Автоматика и телемеханика, № 7, 2005

© 2005 г. О. А. ФИНЬКО, канд. техн. наук
(Краснодар)

МОДУЛЯРНЫЕ ФОРМЫ СИСТЕМ k-ЗНАЧНЫХ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ

Исследованы методы реализации k-значных функций алгебры логики посредством модулярных форм арифметических полиномов, построенных на основе принципа “взвешивания” числами k^i ($i = 0, 1, 2 \ldots$). Рассмотрены модулярные полиномиальные и матричные (теоретико-числовые) преобразования, которые затем обобщены на случай реализации систем k-значных функций. Предложен новый принцип синтеза модулярной формы одного арифметического полинома для реализации систем k-значных функций на основе Китайской теоремы об остатках. Полученные результаты обеспечивают преимущества по сложности аналитического описания и реализации k-значных функций.

1. Введение

Обработка k-значных функций алгебры логики (ФАЛ) имеет многочисленные приложения в системах управления сложными техническими объектами, системах автоматизированного проектирования (синтез и анализ дискретных устройств) интегральных схем и др. [1].

Эффективность *реализации* ФАЛ существенно определяется выбором способа аналитического описания ФАЛ. Так, ряд важных преимуществ, в частности по введению различных форм *параллелизма* логических вычислений при реализации ФАЛ средствами серийной вычислительной техники общего назначения и малогабаритными специализированными процессорами, позволяют получить методы описания ФАЛ арифметическими полиномами [2–6].

Эти преимущества стимулировали дальнейшее развитие арифметических форм представления и реализации ФАЛ, в частности на основе привлечения теоретико-числовых методов цифровой обработки сигналов. Так, в [7, 8] введены модулярные формы арифметического описания и реализации систем булевых функций, которые позволили, с одной стороны, уменьшить сложность полиномиального описания систем булевых функций, а с другой – получить новые формы параллелизма логических вычислений.

В этой работе предлагается: 1) обобщение применения методов модулярной арифметики на область k-значных ФАЛ; 2) исследование реализации системы k-значных функций в форме одного арифметического полинома, построенного на основе Китайской теоремы об остатках.

2. Реализация одной логической функции одним арифметическим полиномом

2.1. Полиномиальная арифметика k-значной логики

Под многозначной ФАЛ $f(X)$ от n переменных $X = x_1, x_2, \ldots, x_n$ будем понимать логическую функцию, заданную на множестве $\{0, 1, \ldots, k-1\}$, значения аргументов которой принадлежат этому же множеству, где k – значность ФАЛ.

$$\overbrace{X = x_1, x_2, \ldots, x_n}^{k\text{-значные переменные}} \qquad \overbrace{f(X)}^{k\text{-значная ФАЛ}}$$

$$\Downarrow \qquad\qquad \Downarrow$$

$$\overbrace{P(X) = \sum_{i=0}^{k^n-1} p_i x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}}^{\text{Арифметический полином}}$$

$$\Downarrow$$

Вычисление над $\mathbb{Q}$

$$\Downarrow$$

$$\overbrace{y = f(X)}^{\text{Значение ФАЛ}}$$

Рис. 1. Схема вычисления *произвольной* k-значной ФАЛ над $\mathbb{Q}$.

$$\overbrace{X = x_1, x_2, \ldots, x_n}^{k\text{-значные переменные}} \qquad \overbrace{p_0, p_1, \ldots, p_{k^n-1}}^{\text{Коэффициенты}}$$

$$\Downarrow \qquad\qquad \Downarrow$$

Вычисление арифметического полинома $P(X)$ *над* $\mathbb{Q}$

$$\Downarrow$$

$$\overbrace{y = f(X)}^{\text{Значение ФАЛ}}$$

Рис. 2. Схема вычисления *заданной* k-значной ФАЛ над $\mathbb{Q}$.

Известно, что любую многозначную ФАЛ можно представить в виде арифметического полинома [4]:

$$Y = P(X) = \sum_{i=0}^{k^n-1} p_i \, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}, \tag{1}$$

где Y – числовое значение, принимаемое полиномом $P(X)$; p_i – коэффициенты такие, что $p_i \in \mathbb{Q}$ ($\mathbb{Q}$ – множество рациональных чисел); $X = x_1, x_2, \ldots, x_n$ – аргументы ФАЛ, $x_u \in \{0, 1, \ldots, k-1\}$ $(u = 1, 2, \ldots, n)$; $(i_1 \, i_2 \, \ldots \, i_n)_k$ – представление параметра i в k-ичной системе счисления:

$$(i_1 \, i_2 \, \ldots \, i_n)_k = \sum_{u=1}^{n} i_u k^{n-u} \quad (i_u \in \{0, 1, \ldots, k-1\}); \quad x_u^{i_u} = \begin{cases} x_u^{i_u}, \ i_u \neq 0, \\ 1, \ i_u = 0. \end{cases}$$

Можно построить две схемы вычисления ФАЛ посредством арифметических полиномов (рис. 1 и 2). Вычисления выполняются над $\mathbb{Q}$ (в отличие от вычислений в кольце целых чисел при реализации булевых функций [9]).

Таблица 1

k	$\mathbf{K}_k$	$\mathbf{K}_k^{-1}$
2	$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
3	$\begin{bmatrix} 2 & 0 & 0 \\ -3 & 4 & -1 \\ 1 & -2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$
4	$\begin{bmatrix} 6 & 0 & 0 & 0 \\ -11 & 18 & -9 & 2 \\ 6 & -15 & 12 & -3 \\ -1 & 3 & -3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \end{bmatrix}$
5	$\begin{bmatrix} 24 & 0 & 0 & 0 & 0 \\ -50 & 96 & -72 & 32 & -6 \\ 35 & -104 & 114 & -56 & 11 \\ -10 & 36 & -48 & 28 & -6 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 16 & 64 & 256 \end{bmatrix}$
6	$\begin{bmatrix} 120 & 0 & 0 & 0 & 0 & 0 \\ -274 & 660 & -600 & 400 & -150 & 24 \\ 225 & -770 & 1070 & -780 & 305 & -20 \\ -85 & 355 & -590 & 490 & -205 & 35 \\ 15 & -70 & 130 & -120 & 55 & -10 \\ -1 & 5 & -10 & 10 & -5 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 \\ 1 & 3 & 9 & 27 & 81 & 243 \\ 1 & 4 & 16 & 64 & 256 & 1024 \\ 1 & 5 & 25 & 125 & 625 & 3125 \end{bmatrix}$

Аналогично двоичной логике в k-ичной логике могут быть определены алгебраический и матричный методы построения арифметического полинома (1) [4].

Прямое и обратное матричные преобразования или логическое дискретное преобразование Фурье [10] (ЛДПФ – в дальнейшем k-ЛДПФ) определяются соответственно выражениями

$$\mathbf{P} = N_{k,n}^{-1}\mathbf{K}_{k^n}\mathbf{Y}, \tag{2}$$

$$\mathbf{Y} = \mathbf{K}_{k^n}^{-1}\mathbf{P}, \tag{3}$$

где $\mathbf{K}_{k^n}$ и $\mathbf{K}_{k^n}^{-1}$ – соответственно матрицы прямого и инверсного арифметического преобразования размерности $k^n \times k^n$ (базис преобразования); $\mathbf{Y}$ – вектор истинности k-значной ФАЛ; $N_{k,n}$ – нормализующий множитель;

$$\mathbf{Y} = \left[\; Y^{(0)} \quad Y^{(1)} \quad \ldots \quad Y^{(k^n-1)} \;\right]^{\mathrm{T}},$$

где $Y^{(i)}$ – числовое значение, принимаемое k-значной ФАЛ на i-м наборе переменных (Т – символ транспонирования матрицы), вектор коэффициентов (спектр) арифметического полинома (1):

$$\mathbf{P} = [\; p_0 \quad p_1 \quad \ldots \quad p_{k^n-1} \;].$$

Матрицы $\mathbf{K}_{k^n}$ и $\mathbf{K}_{k^n}^{-1}$, как и базис преобразования двоичной логики, определяется кронекеровским возведением в степень:

$$\mathbf{K}_{k^n} = \bigotimes_{j=1}^{n}\mathbf{K}_k; \quad \mathbf{K}_{k^n}^{-1} = \bigotimes_{j=1}^{n}\mathbf{K}_k^{-1},$$

где $\mathbf{K}_k$ и $\mathbf{K}_k^{-1}$ – базовые матрицы прямого и обратного преобразования такие, что (i,j)-й элемент $\mathbf{K}_k^{-1}$ равен i^j $(i,\, j = 0,\, 1, \ldots, k-1)$ и $\mathbf{K}_k\mathbf{K}_k^{-1} = \mathbf{I}_k$ (см. табл. 1 – для $k = 2 \ldots 6$).

Пример 1. Пусть $k = 3$ и вектор принимаемых значений ФАЛ при $n = 2$ имеет вид: $\mathbf{Y} = [\ 2\ \ 0\ \ 2\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 2\ ]^{\mathrm{T}}$. Тогда прямое преобразование (2) примет вид:

$$\mathbf{P} = \frac{1}{4}\mathbf{K}_{3^2}\mathbf{Y} =$$

$$= \frac{1}{4}\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 8 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 0 & 0 & 8 & 0 & 0 & -2 & 0 & 0 \\ 9 & -12 & 3 & -12 & 16 & -4 & 3 & -4 & 1 \\ -3 & 6 & -3 & 4 & -8 & 4 & -1 & 2 & -1 \\ 2 & 0 & 0 & -4 & 0 & 0 & 2 & 0 & 0 \\ -3 & 4 & -1 & 6 & -8 & 2 & -3 & 4 & -1 \\ 1 & -2 & 1 & -2 & 4 & -2 & 1 & -2 & 1 \end{bmatrix}\begin{bmatrix} 2 \\ 0 \\ 2 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 2 \end{bmatrix} = \frac{1}{4}\begin{array}{c} \begin{bmatrix} 8 \\ -16 \\ 8 \\ -4 \\ 22 \\ -12 \\ 0 \\ -6 \\ 4 \end{bmatrix} \end{array}\begin{array}{l} \\ x_2 \\ x_2^2 \\ x_1 \\ x_1x_2 \\ x_1x_2^2 \\ x_1^2 \\ x_1^2x_2 \\ x_1^2x_2^2 \end{array}.$$

Таким образом на основании (1) алгебраическая форма будет иметь вид:

$$P(X) = \frac{1}{4}\left(8 - 16x_2 + 8x_2^2 - 4x_1 + 22x_1x_2 - 12x_1x_2^2 + 0x_1^2 - 6x_1^2x_2 + 4x_1^2x_2^2\right) =$$
$$= 2 - 4x_2 + 2x_2^2 - x_1 + \frac{11}{2}x_1x_2 - 3x_1x_2^2 - \frac{3}{2}x_1^2x_2 + x_1^2x_2^2.$$

Например, пусть $x_1 = 1$, $x_2 = 2$, тогда значение ФАЛ определится как:

$$P(X) = \frac{1}{4}\left(8 - 16\cdot 2 + 8\cdot 2^2 - 4\cdot 1 + 22\cdot 1\cdot 2 - 12\cdot 1\cdot 2^2 - 6\cdot 1^2\cdot 2 + 4\cdot 1^2\cdot 2^2\right) =$$
$$= \frac{1}{4}4 = 1.$$

Обратное преобразование (3) будет иметь вид:

$$\mathbf{Y} = \mathbf{K}_{3^2}^{-1}\mathbf{P} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 0 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 4 & 4 & 4 \\ 1 & 2 & 4 & 2 & 4 & 8 & 4 & 8 & 16 \end{bmatrix}\begin{bmatrix} 2 \\ -4 \\ 2 \\ -1 \\ \frac{11}{2} \\ -3 \\ 0 \\ -\frac{3}{2} \\ 1 \end{bmatrix}\begin{array}{l} \\ x_2 \\ x_2^2 \\ x_1 \\ x_1x_2 \\ x_1x_2^2 \\ x_1^2 \\ x_1^2x_2 \\ x_1^2x_2^2 \end{array} = \begin{bmatrix} 2 \\ 0 \\ 2 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}.$$

Недостатком представления (1) является возможность принятия коэффициентами p_i ($i = 0, 1, \ldots, k^n - 1$) как неотрицательных, так и отрицательных значений. Это требует удваивания числового диапазона по сравнению с использованием неотрицательных коэффициентов. При этом абсолютные значения коэффициентов и промежуточных результатов вычисления (1) могут многократно превышать значение k.

Известно представление многозначной ФАЛ с помощью логического полинома [4]:

$$(4) \qquad Y = F(X) = \left|\sum_{i=0}^{k^n-1} f_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_k,$$

где f_i – коэффициенты, такие что $f_i \in \{0, 1, \ldots, k-1\}$; $|*|_k$ – наименьший неотрицательный вычет от $*$ по модулю k; $x_u^{i_u} = \begin{cases} x_u^{i_u}, & i_u \neq 0, \\ 1, & i_u = 0. \end{cases}$

Логический полином (4) является частным случаем *модулярной* формы *арифметического* полинома, так как реализация (4) выполняется в арифметике простого поля $\mathbb{F}_k$. Понятие модулярной формы может быть обобщено и для других значений модулей, отличных от k, *расширяющих* выбор технических средств обработки. Например известно, что определенные преимущества при технической реализации арифметики простого поля $\mathbb{F}_m$ имеют значения модуля m, являющиеся, например, числами Мерсенна, Ферма и др. [11].

2.2. Модулярные формы k-значной логики

Предложение 1. *Пусть $m \geq k$, где k – значность логики и m простое, тогда произвольная ФАЛ может быть представлена арифметическим полиномом* [12]*:*

$$Y = \mu(X) = \left| \sum_{i=0}^{k^n-1} \rho_i \, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m , \tag{5}$$

где $\rho_i \in \mathbb{Z}_m$; $x_u \in \mathbb{Z}_k$; $x_u^{i_u} = \begin{cases} x_u^{i_u}, \ i_u \neq 0, \\ 1, \ i_u = 0. \end{cases}$

Доказательство предложения 1, определяющее связь с формой (1), приведено в Приложении и следует из возможности представления функции в форме полинома над простым полем $\mathbb{F}_m$.

Замечание 1. Связь арифметических полиномов (1) и (5) устанавливается отношением $\rho_i = |p_i|_m$.

Определение 1. Выражение (5) *будем называть модулярной арифметической формой представления k-значной ФАЛ.*

Примитивная процедура (рис. 3) получения (5) состоит из двух шагов: 1) вычисление арифметического полинома (1) и 2) определение арифметического полинома (5) на основании замечания 1. Основные схемы вычисления k-значной ФАЛ посредством модулярной формы (5) представлены на рис. 4 и 5, из которых следует, что вычисления из арифметики поля рациональных чисел $\mathbb{Q}$ перенесены в простое поле $\mathbb{F}_m$. Кроме того, справедливо следующее свойство.

Свойство 1. Если для одной и той же системы k-значной ФАЛ заданы два арифметических полинома $P(X)$ (1) *и $\mu(X)$* (5)*, а K_1 и K_2 – соответственно количество членов этих полиномов, то $K_2 \leq K_1$.*

Данное свойство можно пояснить на следующих примерах.

Пример 2. Выберем значения $k = 2, 3, 4$ и $n = 2$. Определим модуль $m = 5$, величина которого удовлетворяет всем выбранным значениям k (т.е. $m \geq k$). Используем полиномы (1) и (5) для представления следующих элементарных ФАЛ:

$\overline{x} = (k-1) - x$ – инверсия;

Шаг 1	p_0	p_1	$\dots$	p_{k^n-1}
	$\Downarrow$	$\Downarrow$		$\Downarrow$
Шаг 2	$\rho_0 = \lvert p_0 \rvert_m$	$\rho_1 = \lvert p_1 \rvert_m$	$\dots$	$\rho_{k^n-1} = \lvert p_{k^n-1} \rvert_m$

Рис. 3. Пояснения к варианту построения алгоритма получения (5) на основании замечания 1.

$$\overbrace{X = x_1, x_2, \ldots, x_n}^{k\text{-значные переменные}} \qquad\qquad \overbrace{f(X)}^{k\text{-значная ФАЛ}}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\overbrace{\mu(X) = \left| \sum_{i=0}^{k^n-1} \rho_i x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m}^{\text{Модулярная форма арифметического полинома}}$$

$$\Downarrow$$

Вычисление над $\mathbb{F}_m$

$$\Downarrow$$

$$\overbrace{y = f(X)}^{\text{Значение ФАЛ}}$$

Рис. 4. Схема вычисления *произвольной* k-значной ФАЛ над $\mathbb{F}_m$.

$$\overbrace{X = x_1, x_2, \ldots, x_n}^{k\text{-значные переменные}} \qquad\qquad \overbrace{\rho_0, \rho_1, \ldots, \rho_{k^n-1}}^{\text{Коэффициенты}}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

Вычисление арифметического полинома $\mu(X)$ *над* $\mathbb{F}_m$

$$\Downarrow$$

$$\overbrace{y = f(X)}^{\text{Значение ФАЛ}}$$

Рис. 5. Схема вычисления *заданной* k-значной ФАЛ над $\mathbb{F}_m$.

$\widehat{x} = |x+1|_k$ – циклическое отрицание ($\overline{x} = x \oplus 1$ при $k = 2$);

$x_1 \vee x_2 = \max(x_1,\, x_2)$ – дизъюнкция;

$x_1 \wedge x_2 = \min(x_1,\, x_2)$ – конъюнкция;

$|x_1 + x_2|_k$ – сложение по модулю k ($x_1 \oplus x_2$ при $k = 2$);

$|x_1 x_2|_k$ – умножение по модулю k ($x_1 \wedge x_2$ при $k = 2$);

$x_1 \uparrow x_2 = |(x_1 \vee x_2) + 1|_k$ – функция Вебба ($\overline{x_1 \vee x_2} = (x_1 \vee x_2) \oplus 1$ – "стрелка Пирса" при $k = 2$);

$x_1 \downarrow x_2 = \overline{x_1 \wedge x_2}$ – "штрих Шеффера" при $k = 2$.

Результаты использования (1) и (5) для $k = 2,\, 3,\, 4$ представлены соответственно в табл. 2–4.

Для пояснения принципа преобразования представления ФАЛ из (1) в (5) рассмотрим следующий пример.

Таблица 2

$f(X)$	$P(X)$	$\mu(X)$ при $m=5$
$\overline{x}_i$	$1-x_i$	$\lvert 1+4x_i\rvert_5$
$x_1 \wedge x_2$	x_1x_2	$\lvert x_1x_2\rvert_5$
$x_1 \vee x_2$	$x_1+x_2-x_1x_2$	$\lvert x_1+x_2+4x_1x_2\rvert_5$
$x_1 \oplus x_2$	$x_1+x_2-2x_1x_2$	$\lvert x_1+x_2+3x_1x_2\rvert_5$
$x_1 \downarrow x_2$	$1-x_1x_2$	$\lvert 1+4x_1x_2\rvert_5$
$x_1 \uparrow x_2$	$1-x_1-x_2+x_1x_2$	$\lvert 1+4x_1+4x_2+x_1x_2\rvert_5$

Таблица 3

$f(X)$	$P(X)$	$\mu(X)$ при $m=5$
$\overline{x}_i$	$2-x_i$	$\lvert 2+4x_i\rvert_5$
$\widehat{x}_i$	$1+5x_i/2-3x_i^2/2$	$\lvert 1+x_i^2\rvert_5$
$x_1 \wedge x_2$	$5x_1x_2/2-x_1x_2^2-x_1^2x_2+x_1^2x_2^2/2$	$\lvert 4x_1x_2^2+4x_1^2x_2+3x_1^2x_2^2\rvert_5$
$\lvert x_1+x_2\rvert_3$	$x_1+x_2+21x_1x_2/4-15x_1x_2^2/4-$ $-15x_1^2x_2/4+9x_1^2x_2^2/4$	$\lvert x_1+x_2+4x_1x_2+x_1^2x_2^2\rvert_5$
$\lvert x_1x_2\rvert_3$	$x_1x_2/4+3x_1x_2^2/4+$ $+3x_1^2x_2/4-3x_1^2x_2^2/4$	$\lvert 4x_1x_2+2x_1x_2^2+$ $+2x_1^2x_2+3x_1^2x_2^2\rvert_5$
$x_1 \uparrow x_2$	$1+5x_2/2-3x_2^2/2+5x_1/2-$ $-7x_1x_2/4+x_1x_2^2/4-3x_1^2/2+$ $+x_1^2x_2/4+x_1^2x_2^2/4$	$\lvert 1+x_2^2+2x_1x_2+4x_1x_2^2+$ $+x_1^2+4x_1^2x_2+4x_1^2x_2^2\rvert_5$

Таблица 4

$f(X)$	$P(X)$	$\mu(X)$ при $m=5$
$\overline{x}_i$	$3-x_i$	$\lvert 3+4x_i\rvert_5$
$\widehat{x}_i$	$1-x_i/3+2x_i^2-2x_i^3/3$	$\lvert 1+3x_i+2x_i^2+x_i^3\rvert_5$
$x_1 \wedge x_2$	$29x_1x_2/6-15x_1x_2^2/4-$ $-15x_1^2x_2/4+3x_1x_2^3/4+$ $+3x_1^3x_2/4+7x_1^2x_2^2/2-$ $-3x_1^2x_2^3/4-3x_1^3x_2^2/4+x_1^3x_2^3/6$	$\lvert 4x_1x_2+2x_1x_2^3+$ $+2x_1^3x_2+x_1^2x_2^2+$ $+3x_1^2x_2^3+3x_1^3x_2^2+x_1^3x_2^3\rvert_5$
$\lvert x_1+x_2\rvert_4$	$x_1+x_2-121x_1x_2/9+$ $+49x_1x_2^2/3+49x_1^2x_2/3-$ $-38x_1^3x_2/9-38x_1x_2^3/9-$ $-19x_1^2x_2^2+14x_1^2x_2^3/3+$ $+14x_1^3x_2^2/3-10x_1^3x_2^3/9$	$\lvert x_1+x_2+x_1x_2+3x_1x_2^2+$ $+3x_1^2x_2+3x_1^3x_2+3x_1x_2^3+$ $+x_1^2x_2^2+3x_1^2x_2^3+3x_1^3x_2^2\rvert_5$
$x_1 \uparrow x_2$	$1-x_2/3+2x_2^2-2x_2^3/3-$ $-x_1/3-79x_1x_2/18+$ $+37x_1x_2^2/12-19x_1x_2^3/36+$ $+2x_1^2+37x_1^2x_2/12-$ $-15x_1^2x_2^2/6+5x_1^2x_2^3/12-$ $-2x_1^3/3-19x_1^3x_2/36+$ $+5x_1^3x_2^2/12-x_1^3x_2^3/18$	$\lvert 1+3x_2+2x_2^2+x_2^3+$ $+3x_1+2x_1x_2+x_1x_2^2+$ $+x_1x_2^3+2x_1^2+x_1^2x_2+$ $+x_1^3+x_1^3x_2+3x_1^3x_1^3\rvert_5$

Пример 3. При $k=3$ получить модулярную форму арифметического полинома (5) на основе данного арифметического полинома вида (1) ФАЛ $|x_1+x_2|_k$ для произвольного m и $m=5$ (табл. 3):

$$|x_1+x_2|_3 = \Big|x_1+x_2+|21|4^{\varphi(m)-1}|_m|_m x_1x_2 + \left(m-|15|4^{\varphi(m)-1}|_m|_m\right)x_1x_2^2 +$$
$$+\left(m-|15|4^{\varphi(m)-1}|_m|_m\right)x_1^2x_2 + |9|4^{\varphi(m)-1}|_m|_m x_1^2x_2^2\Big|_m =$$
$$= \left|x_1+x_2+4x_1x_2+x_1^2x_2^2\right|_5,$$

где $\varphi(m)$ – функция Эйлера [13].

Пример 4. При $k=3$ получить модулярную форму арифметического полинома из примера 2 для произвольного m и $m=5$:

$$\mu(X) = \left|2-4x_2+2x_2^2-x_1+\frac{11}{2}x_1x_2-3x_1x_2^2-\frac{3}{2}x_1^2x_2+x_1^2x_2^2\right|_m =$$
$$= \Big|2+(m-|4|_m)\,x_2+2x_2^2+(m-1)x_1+|11|_m 2^{\varphi(m)-1}x_1x_2+$$
$$+(m-3)x_1x_2^2+(m-3)2^{\varphi(m)-1}x_1^2x_2+x_1^2x_2^2\Big|_m =$$
$$= \left|2+x_2+2x_2^2+4x_1+3x_1x_2+2x_1x_2^2+x_1^2x_2+x_1^2x_2^2\right|_5.$$

2.3. Логические теоретико-числовые преобразования на k-значной логике

Логические теоретико-числовые преобразования (ЛТЧП) на двузначной логике были введены в [7, 14, 8]. Введем понятие модулярного базиса ЛТЧП на k-значной логике. Обозначим как $\boldsymbol{\Upsilon}_k$ и $\boldsymbol{\Upsilon}_k^{-1}$ базовые матрицы размерности $k\times k$ соответственно прямого и обратного k-ЛТЧП. Причем, если обозначить элементы базовых матриц k-ЛДПФ $\mathbf{K}_k$ и $\mathbf{K}_k^{-1}$ соответственно как k_{ij} и $k_{ij}^{(-1)}$, то элементы υ_{ij} и $\upsilon_{ij}^{(-1)}$ матриц $\boldsymbol{\Upsilon}_k$ и $\boldsymbol{\Upsilon}_k^{-1}$ образуются из элементов матриц $\mathbf{K}_k$ и $\mathbf{K}_k^{-1}$ соответственно как $\upsilon_{ij}=|k_{ij}|_m$ и $\upsilon_{ij}^{(-1)}=\left|k_{ij}^{(-1)}\right|_m$. Тогда модулярный базис ЛТЧП – матрицы $\boldsymbol{\Upsilon}_{k^n}$ и $\boldsymbol{\Upsilon}_{k^n}^{-1}$ – определятся кронекеровским возведением в степень:

$$\boldsymbol{\Upsilon}_{k^n} = \left|\bigotimes_{j=1}^{n}\boldsymbol{\Upsilon}_k\right|_m, \quad \boldsymbol{\Upsilon}_{k^n}^{-1} = \left|\bigotimes_{j=1}^{n}\boldsymbol{\Upsilon}_k^{-1}\right|_m,$$

где запись $|\cdot|_m$ означает, что все арифметические операции с элементами матриц выполняются по модулю m и результат этих преобразований – наименьший неотрицательный вычет.

Пример 5. Зададим значения модуля $m=5$ и $m=7$. Тогда базовые матрицы $\boldsymbol{\Upsilon}_k$ и $\boldsymbol{\Upsilon}_k^{-1}$ для различных значений k будут иметь вид, представленный в табл. 5 и 6.

Предложение 2. Если для ФАЛ задана пара матричных преобразований (ЛДПФ) (2) и (3) и $m\ge k$ (m – простое), то справедливы преобразования:

(6) $$\boldsymbol{\Psi} = \left|R_{k,n}\boldsymbol{\Upsilon}_{k^n}\mathbf{Y}\right|_m,$$

(7) $$\mathbf{Y} = \left|\boldsymbol{\Upsilon}_{k^n}^{-1}\boldsymbol{\Psi}\right|_m,$$

Таблица 5. Расчетные Υ_k и Υ_k^{-1} при $m = 5$

k	Υ_k	Υ_k^{-1}
2	$\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
3	$\begin{bmatrix} 2 & 0 & 0 \\ 2 & 4 & 4 \\ 1 & 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$
4	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 4 & 3 & 1 & 2 \\ 1 & 0 & 2 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 3 & 4 & 2 \end{bmatrix}$
5	$\begin{bmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 2 & 4 \\ 0 & 1 & 4 & 4 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 & 1 \\ 1 & 4 & 1 & 4 & 1 \end{bmatrix}$

Таблица 6. Расчетные Υ_k и Υ_k^{-1} при $m = 7$

k	Υ_k	Υ_k^{-1}
2	$\begin{bmatrix} 1 & 0 \\ 6 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
3	$\begin{bmatrix} 2 & 0 & 0 \\ 4 & 4 & 6 \\ 1 & 5 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$
4	$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 3 & 4 & 5 & 2 \\ 6 & 6 & 5 & 4 \\ 6 & 3 & 4 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 \\ 1 & 3 & 2 & 6 \end{bmatrix}$
5	$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 6 & 5 & 5 & 4 & 1 \\ 0 & 1 & 2 & 0 & 4 \\ 4 & 1 & 1 & 0 & 1 \\ 1 & 3 & 1 & 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 \\ 1 & 3 & 2 & 6 & 4 \\ 1 & 4 & 2 & 1 & 4 \end{bmatrix}$
6	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 2 & 2 & 1 & 4 & 3 \\ 1 & 0 & 6 & 4 & 4 & 1 \\ 6 & 5 & 5 & 0 & 5 & 0 \\ 1 & 0 & 4 & 6 & 6 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 3 & 6 & 2 & 3 \end{bmatrix}$

где $R_{k,n} = \left|\dfrac{1}{N_{k,n}}\right|_m$ *– модулярная форма нормализующего множителя;* Υ_{k^n} *и* $\Upsilon_{k^n}^{-1}$ *– модулярная форма матриц соответственно прямого и инверсного арифметического преобразования размерности* $k^n \times k^n$ *(базис преобразования);* $\mathbf{S}$ *– вектор истинности* k*-значной ФАЛ;* $\mathbf{\Psi} = [\ \rho_0 \quad \rho_1 \quad \ldots \quad \rho_{k^n-1}\ ]$ *– вектор коэффициентов (спектр) арифметического полинома* (5).

Для доказательства предложения 2 необходимо учесть взаимооднозначность связи между матричной (2), (3) и полиномиальной (1) формами представления ФАЛ [9]. Тогда справедливость (6) и (7) вытекает из справедливости (5).

Определение 2. Пару преобразований (6) *и* (7) *будем называть модулярной формой соответственно прямого и обратного матричного арифметического преобразования или ЛТЧП на k-значной логике* (k*-ЛТЧП*).

Пример 6. Продемонстрируем применение 3-ЛТЧП к условиям, использованным в примере 1. Выберем модуль $m = 5$. Предварительно вычислим матрицы $\boldsymbol{\Upsilon}_{k^n}$ и $\boldsymbol{\Upsilon}_{k^n}^{-1}$, воспользовавшись табл. 5:

$$\boldsymbol{\Upsilon}_{3^2} = \left| \begin{bmatrix} 2 & 0 & 0 \\ 2 & 4 & 4 \\ 1 & 3 & 1 \end{bmatrix} \otimes \begin{bmatrix} 2 & 0 & 0 \\ 2 & 4 & 4 \\ 1 & 3 & 1 \end{bmatrix} \right|_5 = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 \\ 4 & 3 & 3 & 3 & 1 & 1 & 3 & 1 & 1 \\ 2 & 1 & 2 & 4 & 2 & 4 & 4 & 2 & 4 \\ 2 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 2 & 4 & 4 & 1 & 2 & 2 & 2 & 4 & 4 \\ 1 & 3 & 1 & 3 & 4 & 3 & 1 & 3 & 1 \end{bmatrix};$$

$$\boldsymbol{\Upsilon}_{3^2}^{-1} = \left| \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \right|_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 0 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 4 & 4 & 4 \\ 1 & 2 & 4 & 2 & 4 & 3 & 4 & 3 & 1 \end{bmatrix}.$$

Прямое 3-ЛТЧП (2) с учетом $R_{3,2} = 4$ примет вид:

$$\boldsymbol{\Psi} = \left| R_{3,2} \boldsymbol{\Upsilon}_{3^2} \mathbf{Y} \right|_5 = \left| 4 \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 \\ 4 & 3 & 3 & 3 & 1 & 1 & 3 & 1 & 1 \\ 2 & 1 & 2 & 4 & 2 & 4 & 4 & 2 & 4 \\ 2 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 2 & 4 & 4 & 1 & 2 & 2 & 2 & 4 & 4 \\ 1 & 3 & 1 & 3 & 4 & 3 & 1 & 3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 2 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 2 \end{bmatrix} \right|_5 = \begin{bmatrix} 2 \\ 1 \\ 2 \\ 4 \\ 3 \\ 2 \\ 0 \\ 1 \\ 1 \end{bmatrix} \begin{matrix} \\ x_2 \\ x_2^2 \\ x_1 \\ x_1 x_2 \\ x_1 x_2^2 \\ x_1^2 \\ x_1^2 x_2 \\ x_1^2 x_2^2 \end{matrix}.$$

Обратное преобразование (3) будет иметь вид:

$$\mathbf{Y} = \left| \boldsymbol{\Upsilon}_{3^2}^{-1} \boldsymbol{\Psi} \right|_5 = \left| \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 0 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 4 & 4 & 4 \\ 1 & 2 & 4 & 2 & 4 & 3 & 4 & 3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 2 \\ 4 \\ 3 \\ 2 \\ 0 \\ 1 \\ 1 \end{bmatrix} \begin{matrix} \\ x_2 \\ x_2^2 \\ x_1 \\ x_1 x_2 \\ x_1 x_2^2 \\ x_1^2 \\ x_1^2 x_2 \\ x_1^2 x_2^2 \end{matrix} \right|_5 = \begin{bmatrix} 2 \\ 0 \\ 2 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}.$$

Метод вычисления многозначных ФАЛ на основе одномодульной арифметики позволяет реализовать гибкие логические вычисления с помощью аппаратурных средств, функционирующих по *требуемому* значению модуля (а не по “*жестко*” заданному модулю k). Размерность промежуточных результатов при использовании модулярных форм уменьшается, что позволяет отказаться от использования арифметики многократной точности и сократить время логических вычислений.

Распространим метод реализации *одной* ФАЛ арифметическими полиномами на случай реализации *системы* ФАЛ.

3. Реализация системы логических функций арифметическим полиномом, построенным по принципу "взвешивания"

Пусть дана d-выходная k-значная ФАЛ $f(X)$ (система ФАЛ) от n переменных $X = x_1, x_2, \ldots, x_n$:

$$(8) \qquad y_1 = f_1(X), \quad y_2 = f_2(X), \quad \ldots, \quad y_d = f_d(X),$$

где y_j – значение, принимаемое j-й ФАЛ $f_j(X)$; $x_i,\ y_j \in \{0, 1, \ldots, k-1\}$ ($i=1, 2, \ldots, n$; $j = 1,\ 2, \ldots, d$).

Известен способ реализации систем k-значных ФАЛ с помощью арифметического полинома:

$$(9) \qquad D = D(X) = \sum_{i=0}^{k^n-1} c_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

где $c_i \in \mathbb{Q}$; D – числовое значение, принимаемое полиномом $D(X)$.

Процедура построения полинома (9) аналогична процедуре построения арифметического полинома представления систем булевых функций [9] и приведена в Приложении. Для случая реализации *системы* ФАЛ с помощью ЛДПФ (2) и (3) примет вид:

$$(10) \qquad \mathbf{C} = N_{k,n}^{-1} \mathbf{K}_{k^n} \mathbf{D},$$

$$(11) \qquad \mathbf{D} = \mathbf{K}_{k^n}^{-1} \mathbf{C},$$

где $N_{k,n}$ – нормализующий множитель; $\mathbf{K}_{k^n}$ и $\mathbf{K}_{k^n}^{-1}$ – соответственно матрицы прямого и инверсного арифметического преобразования размерности $k^n \times k^n$ (базис преобразования); $\mathbf{D}$ – вектор истинности k-значной ФАЛ;

$$\mathbf{D} = [\mathbf{Y}_d | \mathbf{Y}_{d-1} | \ldots | \mathbf{Y}_1]^{\mathrm{T}} = \left[D^{(0)} D^{(1)} \ldots D^{(k^n-1)} \right]^{\mathrm{T}},$$

где $\mathbf{Y}_i = \left[\ Y_i^{(0)} \quad Y_i^{(1)} \quad \ldots \quad Y_i^{(k^n-1)}\ \right]^{\mathrm{T}}$ – вектор истинности i-й ФАЛ $f_i(X)$; $D^{(j)}$ – числовое значение, принимаемое d-выходной k-значной ФАЛ $f(X)$ на j-м наборе аргументов таблицы истинности; $\mathbf{C} = [\ c_0 \quad c_1 \quad \ldots \quad c_{k^n-1}\ ]$ – вектор коэффициентов (спектр) арифметического полинома (9).

Если результат вычисления (9) получить в k-ичной системе счисления, то он будет представлять собой кортеж значений искомых ФАЛ $y_d(X) \odot y_{d-1}(X) \odot \cdots \odot y_1(X)$ ($\odot$ – разделительный знак), интерпретируемый как код целого неотрицательного числа $(y_d\, y_{d-1} \ldots y_1)_k = D = \sum\limits_{j=1}^{d} y_j k^{j-1}$.

В табл. 7 дан пример числового задания 2-выходной 3-значной ФАЛ $f(X)$. Реализация системы ФАЛ может быть осуществлена аналогично принципам, устанавливаемым схемами вычисления для одной ФАЛ (рис. 1 и 2). Однако в силу того, что

Таблица 7. Пример числового задания системы из двух 3-значных ФАЛ

j	x_1	x_2	y_2	y_1	$D^{(j)}$ (десятичная запись)
0	0	0	2	1	7
1	0	1	0	2	2
2	0	2	2	2	8
3	1	0	1	1	4
4	1	1	1	0	3
5	1	2	1	0	3
6	2	0	0	2	2
7	2	1	1	2	5
8	2	2	2	1	7

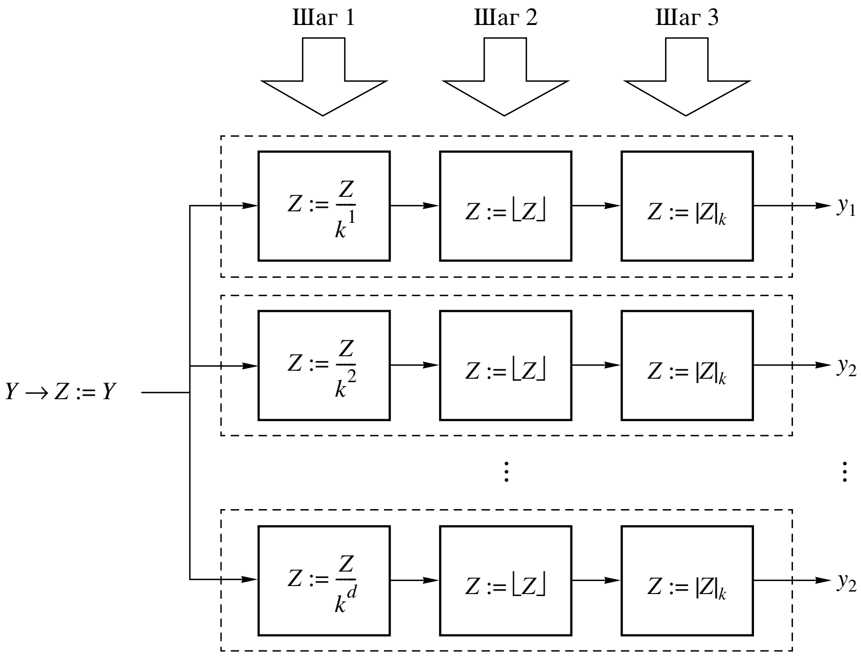

Рис. 6. Структура параллельного алгоритма “извлечения” значений y_1, y_2, $\dots$, y_d ФАЛ из результата вычисления арифметического полиномома (9).

результат D обычно представлен в двоичной системе счисления, дополнительно применяется оператор маскирования $\Xi^t\{D\}$, служащий для определения t-го разряда (выхода) k-ичного представления $D = (y_d \dots y_t \dots y_1)_k$, т.е. $\Xi^t\{D\} = y_t$.

Если для вычисления оператора $\Xi^t\{D\}$ использовать формулу

$$\Xi^t\{D\} = \left| \left\lfloor \frac{D}{k^t} \right\rfloor \right|_k, \tag{12}$$

то структура процедуры “извлечения” значений ФАЛ из результата вычисления арифметического полинома (9) будет содержать три ступени (рис. 6).

Недостатки (9) аналогичны недостаткам полинома (1) и заключаются в высокой сложности представления (9). Для их ослабления так же, как и в случае реализации одной ФАЛ, применимы методы модулярной арифметики.

Предложение 3. Если $m \geq k^d$, где $k^d - 1$, – максимальное значение, принимаемое D, то произвольный кортеж k-значных ФАЛ может быть представлен арифметическим полиномом:

$$D = M(X) = \left| \sum_{i=0}^{k^n-1} \omega_i \, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m, \tag{13}$$

где $\omega_i = |c_i|_m$ $(i = 0, 1, \dots, k^n - 1)$.

В качестве доказательства предложения 3 в Приложении приведена процедура построения (13).

Используя аналогии с k-ЛТЧП (6) и (7) для случая одной ФАЛ и с k-ЛДПФ для случая системы ФАЛ (14) и (15), k-ЛТЧП для случая *системы* ФАЛ (8) примет

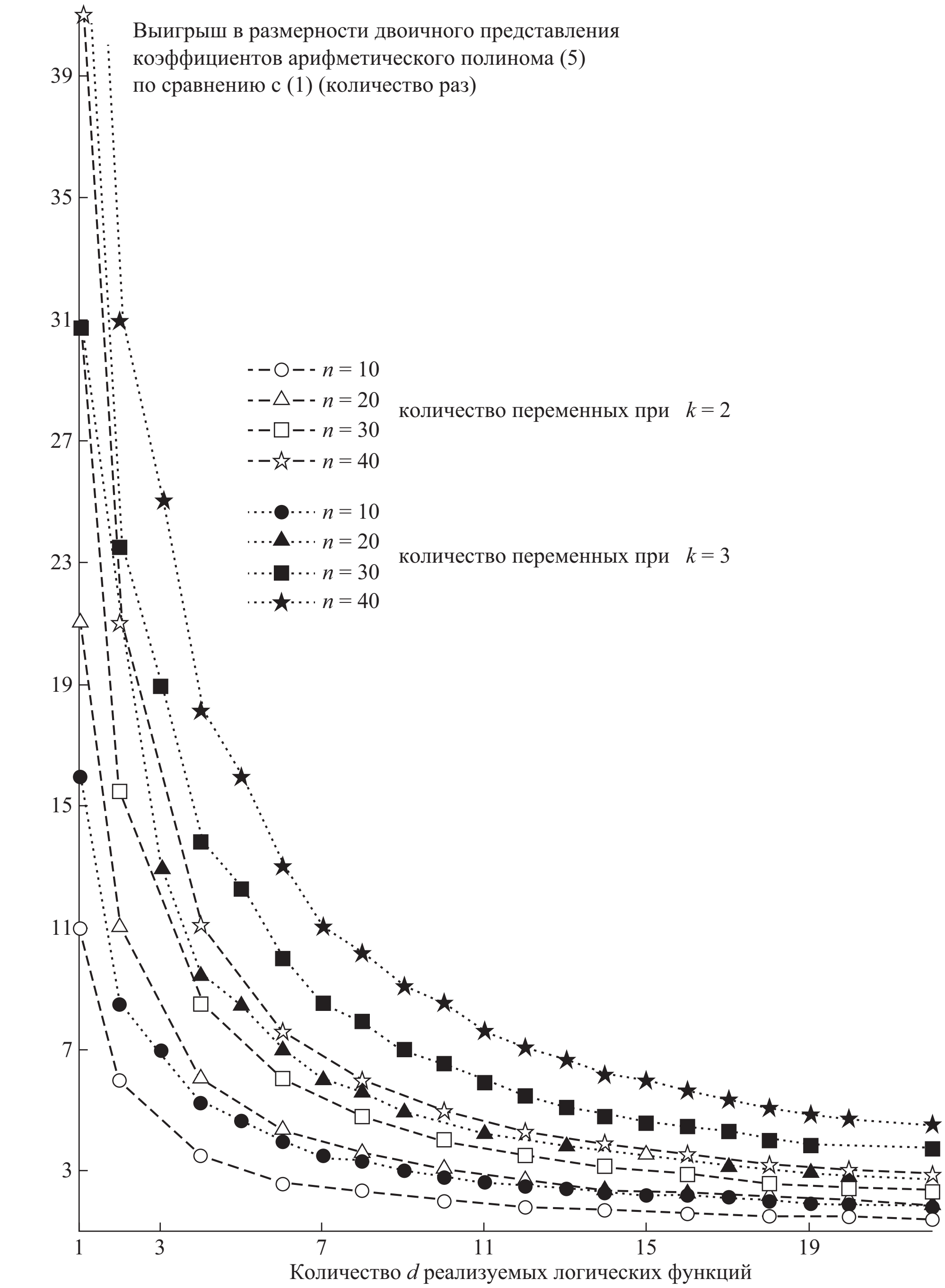

Рис. 7. Теоретический выигрыш (количество раз) – уменьшение максимальной размерности (количества бит) коэффициентов арифметического полинома для $k = 2$ и $k = 3$ формы (5) по сравнению с формой (1).

вид:

$$\mathbf{\Omega} = |R_{k,n}\mathbf{\Upsilon}_{k^n}\mathbf{D}|_m\,, \tag{14}$$

$$\mathbf{D} = \left|\mathbf{\Upsilon}_{k^n}^{-1}\mathbf{\Omega}\right|_m, \tag{15}$$

где $R_{k,n} = \left|\dfrac{1}{N_{k,n}}\right|_m$ – модулярная форма нормализующего множителя; $\mathbf{\Upsilon}_{k^n}$ и $\mathbf{\Upsilon}_{k^n}^{-1}$ – модулярная форма матриц соответственно прямого и инверсного арифметического преобразования размерности $k^n \times k^n$ (базис преобразования); $\mathbf{D}$ – вектор истинности k-значной ФАЛ; $\mathbf{D} = [\mathbf{Y}_d|\mathbf{Y}_{d-1}|\ldots|\mathbf{Y}_1]^{\mathrm{T}} = \left[D^{(0)}D^{(1)}\ldots D^{(k^n-1)}\right]^{\mathrm{T}}$, где $\mathbf{Y}_i = \left[\begin{array}{cccc} Y_i^{(0)} & Y_i^{(1)} & \ldots & Y_i^{(k^n-1)}\end{array}\right]^{\mathrm{T}}$ – вектор истинности i-й ФАЛ $f_i(X)$; $D^{(j)}$ – числовое значение, принимаемое d-выходной k-значной ФАЛ $f(X)$ на j-м наборе аргументов таблицы истинности; $\mathbf{\Omega} = [\begin{array}{cccc}\omega_0 & \omega_1 & \ldots & \omega_{k^n-1}\end{array}]$ – вектор коэффициентов (спектр) арифметического полинома (13).

Для сравнения максимальной размерности коэффициентов полиномов (1) и (5) необходимо проанализировать структуру матриц $\mathbf{K}_{k^n}$ и $\mathbf{K}_{k^n}^{-1}$ в (2) и (3). При $k=2$ согласно [8] максимальный коэффициент результирующего полинома будет давать нижняя строка матриц $\mathbf{K}_{2^n}$ и $\mathbf{K}_{2^n}^{-1}$ преобразования и размерность максимального коэффициента составит $n+d$ двоичных радзряда. Учитывая, что для представления коэффициентов модулярной формы арифметического полинома потребуется $\lceil\log_2 m\rceil$ ($\lceil x\rceil$ – наименьшее целое число, равное или превышающее x) двоичных разряда, при $m = 2^d$ выигрыш модулярной формы арифметического полинома по количеству двоичных разрядов представления максимального коэффициента составит $\dfrac{n}{d}+1$ раз. При $k=3$ этот выигрыш составит $\dfrac{3n}{\lceil\log_2 3^d\rceil}$ раз. Из рис. 7 можно видеть, что преимущества модулярных форм с увеличением k возрастают.

Схемы реализации системы ФАЛ посредством (13) аналогичны схемам реализации для одной ФАЛ (рис. 4 и 5).

Для получения окончательного результата должен быть использован упомянутый выше оператор маскирования, для вычисления которого потребуется три ступени преобразования (рис. 6).

4. Синтез арифметического полинома для реализации систем k-значных функций с помощью Китайской теоремы об остатках

Как следует из (12) и рис. 6, для реализации оператора $\Xi^t\{Y\}$ требуется выполнить три операции: деление, округление и нахождение наименьшего неотрицательного вычета. Это обстоятельство уменьшает скорость вычислений на наиболее критичном этапе – реализации ФАЛ. Рассмотрим альтернативный принцип построения арифметического полинома, на основании Китайской теоремы об остатках.

В соответствии с Китайской теоремой об остатках [15, 13] при $\gcd(m_i, m_j) = 1$ $(i \neq j, \quad i,j = 1,2,\ldots,d)$ система уравнений первой степени (частный случай): $|A|_{m_1} = \phi_1$, $|A|_{m_2} = \phi_2$, $\ldots$, $|A|_{m_d} = \phi_d$ имеет единственное решение A такое, что $0 \le A < m = m_1 m_2 \ldots m_d$.

Решение системы уравнений, предлагаемое Китайской теоремой об остатках, в современной трактовке [15, 13] состоит в вычислении выражения:

$$A = |\phi_1 B_1 + \phi_2 B_2 + \ldots + \phi_d B_d|_m\,, \tag{16}$$

где $B_i = q_i m m_i^{-1}$; q_i находится из сравнения $q_i m m_i^{-1} \equiv 1 \pmod{m_i}$ $(i = 1,\,2,\,\ldots,\,d)$.

Пусть дана система d ФАЛ: $f_1(X),\ f_2(X),\ \ldots,\ f_d(X)$, где k_i – значность i-й ФАЛ, и поставленная в соответствие им система арифметических полиномов вида (5): $\mu_1(X),\ \mu_2(X),\ \ldots,\ \mu_d(X)$.

П р е д л о ж е н и е 4. *Если даны простые модули $m_1,\ m_2,\ \ldots,\ m_d$ (в общем случае порядок следования произволен) такие, что $m_i \geq k_t$ $(i,\ t = 1,\ 2,\ \ldots,\ d)$, то произвольный кортеж k-значных ФАЛ может быть представлен арифметическим полиномом:*

$$T = \Theta(X) = \left| \sum_{i=0}^{k^n-1} \zeta_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m , \tag{17}$$

где $0 \leq \zeta_i < m$, причем для "извлечения" значения i-й ФАЛ y_i из результата вычисления полинома (17) достаточно вычислить значение наименьшего неотрицательного вычета от этого результата по соответствующему номеру модуля m_i: $y_1 = |T|_{m_1}$, $y_2 = |T|_{m_2}$, $\ldots$, $y_d = |T|_{m_d}$.

Д о к а з а т е л ь с т в о. Выбранные в предложении 4 модули $m_1,\ m_2,\ \ldots,\ m_d$ удовлетворяют условию $\gcd(m_i,\ m_j) = 1$ $(i \neq j,\ i, j = 1,\ 2,\ \ldots,\ d)$, так как указано, что они являются простыми числами. Условие однозначности модулярного кодирования для каждой ФАЛ, определенное предложением 1, соблюдено требованием $m_i \geq k_t$ $(i,\ t = 1,\ 2,\ \ldots,\ d)$. Это же требование обеспечивает условие $0 \leq A < m = m_1 m_2 \ldots m_d$.

Будем отождествлять полиномы $\mu_1(X),\ \mu_2(X),\ \ldots,\ \mu_d(X)$ с вычетами $\phi_1,\ \phi_2,\ \ldots,\ \phi_d$ в формуле (16), где $m = m_1 m_2 \ldots m_d$. Рассмотрим следующую процедуру.

П р о ц е д у р а 1.

Ш а г 1. Построение полиномов вида (5) для представления каждой ФАЛ:

$$\mu_1(X) = \left| \sum_{i=0}^{k^n-1} \rho_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_{m_1} ,$$

$$\mu_2(X) = \left| \sum_{i=0}^{k^n-1} \rho_{2,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_{m_2} ,$$

$$\vdots$$

$$\mu_d(X) = \left| \sum_{i=0}^{k^n-1} \rho_{d,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_{m_d}$$

и запись в виде:

$$\mu_1^*(X) = \sum_{i=0}^{k^n-1} \rho_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

$$\mu_2^*(X) = \sum_{i=0}^{k^n-1} \rho_{2,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

$$\vdots$$

$$\mu_d^*(X) = \sum_{i=0}^{k^n-1} \rho_{d,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

Шаг 2. Выполнение модулярных умножений:

$$
\begin{aligned}
|B_1\mu_1^*(X)|_m &= \sum_{i=0}^{k^n-1} \zeta_{1,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},\\
|B_2\mu_1^*(X)|_m &= \sum_{i=0}^{k^n-1} \zeta_{2,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},\\
&\vdots\\
|B_d\mu_1^*(X)|_m &= \sum_{i=0}^{k^n-1} \zeta_{d,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},
\end{aligned}
$$

где $\zeta_{j,\,i}^*(X) = |B_j\rho_{j,\,i}|_m$, $i = 0, 1, \ldots, k^n - 1$; $j = 1, \ldots, d$ (числа B_i оговорены выше).

Шаг 3.

$$
\Theta(X) = \left| \sum_{i=0}^{k^n-1} \sum_{j=1}^{d} \zeta_{j,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m = \left| \sum_{i=0}^{k^n-1} \zeta_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m,
$$

где $\zeta_i = \sum_{j=1}^{d} \zeta_{j,\,i}^*$ $(i = 0, 1, \ldots, k^n - 1)$.

Корректность вычислений в конечном поле обеспечивается соблюдением условия простоты модулей.

Определение 3. Выражение (17) *будем называть КТО-формой* (*КТО – Китайская теорема об остатках*).

Пример 7. Рассмотрим применение предложения 4 для случая реализации двух 3-значных ФАЛ, векторы значений которых при $n = 2$, имеют вид:

$$
\begin{aligned}
\mathbf{S}_1 &= [\,0\;\;0\;\;2\;\;2\;\;1\;\;1\;\;0\;\;0\;\;2\,]^{\mathrm{T}},\\
\mathbf{S}_2 &= [\,2\;\;0\;\;2\;\;1\;\;1\;\;1\;\;0\;\;1\;\;2\,]^{\mathrm{T}}.
\end{aligned}
$$

Им соответствуют арифметические полиномы вида (1):

$$
\begin{aligned}
P_1(X) &= -x_2 + x_2^2 + 4x_1 - x_1x_2 - x_1x_2^2 - 2x_1^2 + \frac{1}{2}x_1^2x_2 + \frac{1}{2}x_1^2x_2^2,\\
P_2(X) &= 2 - 4x_2 + 2x_2^2 - x_1 + \frac{11}{2}x_1x_2 - 3x_1x_2^2 - \frac{3}{2}x_1^2x_2 + x_1^2x_2^2.
\end{aligned}
$$

В соответствии с предложением 4 выберем модули: $m_1 = 3$, $m_2 = 5$. Тогда $m = m_1m_2 = 15$, значения констант B_1 и B_2 в соответствии с (16) составят:

$$
B_1 = \frac{q_1m}{m_1} = \frac{2\cdot 15}{3} = 10, \quad B_2 = \frac{q_2m}{m_2} = \frac{2\cdot 15}{5} = 6.
$$

Применение процедуры 1 в этом случае будет выглядеть следующим образом:

Шаг 1. Построение полиномов вида (5) (пример 6):

$$
\begin{aligned}
\mu_1(X) &= \left|2x_2 + x_2^2 + x_1 + 2x_1x_2 + 2x_1x_2^2 + x_1^2 + 2x_1^2x_2 + 2x_1^2x_2^2\right|_3,\\
\mu_2(X) &= \left|2 + x_2 + 2x_2^2 + 4x_1 + 3x_1x_2 + 2x_1x_2^2 + x_1^2x_2 + x_1^2x_2^2\right|_5
\end{aligned}
$$

и запись их в “немодулярном” виде:

$$
\begin{aligned}
\mu_1^*(X) &= 2x_2 + x_2^2 + x_1 + 2x_1x_2 + 2x_1x_2^2 + x_1^2 + 2x_1^2x_2 + 2x_1^2x_2^2,\\
\mu_2^*(X) &= 2 + x_2 + 2x_2^2 + 4x_1 + 3x_1x_2 + 2x_1x_2^2 + x_1^2x_2 + x_1^2x_2^2.
\end{aligned}
$$

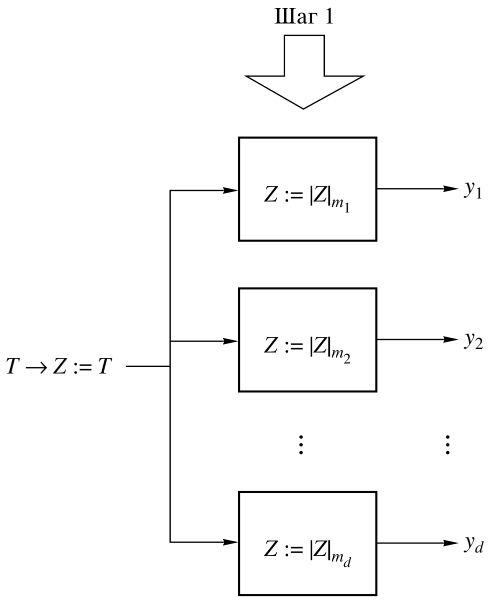

Рис. 8. Структура параллельного алгоритма “извлечения” значений y_1, y_2, $\ldots$, y_d ФАЛ из результата вычисления арифметического полиномома (17).

Шаг 2. Выполнение модулярных умножений:

$$\begin{aligned}
&|10\mu_1^*(X)|_{15} = |10 \cdot 2|_{15}x_2 + 10x_2^2 + 10x_1 + |10 \cdot 2|_{15}x_1x_2 + \\
&+ |10 \cdot 2|_{15}x_1x_2^2 + 10x_1^2 + |10 \cdot 2|_{15}x_1^2x_2 + |10 \cdot 2|_{15}x_1^2x_2^2 = \\
&= 5x_2 + 10x_2^2 + 10x_1 + 5x_1x_2 + 5x_1x_2^2 + 10x_1^2 + 5x_1^2x_2 + 5x_1^2x_2^2, \\
&|6\mu_1^*(X)|_{15} = |6 \cdot 2|_{15} + 6x_2 + |6 \cdot 2|_{15}x_2^2 + |6 \cdot 4|_{15}x_1 + \\
&+ |6 \cdot 3|_{15}x_1x_2 + |6 \cdot 2|_{15}x_1x_2^2 + 6x_1^2x_2 + 6x_1^2x_2^2 = \\
&= 12 + 6x_2 + 12x_2^2 + 9x_1 + 3x_1x_2 + 12x_1x_2^2 + 6x_1^2x_2 + 6x_1^2x_2^2.
\end{aligned}$$

Шаг 3.

$$\begin{aligned}
&\Theta(X) = |0 + 12|_{15} + |5 + 6|_{15}x_2 + |10 + 12|_{15}x_2^2 + \\
&+ |10 + 9|_{15}x_1 + |5 + 3|_{15}x_1x_2 + |5 + 12|_{15}12x_1x_2^2 + \\
&+ |10 + 0|_{15}x_1^2 + |5 + 6|_{15}x_1^2x_2 + |5 + 6|_{15}x_1^2x_2^2.
\end{aligned}$$

Таким образом,

$$\Theta(X) = 12 + 11x_2 + 7x_2^2 + 4x_1 + 8x_1x_2 + 2x_1x_2^2 + 10x_1^2 + 11x_1^2x_2 + 11x_1^2x_2^2.$$

Для проверки рассмотрим два случая. Первый случай: $x_1 = 0$ и $x_2 = 0$ (первая строка таблицы истинности). Второй случай: $x_1 = 2$ и $x_2 = 2$ (последняя строка таблицы истинности). В первом случае получим $\Theta(X) = |12|_{15} = 12$. Результат (см. исходные условия):

$$y_1 = |12|_3 = 0, \quad y_2 = |12|_5 = 2.$$

Во втором случае:

$$\Theta(X) = \big|12 + |11 \cdot 2|_{15} + |7 \cdot 2^2|_{15} + |4 \cdot 2|_{15} + |8 \cdot 2 \cdot 2|_{15} + |2 \cdot 2 \cdot 2^2|_{15} +$$
$$+ |10 \cdot 2^2|_{15} + |11 \cdot 2^2 \cdot 2|_{15} + |11 \cdot 2^2 \cdot 2^2|_{15}\big|_{15} =$$
$$= |12 + 7 + 13 + 8 + 2 + 1 + 10 + 13 + 11|_{15} = |77|_{15} = 2.$$

Результат:

$$y_1 = |2|_3 = 2, \quad y_2 = |2|_5 = 2.$$

В отличие от рис. 4 и рис. 5 вычисления посредством (17) осуществляются в конечном кольце $\mathbb{Z}_m$.

К *недостаткам* (17) можно отнести более сложную процедуру формирования полинома (см. доказательство). Однако этот недостаток не сказывается при использовании второй схемы вычисления ФАЛ, аналогичной рис. 5.

Достоинством (17) является более *простая* схема получения окончательного результата (рис. 8), которая будет состоять из *одного* этапа в противоположность *трехэтапному* преобразованию (рис. 6) в соответствии с (12).

5. Заключение

Получено *обобщение* модулярных форм арифметических полиномов на область представления функций и *систем* функций k-значной логики. Введены теоретико-числовые преобразования на k-значной логике. При этом достигается ряд преимуществ, важных для решения вопросов *технической реализации* параллельных логических вычислений. Так, применение модулярных форм позволило существенно *ограничить* размерность коэффициентов арифметического полинома и расчетных промежуточных результатов; вычисления из арифметики поля рациональных чисел $\mathbb{Q}$ перенесены в *целочисленную* арифметику простого поля $\mathbb{F}_m$. Предложен новый способ представления *систем* k-значных ФАЛ *одним* арифметическим полиномом, основанный на применении Китайской теоремы об остатках. В отличие от известных способов, использующих принцип "взвешивания", данный способ имеет преимущества по *сложности реализации* ФАЛ.

Рассмотрены процедуры построения соответствующих модулярных форм, пригодные для практического использования.

ПРИЛОЖЕНИЕ

Доказательство предложения 1. Пусть дан арифметический полином $P(X)$ (1). Тогда согласно теории сравнений [13] справедливо:

$$|Y|_m = \left|\sum_{i=0}^{k^n-1} p_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m = \left|\sum_{i=0}^{k^n-1} |p_i|_m\; x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m. \tag{18}$$

Но при условии $Y < m$ (Y неотрицательное) выполняется $|Y|_m = Y$. Следовательно, при $Y < m$:

$$Y = \left|\sum_{i=0}^{k^n-1} |p_i|_m\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m = \left|\sum_{i=0}^{k^n-1} \rho_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m, \tag{19}$$

где $\rho_i = |p_i|_m$.

Процедура построения полинома (9):

Шаг 1. Поставим в соответствие системе ФАЛ $f_1(X),\ f_2(X),\ \ldots,\ f_d(X)$ арифметические полиномы вида (1):

$$P_1(X) = \sum_{i=0}^{k^n-1} p_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

$$P_2(X) = \sum_{i=0}^{k^n-1} p_{2,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

$$\vdots$$

$$P_d(X) = \sum_{i=0}^{k^n-1} p_{d,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

Шаг 2. Умножим эти полиномы на веса k^{j-1} ($j = 1,\, 2,\, \ldots,\, d$):

$$P_1^*(X) = \quad k^0 P_1(X) = \sum_{i=0}^{k^n-1} p_{1,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

$$P_2^*(X) = \quad k^1 P_2(X) = \sum_{i=0}^{k^n-1} p_{2,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

$$\vdots$$

$$P_d^*(X) = k^{d-1} P_{d-1}(X) = \sum_{i=0}^{k^n-1} p_{d,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

где $p_{j,\,i}^* = k^{j-1} p_{j,i}$ ($j = 1, 2, \ldots, d;\ i = 0, 1, \ldots, k^n - 1$).

Шаг 3. Получение арифметического полинома

$$D(X) = \sum_{i=0}^{k^n-1} \sum_{j=1}^{d} p_{j,\,i}^*\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = \sum_{i=0}^{k^n-1} c_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

где $c_i = \sum\limits_{j=1}^{d} p_{j,\,i}^*$ ($i = 0, 1, \ldots, k^n - 1$).

Процедура построения полинома (13):

Шаг 1. Поставим системе d ФАЛ $f_1(X),\ f_2(X),\ \ldots,\ f_d(X)$ в соответствие арифметические полиномы вида (5):

$$\mu_1(X) = \left| \sum_{i=0}^{k^n-1} \rho_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m,$$

$$\mu_2(X) = \left| \sum_{i=0}^{k^n-1} \rho_{2,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m,$$

$$\vdots$$

$$\mu_d(X) = \left| \sum_{i=0}^{k^n-1} \rho_{d,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|_m.$$

Шаг 2. Найдем модулярные произведения:

$$\begin{aligned}
\left|l_0 \mu_1(X)\right|_m &= \left|\sum_{i=0}^{k^n-1} \rho^*_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m, \\
\left|l_1 \mu_1(X)\right|_m &= \left|\sum_{i=0}^{k^n-1} \rho^*_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m, \\
&\vdots \\
\left|l_{d-1} \mu_1(X)\right|_m &= \left|\sum_{i=0}^{k^n-1} \rho^*_{1,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m,
\end{aligned}$$

где $\rho^*_{j,\,i} = \left|l_{j-1}\rho_{j,\,i}\right|_m$; $l_{j-1} = \left|k^{j-1}\right|_m$; $(j = 1, 2, \ldots, d;\ i = 0, 1, \ldots, k^n - 1)$.

Шаг 3.

$$M(X) = \left|\sum_{i=0}^{k^n-1} \sum_{j=1}^{d} \rho^*_{j,\,i}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m = \left|\sum_{i=0}^{k^n-1} \omega_i\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\right|_m,$$

где $\omega_i = \sum\limits_{j=1}^{d} \rho^*_i$ $(i = 0, 1, \ldots, k^n - 1)$.

СПИСОК ЛИТЕРАТУРЫ

1. *Карпенко А.С.* Многозначные логики / Логика и компьютер. Вып. 4. М.: Наука, 1997.
2. *Асланова Н.Х., Фараджев Р.Г.* Об арифметическом представлении функций многозначной логики и параллельном алгоритме нахождения такого представления // АиТ. 1992. № 2. С. 120–131.
3. *Дзюжаньски П., Малюгин В., Шмерко В., Янушкевич С.* Линейные модели схем на многозначных элементах // АиТ. 2002. № 6. С. 99–119.
4. *Кухарев Г.А., Шмерко В.П., Зайцева Е.Н.* Алгоритмы и систолические процессоры для обработки многозначных данных. Минск: Наука и техника, 1990.
5. *Тошич Ж.* Арифметические представления логических функций / Дискретные автоматы и сети связи. М.: Наука, 1970.
6. *Strazdins J.* The polinomial arithmetic of multivalued logic // Algebra, Combinat. Logic Comput. Sci. 1986. V. 42. P. 777–785.
7. *Финько О.А.* Логические вычисления на основе теоретико-числовых преобразований // Тр. II Междунар. конф. по проблемам управления (МКПУ II). М.: Ин-т пробл. упр. им. В.А. Трапезникова РАН, Москва, 16–20 июня 2003. С. 159–166.
8. *Финько О.А.* Реализация систем булевых функций большой размерности методами модулярной арифметики // АиТ. 2004. № 6. С. 37–60.
9. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов. М.: Наука. Физматлит, 1997.
10. *Шмерко В.П.* Синтез арифметических форм булевых функций посредством преобразования Фурье // АиТ. 1989. № 5. С. 134–142.
11. *Кнут Д.Э.* Искусство программирования. Т. 2. Получисленные алгоритмы, 3-е изд.: Пер. с англ. М.: Издательский дом “Вильямс”, 2000.

12. *Финько О.А.* Полиномиальная арифметика функций многозначной логики // Изв. вузов. Приборостроение. 2004. Т. 47. № 5. С. 41–46.

13. *Бухштаб А.А.* Теория чисел. М.: Просвещение, 1966.

14. *Финько О.А.* Применение цифровой обработки сигналов для реализации интенсивных логических вычислений // 6-я Междунар. конф. "Цифровая обработка сигналов и ее применение" (DSPA-2004). Москва, 31 марта – 2 апреля 2004. Сб. тр. М.: Радиотехника, 2004. Т. 1. С. 265–268.

15. *Амербаев В.М.* Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976.

Статья представлена к публикации членом редколлегии О.П. Кузнецовым.

Поступила в редакцию 20.09.2004