GOTO Z3;
            Z5:DO L=L1 TO 1 BY -1;
                 IF IN(L)<KO/2+L-L1 THEN GOTO Z6;
               END;

            GOTO Z8;
            Z6:IN(L)=IN(L)+1;
            DO L=L+1 TO L1;
              IN(L)=IN(L-1)+1;
            END;
            GOTO Z1;
          Z7:END;
          PUT SKIP EDIT('REALIZALODO RENDSZERT ALKOT AZ ELORE KIVALASZ
          TOTTAKKAL EGYUTT',(KA(IN(L))DO L=1 TO KJ))(A,SKIP,25F(8));
          GOTO Z9;
        Z8:END;
        PUT SKIP EDIT ('MINDEN',KK,'-SZAMU KARAKTERHALMAZHOZ VAN
        ASSZOCIALT ALCSOPORT')(A,F(8),A);
Z9:END;
```

f)

Подобно c) и для случая K=3 мы сможем перечислить образующие элементы всех различных подгрупп порядка 8, так, что представляем их в виде строк битов, для которых компонент с наибольшим индексом общий. Т.к. в каждой такой подгруппе есть четыре элемента с таким свойством (и очевидно любой из них может быть получен произведением оставшихся 3-х) то две различные тройки чисел не будут генерировать одну и ту же группу.

Матрица B2 определяется аналогиено случаю K=2, здесь нужно иследовать 8 характеров для каждой подгруппы.

```
DO I=1 TO 4;
  K(I)=I;
END;
J=1;
C4:DO L=N TO 1 BY -1;
     IF K(4)>=2**L THEN DO; LL=L;GOTO Q1;END;
   END;
GOTO C5;
Q1:IF K(3)<2**LL!K(2)<2**LL THEN GOTO C5;
   IF ((K(4)&¬K(3)!¬K(4)&K(3))&¬K(2)!¬(K(4)&¬K(3)!
   ¬K(4)&K(3))&K(2))¬=K(1) THEN GOTO C5;
                    .
                    .
                    .
```

```
C5:DO L=4 TO 1 BY -1;
     IF K(L)<KO+L-4 THEN GOTO C6;
   END;
GOTO V8;
C6:K(L)=K(L)+1;
   DO L=L+1 TO 4;
     K(L)=K(L-1)+1;
   END;
GOTO C4;
M6=K(1)&K(2)-2**LL;
M7=K(2)&K(3)-2**LL;
M8=K(1)&K(3)-2**LL;
IF LL=4!(K(1)&K(2)&K(3)-16)¬=0 THEN GOTO V1;
DO J1=1 TO KH;
   IF B(K(1),J1)='0'B&B(K(2),J1)='0'B&B(K(3),J1)='0'B
                                   THEN B2(J,J1)='1'B;
END; J=J+1;
```

Результаты прогона программы:

N	K	l(n,K)	время/мин
4	2	9	5
5	2	13	50
5	3	24	450

Программа может применяться и в случае $N > 5$, но это ведёт к большим затратам в машинном времени и для $K=2,3$ Производя небольшие изменения можно определить и реализуемость системы характеров.

Литература

[1] К. Бузаши-А. Пете-П. Лакатош, О кодовых расстояниях одного класса групповых кодов. Проблемы передачи информаций (под редакции)

[2] С.Д. Берман, Полупростые циклические коды. Кибернетика N° 2-3(1967) 21-30.

[3] С.Д. Берман-А.Б. Юданина, Коды с обобщённым мажаритарным декодированием и свёрточные коды. Продлемы передачи информаций т.6. (1970) 6-19.

Összefoglaló

Ábel kódok egy osztályának vizsgálata számológép segitségével

Lakatos P., Pető A.

A másodrendű ciklikus csoportok véges direkt szorzatából képzett csoportalgebra ideáljai az Ábel féle kódok fontos osztályát alkotják. Ebben a cikkben leirunk egy PL/1 nyelvű algoritmust, amellyel a csoport bizonyos tulajdonságú karakterrendszereit lehet meghatározni. Ezek alkalmazhatók adott súlyú kódszavak meghatározásához.

Summary

Investigation of a class of Abelian codes using computer algorithm

The ideals of the group algebra, which is built on the finite direct product of second order cyclic groups, is an important class of Abelian codes. In this paper we describe a computer algorithm on PL/1 that determines character systems with certain properties of the group. One can use it in determining code words with given weight.