УДК 519.7

О. А. Финько

Параллельные логические вычисления — прикладная область модулярной арифметики

(Краснодарское высшее военное училище (военный институт))

Предложено отображение классической алгебры логики на модулярную арифметику, которое открывает новые уникальные возможности по достижению высоких уровней производительности и отказоустойчивости средств гибких логических вычислений.

Сокращения:

АП — арифметический полином;
БФ — булева (ы) функция (и);
ЛДПФ — логическое дискретное преобразование Фурье (в заданном базисе);
ЛТЧП — логические теоретико-числовые преобразования (в заданном базисе);
ЦОС — цифровая обработка сигналов.

1. Введение

При решении задач синтеза и анализа дискретных устройств, построения систем логического управления сложными техническими

объектами и процессами реального времени, реализации средств криптографической защиты информации возникает необходимость в интенсивной обработке больших объемов логических типов данных. Однако традиционные методы описания логических функций, которые основаны на булевых формулах и полиномах Жегалкина, не обеспечивают требуемой эффективности при реализации их с помощью существующего парка информационно-вычислительных средств.

Ключ к решению этого противоречия дают методы реализации БФ с помощью АП, устанавливающие фундаментальную взаимосвязь между логическими и арифметическими типами данных [1—3]. В ряде работ предприняты усилия к расширению классов арифметико-логических форм БФ на основе представления БФ в спектральной области [4]. Это позволило установить связь разнообразных форм представления булевых функций и методов их синтеза, а также воспользоваться эффективным математическим аппаратом и средствами цифровой обработки сигналов для целей анализа и синтеза БФ.

Ряд важных преимуществ, связанных с ограничением числового диапазона представления результатов промежуточных вычислений, распараллеливанием вычислений, обеспечением контроля ошибок и отказоустойчивости вычислительных структур позволяют получить модулярные преобразования.

В докладе излагаются некоторые результаты автора [5—14], посвященные построению модулярных арифметических форм представления булевых функций, которые должны позволить распространить преимущества модулярной арифметики на ее новую прикладную область — параллельные логические вычисления.

2. Представление систем БФ посредством АП. Постановка задачи

Пусть дана система БФ от n переменных $X = x_1, x_2, \mathbf{K}, x_n$:

$$y_1 = f_1(X), \quad y_2 = f_2(X), \quad \mathbf{K}, \quad y_d = f_d(X), \qquad (1)$$

где y_j — значение, принимаемое j-й БФ $f_j(X)$; $x_i, y_j \in \{0,1\}$ $(i = 1, \mathbf{K}, n; \quad j = 1, \mathbf{K}, d)$. При этом кортеж значений БФ $y_d * y_{d-1} * \mathbf{K} * y_1$, где $*$ — разделительный знак, интерпретируется

как код целого неотрицательного числа Y, представленного в двоичной системе счисления: $(y_d y_{d-1} \mathbf{K} y_1)_2 = Y = \sum_{j=1}^{d} y_j 2^{j-1}$,

где $(y_d y_{d-1} \mathbf{K} y_1)_b = Y$ — представление Y в системе счисления по основанию b.

Пример 1.

Представление Y, соответствующее системе БФ

$$\begin{cases} f_1(X) = \overline{x_1 \oplus x_2}, \\ f_2(X) = \overline{x_1 \vee x_2}, \end{cases} \qquad (2)$$

приведено в табл. 1 (здесь и далее $\vee, \wedge, \oplus, \neg$ — символы операций логического сложения, умножения, сложения по модулю 2 и инверсии соответственно).

Таблица 1.

x_1	x_2	y_1	y_2	Y (десятичная запись)
0	0	1	1	3
0	1	0	0	0
1	0	0	0	0
1	1	0	1	1

2.1. Теорема о представлении системы БФ одним АП

Теорема 1 [1—3]

Произвольный кортеж БФ $f_d(X) * f_{d-1}(X) * \mathbf{K} * f_1(X)$ может быть представлен АП (В.Д. Малюгин):

$$Y = D(X) = \sum_{i=0}^{2^n-1} c_i x_1^{i_1} x_2^{i_2} \mathbf{K} x_n^{i_n}, \qquad (3)$$

где здесь и далее по тексту статьи $i_1 i_2 \mathbf{K} i_n = \sum_{u=1}^{n} i_u 2^{n-u}$, $i_u \in \{0, 1\}$;

$x_u^{i_u} = \begin{cases} x_u, & i_u = 1, \\ 1, & i_u = 0; \end{cases}$ $c_i \in Z$ $(i = 0, 1, \mathbf{K}, 2^n - 1)$ и притом единственным образом.

В качестве *доказательства* этой теоремы далее будут рассмотрены алгоритмы получения (3).

2.2. Алгебраический метод получения АП. Линейные АП

Алгебраический метод получения АП (3) заключается в реализации следующего алгоритма.

А Л Г О Р И Т М 1

Ш а г 1 . Получение АП $P_j(X)$ для каждой БФ $y_j = f_j(X)$, $j = 1, \mathbf{K}, d$:

$$f_j(X) = P_j(X) = \sum_{i=0}^{2^n-1} r_{j,i} x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n}. \qquad (4)$$

Ш а г 2 . Получение АП, взвешенных весами 2^{j-1} $(j = 1, \mathbf{K}, d)$:

$$P'_j(X) = P_j(X) 2^{j-1} = \sum_{i=0}^{2^n-1} r'_{j,i} x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n}, \qquad (5)$$

где $r'_{j,i} = r_{j,i} 2^{j-1}$ $\left(j = 1, \mathbf{K}, d; \quad i = 0, 1, \mathbf{K}, 2^n - 1\right)$.

Ш а г 3 . Получение искомого АП $D(X)$ (3) путем суммирования коэффициентов АП $P'_j(X)$ для всех $j = 1, \mathbf{K}, d$:

$$D(X) = \sum_{i=0}^{2^n-1} \sum_{j=1}^{d} r'_{j,i} x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n} = \sum_{i=0}^{2^n-1} c_i x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n}, \qquad (6)$$

где $c_i = \sum_{j=1}^{d} r'_{j,i}$ $\left(i = 0, 1, \mathbf{K}, 2^n - 1\right)$.

Пример 2.

Для системы БФ (2) реализация алгоритма 1 имеет вид.

Ш а г 1 . Используя соотношения

$$x_1 \wedge x_2 = x_1 x_2,$$
$$x_1 \vee x_2 = x_1 + x_2 - x_1 x_2,$$
$$x_1 \oplus x_2 = x_1 + x_2 - 2x_1 x_2,$$
$$\bar{x} = 1 - x,$$

получим

$$f_1(X) = P_1(X) = \overline{x_1 \oplus x_2} = 1 - x_1 - x_2 + 2x_1 x_2,$$
$$f_2(X) = P_2(X) = \overline{x_1 \vee x_2} = 1 - x_1 - x_2 + x_1 x_2.$$

Ш а г 2 .

$$P_1'(X) = 2^0(1 - x_1 - x_2 + 2x_1 x_2) = 1 - x_1 - x_2 + 2x_1 x_2,$$
$$P_2'(X) = 2^1(1 - x_1 - x_2 + x_1 x_2) = 2 - 2x_1 - 2x_2 + 2x_1 x_2.$$

Ш а г 3 .

$$D(X) = 1 + 2 - (1+2)x_1 - (1+2)x_2 + (2+2)x_1 x_2 = 3 - 3x_1 - 3x_2 + 4x_1 x_2.$$

Из этого примера можно видеть, что числовой диапазон, требуемый для представления коэффициентов и результатов промежуточных вычислений АП, может значительно *превосходить* числовой диапазон, достаточный для представления Y .

Большое значение для представления d -выходных БФ $f(X)$ имеют *линейные* АП $L(X)$, которые определяются выражением

$$U = L(X) = d_0 + \sum_{i=1}^{n} d_i x_i = d_0 + d_1 x_1 + \mathbf{K} + d_n x_n, \qquad (7)$$

где коэффициенты $d_0, d_1, \mathbf{K}, d_n$ — целые числа [3, 15]. При вычислении $f_j(X)$ используется оператор маскирования $\Xi^t\{U\}$ [15], служащий для определения t -го двоичного разряда (выхода) представления $U = a_r 2^{r-1} + \mathbf{K} + a_t 2^{t-1} + \mathbf{K} + a_2 2^1 + a_1 2^0$, т. е. $\Xi^t\{U\} = a_t$.

Пример 3.

Для линеаризации АП $P_j(X) = x_1 + x_2 - x_1 x_2$, соответствующего БФ $f_j(X) = x_1 \vee x_2$ используется введение дополнительной (избыточной) БФ $f_j^{(1)}(X)$. При этом образуется система БФ:

$$f_j^{(1)}(X) = 1 \oplus x_1 \oplus x_2,$$
$$f_j^{(2)}(X) = x_1 \vee x_2.$$

Тогда $U = L(X) = 2^1 f_j^{(2)}(X) + 2^0 f_j^{(1)}(X) = 1 + x_1 + x_2$ и $f_j(X) = \Xi^2\{U\}$.

Таким образом, для представления систем БФ (1) с помощью линейных АП $L(X)$ используется тот же принцип взвешивания представлений БФ с помощью весов 2^i ($i = 0, 1, \mathbf{K}$), что и при построении АП $D(X)$ (3). Однако значения i при этом выбираются с учетом введенных дополнительных БФ.

Пример 4.

Дана система БФ:

$$\begin{cases} f_A(X) = x_1 \wedge x_3, \\ f_B(X) = \bar{x}_1 \wedge x_2, \\ f_C(X) = \bar{x}_2 \wedge x_3. \end{cases} \qquad (8)$$

Для обеспечения линейности результирующего АП добавляют вспомогательные БФ $f_A^{(1)}(X)$, $f_B^{(3)}(X)$, $f_C^{(5)}(X)$ и получают систему БФ:

$$\begin{cases} f_A^{(1)}(X) = x_1 \oplus x_3, \\ f_A^{(2)}(X) = f_A(X), \end{cases} \quad \begin{cases} f_B^{(3)}(X) = \bar{x}_1 \oplus x_2, \\ f_B^{(4)}(X) = f_B(X), \end{cases} \quad \begin{cases} f_C^{(5)}(X) = \bar{x}_2 \oplus x_3, \\ f_C^{(6)}(X) = f_C(X). \end{cases}$$

Далее, в соответствии с (7) и примером 2 имеем:

$$U_A = L'_A(X) = 2^1 f_A^{(1)}(X) + 2^0 f_A^{(2)}(X) = x_1 + x_3,$$
$$U_B = L'_B(X) = 2^1 f_B^{(3)}(X) + 2^0 f_B^{(4)}(X) = 1 - x_1 + x_2,$$
$$U_C = L'_C(X) = 2^1 f_C^{(5)}(X) + 2^0 f_C^{(6)}(X) = 1 - x_2 + x_3.$$

Получаем линейный АП:

$$U = L(X) = 2^0 L'_A(X) + 2^2 L'_B(X) + 2^4 L'_C(X) = 20 - 4x_1 - 12x_2 + 16x_3. \qquad (9)$$

Для определения t-й БФ воспользуемся оператором маскирования $\Xi^t\{Y\}$:

$$f_A(X) = \Xi^2\{U\},$$
$$f_B(X) = \Xi^4\{U\},$$
$$f_C(X) = \Xi^6\{U\}.$$

Отметим, что линейная форма АП (9) достигнута за счет введения избыточных БФ и увеличения числового диапазона, необходимого для представления U в 2^3 раза.

2.3. Матричные преобразования

Под прямым и обратным матричным преобразованием (логическим дискретным преобразованием Фурье — ЛДПФ) понимают соответственно пару преобразований [4]:

$$\mathbf{C} = \mathbf{A}_{2^n}\mathbf{Y}, \qquad (10)$$

$$\mathbf{Y} = \mathbf{A}_{2^n}^{-1}\mathbf{C}, \qquad (11)$$

где $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ — соответственно матрицы прямого и инверсного арифметического преобразования размерности $2^n \times 2^n$ (базис преобразования); $\mathbf{Y}$ — вектор истинности d-выходной БФ $f(X)$ такой, что $\mathbf{Y} = [\mathbf{Y}_d \mid \mathbf{Y}_{d-1} \mid \mathbf{K} \mid \mathbf{Y}_1]^T = \left[Y^{(0)}\, Y^{(1)}\, \mathbf{K}\, Y^{(2^n-1)}\right]^T$, где T — символ транспонирования; $Y^{(i)}$ — числовое значение, принимаемое d-выходной БФ $f(X)$ на i-м наборе булевых аргументов обычной таблицы истинности (см. пример 1); $\mathbf{C} = \left[c_0 \quad c_1 \quad \mathbf{K} \quad c_{2^n-1}\right]^T$ — вектор коэффициентов АП (3) (арифметический спектр БФ). Матрица $\mathbf{A}_{2^n} = \begin{bmatrix} \mathbf{A}_{2^{n-1}} & 0 \\ -\mathbf{A}_{2^{n-1}} & \mathbf{A}_{2^{n-1}} \end{bmatrix}$ является n-й кронекеровской степенью $\mathbf{A}_{2^n} = \bigotimes_{j=1}^{n} \mathbf{A}_1$ базовой матрицы $\mathbf{A}_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$; $\mathbf{A}_{2^n}^{-1} = \bigotimes_{j=1}^{n} \mathbf{A}_1^{-1}$, где $\mathbf{A}_1^{-1} = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}$ — базовая матрица обратного преобразования. Матрица $-\mathbf{A}_{2^{n-1}}$ образуется из $\mathbf{A}_{2^{n-1}}$ заменой знаков единичных элементов на противоположные. Матричные преобразования хорошо алгоритмизируемы и удобны для практического применения.

Пример 5

Пусть задана трехвыходная БФ, векторы принимаемых значений, которой имеют вид:

$$\mathbf{Y}_1 = [01011011]^T,\ \ \mathbf{Y}_2 = [01100111]^T,\ \ \mathbf{Y}_3 = [01101001]^T.$$

Тогда

$$\mathbf{Y} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 7 \\ 6 \\ 1 \\ 5 \\ 2 \\ 3 \\ 7 \end{bmatrix}.$$

Выполняя прямое ЛДПФ (10), получим

$$\mathbf{C} = \mathbf{A}_{2^3} \cdot \mathbf{Y} = \left[\begin{array}{cccc:cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ \hdashline -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{array}\right] \cdot \begin{bmatrix} 0 \\ 7 \\ 6 \\ 1 \\ 5 \\ 2 \\ 3 \\ 7 \end{bmatrix} = \begin{bmatrix} 0 \\ 7 \\ 6 \\ -12 \\ 5 \\ -10 \\ -8 \\ 19 \end{bmatrix} \begin{matrix} \\ x_3 \\ x_2 \\ x_2x_3 \\ x_1 \\ x_1x_3 \\ x_1x_2 \\ x_1x_2x_3 \end{matrix}.$$

Из анализа структуры матриц $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ следует, что максимальное количество единичных элементов находится в последней строке обеих матриц. Причем количество единичных элементов с одинаковыми знаками в нижней строке матрицы $\mathbf{A}_{2^n}$ равно 2^{n-1}. Учитывая, что максимальное значение, принимаемое элементами матрицы $\mathbf{Y}$, равно $2^d - 1$ (d — количество реализуемых одновыходных БФ), можно сделать вывод о том, что в результирующей матрице $\mathbf{C}$ максимальное абсолютное значение может иметь коэффициент $abs\left(c_{2^n-1}\right) = 2^{n-1}\left(2^d - 1\right)$, где $abs(a)$ — абсолютная величина a. Для его представления в двоичной системе счисления с учетом необходимости представления знака числа потребуется

$$N_{\mathbf{C}} = \left\lfloor \log_2 (2^{n-1}(2^d - 1)) \right\rfloor + 2 = n + d \qquad (12)$$

двоичных разрядов ($\lfloor x \rfloor$ — наибольшее целое число, не превосходящее x).

Для линейных АП проблема больших коэффициентов является еще

более критичной. Однако в этом случае причиной большой величины коэффициентов является, прежде всего, большое количество реализуемых БФ, что в свою очередь вызвано необходимостью введения избыточных БФ, имеющих вспомогательный (служебный) характер.

3. Модулярные арифметико-логические формы

Одномодульной арифметикой будем называть арифметику кольца вычетов Z_m, где m — значение модуля. Наименьший неотрицательный вычет (в дальнейшем — вычет) целого числа N по модулю m будем обозначать как $\langle N \rangle_m^+$.

3.1. Полиномиальные модулярные арифметико-логические формы.

Теорема 2

Если $m > Y_{\max}$, где $Y_{\max}$ — максимальное значение, принимаемое Y, то произвольный кортеж БФ может быть представлен АП:

$$Y = m(X) = \left\langle \sum_{i=0}^{2^n-1} y_i x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n} \right\rangle_m^+, \qquad (13)$$

где $y_i = \langle c_i \rangle_m^+$, $\left(i = 0, 1, \mathbf{K}, 2^n - 1\right)$.

Замечание 1. В общем случае $m \geq 2^d$.

Определение 1. Выражение (13) будем называть представлением БФ $f(X)$ на основе модулярной формы АП или обобщенным АП Жегалкина.

Сравнительный анализ АП $D(X)$ и $m(X)$ можно выполнить на примере некоторых элементарных БФ (табл. 2).

Принцип реализации БФ на основе одномодульной арифметики поясняется с помощью блок-схемы, представленной на рис. 1.

Таблица 2.

$f(X)$	$D(X)$	$m(X)$
$\bar{x}_i$	$1-x_i$	$\langle 1+(m-1)x_i \rangle_m^+$
$x_1 \wedge x_2$	$x_1 x_2$	$x_1 x_2$
$x_1 \vee x_2$	$x_1 + x_2 - x_1 x_2$	$\langle x_1 + x_2 + (m-1)x_1 x_2 \rangle_m^+$
$x_1 \oplus x_2$	$x_1 + x_2 - 2x_1 x_2$	$\langle x_1 + x_2 + (m-2)x_1 x_2 \rangle_m^+$
$\overline{x_1 \wedge x_2}$	$1-x_1 x_2$	$\langle 1+(m-1)x_1 x_2 \rangle_m^+$
$\overline{x_1 \vee x_2}$	$1-x_1-x_2+x_1 x_2$	$\langle 1+(m-1)x_1+(m-1)x_2+x_1 x_2 \rangle_m^+$

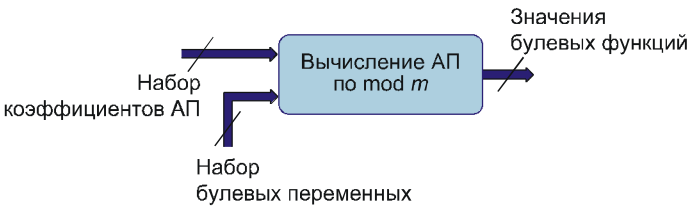

Рис. 1. Принцип реализации БФ на основе одномодульной арифметики

Следствие 1.

Коэффициенты АП $m(X)$ (13) лежат в области целых неотрицательных чисел, а их числовой диапазон равен значению модуля m.

Следствие 2.

Если для одной и той же системы БФ заданы два арифметических полинома $D(X)$ (3) и $m(X)$ (13), а K_1 и K_2 — количество членов этих полиномов, то $K_2 \le K_1$.

Для пояснения следствия 2 рассмотрим следующий пример.

Пример 6.

Вернемся к рассмотрению системы БФ (2), которой согласно выражению (3) (пример 2) соответствует АП:

$Y = D(X) = 3 - 3x_1 - 3x_2 + 4x_1x_2$. Применение теоремы 2 в общем случае дает: $Y = m(X) = \langle 3 + (m-3)x_1 + (m-3)x_2 + 4x_1x_2 \rangle_m^+$. При $m = 4$ получим $m(X) = \langle 3 + x_1 + x_2 \rangle_4^+$.

Таким образом, следствие 2 указывает на то, что модулярная форма АП (13) как минимум не усложняет полиномиальной формы представления систем БФ по показателям K_1 и K_2, а как максимум — позволяет уменьшить сложность АП за счет сокращения коэффициентов, кратных m. Следовательно, значение модуля m может выбираться не только по критерию собственной минимальности, но и по критерию минимальности K_2.

Лемма 1.

Если кортеж БФ (1) задан линейным АП (7), то при $m > U_{\max}$ справедлива модулярная форма линейного АП:

$$U = l(X) = \left\langle w_0 + \sum_{i=1}^{n} w_i x_i \right\rangle_m^+ = \langle w_0 + w_1 x_1 + \mathbf{K} + w_n x_n \rangle_m^+, \qquad (14)$$

где $w_j = \langle d_j \rangle_m^+ \ (j = 0, 1, \mathbf{K}, n)$.

Замечание 2. Значения параметра t оператора $\Xi^t\{U\}$ при переходе от (7) к (14) не изменяются.

Определение 2. Выражение (14) будем называть представлением БФ на основе модулярной формы линейного АП.

Пример 7.

Для системы БФ (8), заданной линейным АП (9), параметр t оператора $\Xi^t\{U\}$ имеет максимальное значение $t_{\max} = 6$ и $U_{\max} = 36$. Выберем $m = 2^6 > 36$. Тогда $U = \langle 20 + 60x_1 + 52x_2 + 16x_3 \rangle_{64}^+$.

Пусть $x_1x_2x_3 = (011)_2$. Следовательно, $U = \langle 88 \rangle_{64}^+ = (24)_{10} = (011000)_2$. Окончательно имеем:

$$f_A(X) = \Xi^2\{011000\} = 0,$$
$$f_B(X) = \Xi^4\{011000\} = 1,$$
$$f_C(X) = \Xi^6\{011000\} = 0.$$

Связь оператора $\Xi^t\{U\}$ с модулярной арифметикой устанавливается отношением: $\Xi^t\{U\} = \left\langle \left\lfloor \frac{U}{2^t} \right\rfloor \right\rangle_2^+$.

Замечание 3. Если для получения U используются избыточные БФ с номерами, превышающими $t_{\max}$ — максимальное значение параметра t оператора $\Xi^t\{U\}$, то модулю m можно присвоить значение $2^{t_{\max}}$. В этом случае вместо U в (14) следует писать $u = \langle U \rangle_{2^{t_{\max}}}^+$, при этом $u \le U$.

Таким образом основным свойством модулярной формы АП (13) является уменьшение числового диапазона, требуемого для его вычисления. Прежде чем сделать более точную оценку числового диапазона, рассмотрим принципы реализации *матричных* преобразований, основанных на модулярной арифметике.

3.2. Логические теоретико-числовые преобразования в базисе $\mathbf{A}_{2^n}$.

Теорема 3.

Если для d-выходной БФ $f(X)$ задана пара ЛДПФ (10) и (11) и $m > Y_{\max}$, где $Y_{\max}$ — максимальное значение, принимаемое Y, то справедлива следующая модулярная форма преобразований:

$$\mathbf{\Psi} = \left\langle \mathbf{A}_{2^n} \mathbf{Y} \right\rangle_m^+, \tag{15}$$

$$\mathbf{Y} = \left\langle \mathbf{A}_{2^n}^{-1} \mathbf{\Psi} \right\rangle_m^+, \tag{16}$$

где $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ — соответственно матрицы прямого и инверсного арифметического преобразования; $\mathbf{Y}$ и $\mathbf{\Psi}$ — соответственно вектор истинности БФ $f(X)$ и вектор коэффициентов модулярной формы АП $m(X)$ (13). Запись $\langle \cdot \rangle_m^+$, означает, что арифметические

операции, используемые при произведении матриц $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ на вектор-столбец $\mathbf{Y}$ или $\mathbf{\Psi}$, выполняются по модулю m.

Для доказательства теоремы 3 необходимо учесть взаимооднозначность связи между матричной (10), (11) и полиномиальной (3) формами представления системы БФ. Тогда справедливость (15) и (16) вытекает из справедливости (13).

Полученная пара преобразований имеет много общего с теоретико-числовыми преобразованиями (number theoretic transforms) методов ЦОС [16].

Определение 3. Преобразования (15) и (16) будем соответственно называть модулярной формой прямого и обратного матричного арифметического преобразования или логическими теоретико-числовыми преобразованиями (ЛТЧП, logical number theoretic transforms).

Учитывая, что $\langle -1 \rangle_m^+ = m-1$, выражение (15) можно переписать в другой форме:

$$\mathbf{\Psi} = \left\langle \mathbf{M}_{2^n} \mathbf{Y} \right\rangle_m^+, \qquad (17)$$

где $\mathbf{M}_{2^n} = \left\langle \mathbf{A}_{2^n} \right\rangle_m^+$. Запись $\left\langle \mathbf{A}_{2^n} \right\rangle_m^+$ означает, что отрицательные элементы (единицы) матрицы $\mathbf{A}_{2^n}$ заменяются на $m-1$.

Пример 8.

Продемонстрируем применение ЛТЧП (15) и (16) к двухвыходной БФ (2) с матрицей истинности, заданной табл. 1 (см. для сопоставления пример 2):

$$\mathbf{\Psi} = \left\langle \mathbf{A}_{2^2} \cdot \mathbf{Y} \right\rangle_{2^2}^+ = \left\langle \left[\begin{array}{c|c|c|c} 1 & 0 & 0 & 0 \\ \hline -1 & 1 & 0 & 0 \\ \hline -1 & 1 & 0 & 0 \\ \hline 1 & -1 & -1 & 1 \end{array}\right] \cdot \begin{bmatrix} 3 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\rangle_{2^2}^+ = \begin{bmatrix} 3 \\ 1 \\ 1 \\ 0 \end{bmatrix} \begin{matrix} \\ x_2 \\ x_1 \\ x_1 x_2 \end{matrix},$$

$$\mathbf{Y} = \left\langle \mathbf{A}_{2^2}^{-1} \cdot \mathbf{\Psi} \right\rangle_{2^2}^+ = \left\langle \left[\begin{array}{c|c|c|c} 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 \end{array}\right] \cdot \begin{bmatrix} 3 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\rangle_{2^2}^+ = \begin{bmatrix} 3 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Пример 9.

Применение прямого ЛТЧП (17) при $m = 2^3$ к трехвыходной БФ из примера 5 дает результат:

$$\boldsymbol{\Psi} = \left\langle \mathbf{M}_{2^3} \mathbf{Y} \right\rangle_{2^3}^{+} = \left\langle \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 7 & 7 & 1 & 0 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 7 & 0 & 0 & 7 & 1 & 0 & 0 \\ 1 & 0 & 7 & 0 & 7 & 0 & 1 & 0 \\ 7 & 1 & 1 & 7 & 1 & 7 & 7 & 1 \end{array}\right] \cdot \left[\begin{array}{c} 0 \\ 7 \\ 6 \\ 1 \\ 5 \\ 2 \\ 3 \\ 7 \end{array}\right] \right\rangle_{2^3}^{+} = \left[\begin{array}{cc} 0 & \\ 7 & x_3 \\ 6 & x_2 \\ 4 & x_2x_3 \\ 5 & x_1 \\ 6 & x_1x_3 \\ 0 & x_1x_2 \\ 3 & x_1x_2x_3 \end{array}\right].$$

По аналогии с ЛДПФ в качестве оценки сложности ЛТЧП выберем размер матрицы-спектра. Для представления элементов матрицы $\boldsymbol{\Psi}$ потребуется $N_{\boldsymbol{\Psi}} = \lceil \log_2 m \rceil$ ($\lceil x \rceil$ — наименьшее целое число равное или превышающее x) двоичных разрядов или, при $m = 2^d$, $N_{\boldsymbol{\Psi}} = d$ двоичных разрядов, что в

$$\frac{N_{\mathbf{C}}}{N_{\boldsymbol{\Psi}}} = \frac{n}{d} + 1 \qquad (18)$$

раз меньше по сравнению с количеством разрядов $N_{\mathbf{C}}$, необходимых для представления элементов матрицы $\mathbf{C}$ (12).

Так как $N_{\mathbf{C}}$ и $N_{\boldsymbol{\Psi}}$ — это максимальные размерности (количество двоичных разрядов) коэффициентов АП (3) и (13) соответственно, то оценка (18) применима и к АП (13).

На рис. 2. представлена геометрическая интерпретация получаемого выигрыша в виде представления матриц $\mathbf{Y}$, $\mathbf{C}$ и $\boldsymbol{\Psi}$ (здесь ширина матриц означает количество двоичных символов, необходимых для представления элементов матриц-столбцов, ПЛДПФ и ОЛДПФ — соответственно прямое и обратное ЛДПФ, а ПЛТЧП и ОЛТЧП — соответственно прямое и обратное ЛТЧП).

Однако этот выигрыш не удается сохранить для линейных АП, для которых числовой диапазон представления коэффициентов гарантированно можно уменьшить только в два раза — за счет переноса вычислений в область неотрицательных чисел. Препятствием для дальнейшего уменьшения, используемого числового диапазона является большая величина модуля m.

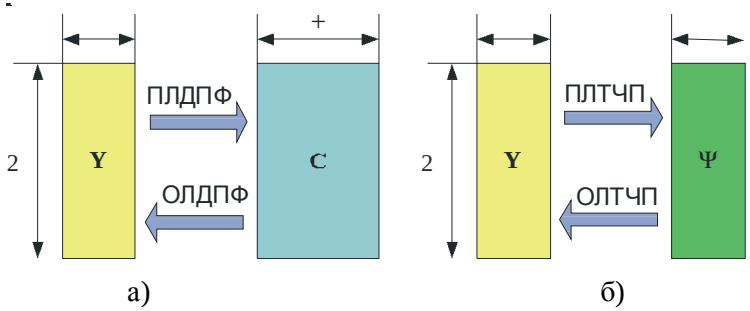

Рис. 2. Геометрическая интерпретация получаемого выигрыша

4. Модулярные арифметико-логические формы, основанные на Китайской теореме об остатках

При моделировании реальных цифровых устройств абсолютные значения коэффициентов линейных АП могут превышать величину 2^{100}. Поэтому требуется поиск более радикальных путей уменьшения используемых числовых диапазонов.

Пусть модуль m для (13) и (14) обладает свойством $m = \prod_{k=1}^{v} m_k$, причем $\gcd(m_i, m_j) = 1$; $i, j = 1, \mathbf{K}, v$; $i \neq j$ (здесь и далее $\gcd(a, b)$ — наибольший общий делитель a и b). Тогда в соответствии с Китайской теоремой об остатках Y можно взаимно однозначно отобразить в последовательность $\{Y\} = (f_1, f_2, \mathbf{K}, f_v)$, где $f_k = \langle Y \rangle_{m_k}^{+}$ $(k = 1, \mathbf{K}, v)$. При этом $Y \in Z_m$. Применение для каждого вычета f_k $(k = 1, \mathbf{K}, v)$ рассмотренного выше подхода позволяет получить следующие положения.

4.1. Полиномиальные модулярные арифметико-логические формы, основанные на Китайской теореме об остатках.

Теорема 4.

Если $m > Y_{\max}$, причем $m = \prod_{k=1}^{v} m_k$ и $\gcd(m_i, m_j) = 1$ $(i, j = 1, \mathbf{K}, v;\ i \neq j)$, то произвольный кортеж БФ может быть одно-

значно представлен системой модулярных форм АП:

$$\begin{cases} f_1 = m_1(X) = \left\langle \sum\limits_{i=0}^{2^n-1} y_{i,1} x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n} \right\rangle_{m_1}^{+}, \\ f_2 = m_2(X) = \left\langle \sum\limits_{i=0}^{2^n-1} y_{i,2} x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n} \right\rangle_{m_2}^{+}, \\ \mathbf{M} \\ f_v = m_v(X) = \left\langle \sum\limits_{i=0}^{2^n-1} y_{i,v} x_1^{i_1} x_2^{i_2} \mathbf{K}\, x_n^{i_n} \right\rangle_{m_v}^{+}, \end{cases} \qquad (19)$$

где $y_{i,k} = \langle c_i \rangle_{m_k}^{+} \quad (i = 0, 1, \mathbf{K}, 2^n - 1; \quad k = 1, \mathbf{K}, v)$.

Определение 4. Систему АП (19) будем называть полиномиальной формой представления БФ, основанной на Китайской теореме об остатках.

Замечание 4. Модулярные формы (19) и (13) связаны отношениями:

$$\{Y\} = (f_1, f_2, \mathbf{K}, f_v),$$

$$\left(y_{i,1}, y_{i,2}, \mathbf{K}, y_{i,v}\right) = \left\{y_i\right\} = \left|c_i\right|_m^{+} \quad \left(i = 0, 1, \mathbf{K}, 2^n - 1\right).$$

Для каждого АП системы (19) справедливы и следствия 1 и 2 (при этом вместо m необходимо рассматривать соответствующий модуль m_j $(j = 1, \mathbf{K}, v)$).

Лемма 2.

Если кортеж БФ (1) задан линейным АП $L(X)$ (7), то при $m > U_{\max}$, где $m = \prod_{k=1}^{v} m_k$, причем $\gcd(m_i, m_j) = 1$ $(i, j = 1, \mathbf{K}, v; \quad i \neq j)$, справедлива следующая модулярная форма линейного АП:

$$\begin{cases} f_1 = l_1(X) = \left\langle w_{0,1} + w_{1,1}x_1 + \mathbf{K} + w_{n,1}x_n \right\rangle_{m_1}^{+}, \\ f_2 = l_2(X) = \left\langle w_{0,2} + w_{1,2}x_1 + \mathbf{K} + w_{n,2}x_n \right\rangle_{m_2}^{+}, \\ \mathbb{M} \\ f_v = l_v(X) = \left\langle w_{0,v} + w_{1,v}x_1 + \mathbf{K} + w_{n,v}x_n \right\rangle_{m_v}^{+}, \end{cases} \qquad (20)$$

где $w_{j,k} = \left\langle d_j \right\rangle_{m_k}^{+} \quad (j = 0, 1, \mathbf{K}, n; \quad k = 1, 2, \mathbf{K}, v)$.

Справедливость (20) следует из применения доказательства справедливости (14) для каждого номера модуля (20) в отдельности и из Китайской теоремы об остатках.

Определение 5. Систему АП (20) будем называть линейной полиномиальной формой представления БФ, основанной на Китайской теореме об остатках.

Замечание 5. Модулярные формы (20) и (14) связаны отношениями:

$$\{U\} = (f_1, f_2, \mathbf{K}, f_v);$$

$$\left(w_{j,1}, w_{j,2}, \mathbf{K}, w_{j,v}\right) = \left\{w_i\right\} = \left\langle d_j \right\rangle_m^{+} \quad (j = 0, 1, \mathbf{K}, n).$$

Для упрощения изложения в дальнейшем не будем различать числа Y и U.

Решение системы равенств

$$\begin{cases} Y \equiv f_1 \pmod{m_1}, \\ Y \equiv f_2 \pmod{m_2}, \\ \mathbb{M} \\ Y \equiv f_v \pmod{m_v} \end{cases}$$

дает Китайская теорема об остатках. Для этого будем использовать запись

$$Y = \underset{k=1}{\overset{v}{\mathrm{CRT}}} f_k \pmod{m_k}. \qquad (21)$$

В современной трактовке Китайской теоремы об остатках для вычисления (21) используется формула

$$Y = \overset{v}{\underset{k=1}{\mathrm{CRT}}} f_k \pmod{m_k} = \langle f_1 B_1 + f_2 B_2 + \mathbf{K} + f_v B_v \rangle_m^+, \qquad (22)$$

где $B_k = q_k M m_k^{-1}$, q_k находится из сравнения $q_k M m_k^{-1} \equiv 1 \pmod{m_k}$ $(k = 1, \mathbf{K}, v)$ (здесь $a \equiv b \pmod{m_k}$ — a сравнимо с b по модулю m_k). Несмотря на классический вид формулы (22) она не всегда удобна для практического использования, в частности, из-за необходимости обеспечения большого числового диапазона. Более приемлемые для технической реализации формулы предложены в [16—19].

Примитивная блок-схема, поясняющая принцип реализации БФ посредством модулярных форм АП, основанных на Китайской теореме об остатках, представлена на рис. 3.

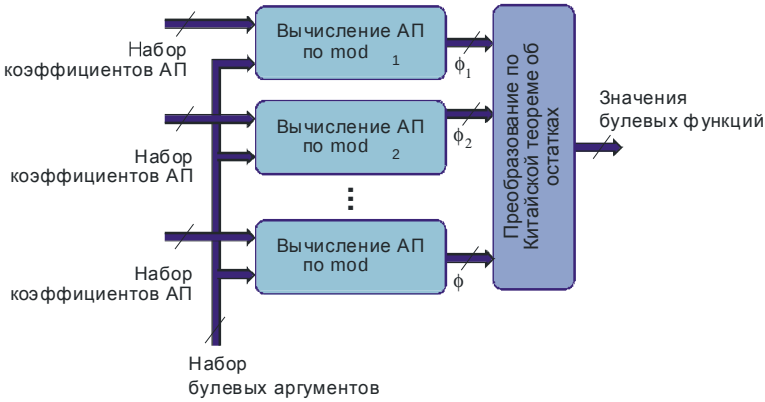

Рис. 3. Примитивная блок-схема принципа реализации БФ

4.2. Теоретико-числовые преобразования в базисе $\mathbf{A}_{2^n}$, основанные на Китайской теореме об остатках.

Лемма 3.

Если для d-выходной БФ $f(X)$ задана пара ЛТЧП (15) и (16) и $m > Y_{\max}$, причем $m = \prod_{k=1}^{v} m_k$ и $\gcd(m_i, m_j) = 1$ $(i, j = 1, \mathbf{K}, v;\ i \neq j)$, то справедлива следующая модулярная арифметико-логическая форма преобразований:

$$\begin{cases} \boldsymbol{\Psi}_1 = \left\langle \mathbf{A}_{2^n} \boldsymbol{\Phi}_1 \right\rangle_{m_1}^{+}, \\ \boldsymbol{\Psi}_2 = \left\langle \mathbf{A}_{2^n} \boldsymbol{\Phi}_2 \right\rangle_{m_2}^{+}, \\ \mathbb{M} \\ \boldsymbol{\Psi}_v = \left\langle \mathbf{A}_{2^n} \boldsymbol{\Phi}_v \right\rangle_{m_v}^{+}; \end{cases} \tag{23}$$

$$\begin{cases} \boldsymbol{\Phi}_1 = \left\langle \mathbf{A}_{2^n}^{-1} \boldsymbol{\Psi}_1 \right\rangle_{m_1}^{+}, \\ \boldsymbol{\Phi}_2 = \left\langle \mathbf{A}_{2^n}^{-1} \boldsymbol{\Psi}_2 \right\rangle_{m_2}^{+}, \\ \mathbb{M} \\ \boldsymbol{\Phi}_v = \left\langle \mathbf{A}_{2^n}^{-1} \boldsymbol{\Psi}_v \right\rangle_{m_v}^{+}, \end{cases} \tag{24}$$

где $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ — соответственно матрицы прямого и инверсного арифметического преобразования;

$$\boldsymbol{\Phi}_k = [f_k^{(0)}, f_k^{(1)}, \mathbf{K}, f_k^{(2^n-1)}]^T, \; f_k^{(r)} = \left\langle Y^{(i)} \right\rangle_{m_k}^{+}, \; k = 1, \mathbf{K}, v;$$

$$\boldsymbol{\Psi}_k = [y_{0,k}, y_{1,k}, \mathbf{K}, y_{2^n-1,k}]^T \quad (k = 1, \mathbf{K}, v).$$

Доказательство справедливости (23) и (24) следует 1) из взаимооднозначности связи матричной (10) и (11) и полиномиальной (3) форм представления БФ и 2) из доказательства справедливости полиномиальной формы представления (19), основанной на Китайской теореме об остатках.

Определение 6. Пару систем матричных преобразований (23) и (24) будем называть ЛТЧП, основанными на Китайской теореме об остатках (ЛТЧП КТО).

Замечание 6. ЛТЧП КТО (23) и (24) связаны с ЛТЧП (15) и (16) следующими отношениями

$$\boldsymbol{\Psi} = \operatorname*{CRT}_{k=1}^{v} \boldsymbol{\Psi}_k \pmod{m_k}, \qquad \mathbf{Y} = \operatorname*{CRT}_{k=1}^{v} \boldsymbol{\Phi}_k \pmod{m_k}.$$

На рис. 4 показана геометрическая интерпретация ЛТЧП КТО и его

взаимосвязь с ЛДПФ и ЛТЧП.

Согласно этой диаграмме смысл ЛТЧП КТО сводится к разложению каждой из матриц **Y** и **C** на v матриц меньшей «ширины» — $l_1, l_2, \mathbf{K}, l_v$, где $l_k = \lceil \log_2 m_k \rceil$, что позволяет упростить преобразование для каждой из полученных матриц $\mathbf{\Psi}_k$ или $\mathbf{\Phi}_k$ $(k = 1, 2, \mathbf{K}, v)$ в отдельности. Полученные результаты затем восстанавливаются с помощью Китайской теоремы об остатках. При этом спектр $\mathbf{\Psi}$ является матрицей ЛТЧП по модулю $m = \prod_{k=1}^{v} m_k$.

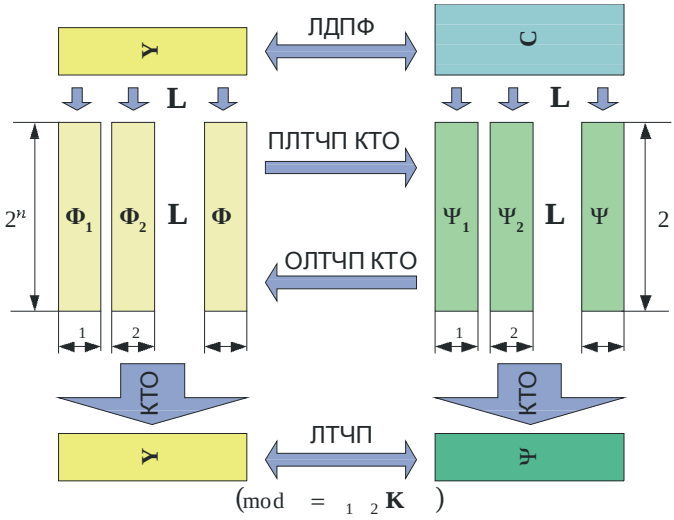

Рис. 4. Геометрическая интерпретация ЛТЧП КТО

5. Заключение

Основы вычислительных методов алгебры логики, используемые в настоящее время, были созданы в «докомпьютерную» эпоху и *плохо согласуются* с методами организации вычислений в современной компьютерной технике. Напротив, арифметическая логика полностью *соответствует* принципам построения современных и перспективных ЭВМ и позволяет раскрыть неиспользуемый в настоящее время потенциал вычислительной техники по реализации высокопроизводительных, гибких, параллельных логических вычислений.

Модулярные арифметико-логические формы (общая классификация представлена на рис. 5) обладают рядом новых полезных свойств и ориентированы на *воплощение в современную и перспективную практику цифровой обработки информации идей арифметической логики* на основе высокоразвитого и прогрессивного научно-методического аппарата модулярной арифметики.

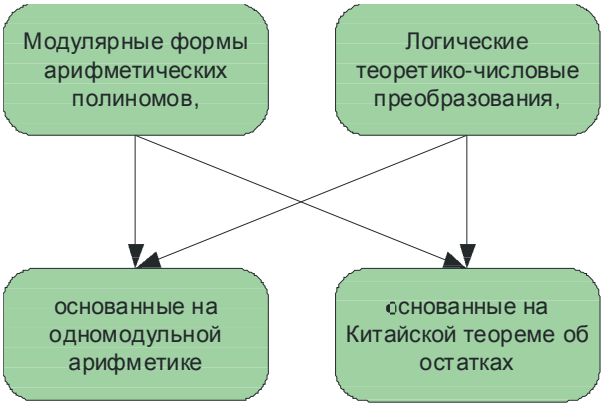

Рис. 5. Общая классификация модулярных арифметико-логических форм

Достоинствами модулярных арифметико-логических форм являются:

- высокая степень *параллелизма* логических вычислений, которая может быть классифицирована как сверхпараллелизм;
- уникальные возможности по обеспечению *отказоустойчивости* и *живучести* средств логических вычислений;
- обеспечение *контроля* и *коррекции* ошибок на всех стадиях обработки, хранения, а также передачи информации;
- создание благоприятных условий для приоритетного использования быстродействующих *табличных* операционных устройств (в том числе на базе программируемой логики) за счет существенного уменьшения (по сравнению с двоичной системой счисления — на порядки) объема таблиц;
- уменьшение *сложности* представления логических функций на основе АП;
- возможность *многоцелевого* использования средств логических

вычислений, которая, в свою очередь, может быть использована для обеспечения отказоустойчивости и живучести вычислительной системы или для сокращения аппаратурных затрат за счет разделения решения задач во времени;

- реализация широкого класса логических алгоритмов, в том числе и нейросетевых алгоритмов (пороговый элемент представим одним линейным АП, система пороговых элементов (слой) — это система логический функций, поэтому также представима одним линейным АП).

В настоящее время модулярная арифметика широко применяется в методах и средствах ЦОС. Модулярные арифметико-логические формы позволяют *задействовать* высокоразвитый математический аппарат и совершенные технические средства ЦОС, базирующиеся на методах модулярной арифметики, для высококачественной реализации параллельных логических вычислений. В настоящей работе даны основы построения безызбыточных модулярных арифметико-логических форм. Принципы обеспечения контроля ошибок логических вычислений и построения отказоустойчивых вычислительных структур (в классе логических алгоритмов) даны в [5]. Обобщение модулярных арифметико-логических форм на многозначные логические функции дано в [5, 13, 14].

Таким образом, модулярные арифметико-логические формы, повидимости, позволяют преодолеть важное *противоречие* двух основных способов реализации логических алгоритмов: *программного* (гибкого) и *аппаратного* (жесткого). Логические вычисления, обладающие достоинствами программной реализации, становится возможным реализовать специализированными вычислительными средствами, характеризующимися требуемым комплексом технических характеристик.

Литература

1. *Малюгин В. Д.* Параллельные логические вычисления посредством арифметических полиномов. — М.: Наука. Физматлит, 1997.
2. *Малюгин В. Д.* Реализация булевых функций арифметическими полиномами. — Автоматика и телемеханика. 1982. №4. С. 84–93.

3. *Малюгин В. Д.* Реализация кортежей булевых функций посредством линейных арифметических полиномов. — Автоматика и телемеханика. 1984. № 2. С. 114–121.

4. *Шмерко В. П.* Синтез арифметических форм булевых функций посредством преобразования Фурье. — Автоматика и телемеханика. 1989. № 5. С. 134–142.

5. *Финько О. А.* Модулярная арифметика параллельных логических вычислений: Монография / Под. ред. В.Д. Малюгина. — М.: ИПУ РАН, 2003. 214 с.

6. *Финько О. А.* Реализация систем булевых функций большой размерности методами модулярной арифметики. — Автоматика и телемеханика. 2004. № 6. С. 37–60.

7. *Финько О. А.* Вариант классификации арифметических форм представления логических функций. — XIV Междунар. школа-семинар «Синтез и сложность управляющих систем». Н. Новгород, 27 октября — 1 ноября 2003. Сборник трудов / Под ред. академика РАН О.Б. Лупанова. — Н. Новгород: Изд-во Нижегородского педагогического ун-та, 2003. С. 83–84.

8. *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. Трапезникова РАН, Москва, 16–20 июня 2003.

9. *Финько О. А.* Модулярные формы арифметических полиномов для реализации систем булевых функций. — Тр. Междунар. конф. «Искусственные интеллектуальные системы» (IEEE AIS'03) и «Интеллектуальные САПР» (CAD-2003). — М.: Наука. Физматлит, 2003. С. 548–560.

10. *Финько О. А.* Параллельные логические вычисления методами модулярной арифметики. — II Междунар. конф. «Параллельные вычисления и задачи управления» (PACO–2004). Москва, 4–6 октября 2004. Сборник трудов. — М.: Ин-т проблем управ. им. В.А. Трапезникова РАН, 2004. 88 с.

11. *Финько О. А.* Сверхпараллельные логические вычисления методами модулярной арифметики. — Тр. Междунар. конф. «Искусственные интеллектуальные системы» (IEEE AIS'02) и «Интеллектуальные САПР» (CAD-2002). — М.: Наука. Физматлит, 2002. С. 448–455.

12. *Finko O. A.* Methods of problem-oriented representation and data processing in resources of the hardware support of intellectual systems. — Proc. IEEE Conf. Artificial Intelligence Syst. (AIS'02). September 5–10, 2002. P. 453–454. (in USA).

13. *Финько О. А.* Полиномиальная арифметика функций многозначной логики. — Известия вузов. Приборостроение. 2004. Т. 47, № 5. С. 41–46.

14. *Финько О. А.* Модулярные формы *k*-значных функций алгебры логики. — Автоматика и телемеханика. 2005. № 7.

15. *Шмерко В. П.* Теоремы Малюгина: новое понимание в логическом управлении, проектировании СБИС и структурах данных для новых технологий. — Автоматика и телемеханика. 2004. № 6. С. 6–36.

16. *Норден П., Китте К.* Алгебраическая алгоритмика: Пер. с франц. — М.: Мир, 1999.

17. *Червяков Н. И., Коршунов 0. Е., Финько О. А.* Преобразователь кода системы остаточных классов в позиционный код. А.с. № 1343553. — Б.И. 1987. № 37. С. 288.

18. *Червяков Н.И., Коршунов О. Е., Финько О. А.* Преобразователь кода из системы остаточных классов в позиционный код. А.с. № 1388996. — Б.И. 1988. № 14. С. 167.

19. *Финько О. А.* Восстановление числа в системе остаточных классов с минимальным количеством оснований. — Электронное моделирование. 1998. Т. 20. № 3. С. 56–61. / *Finko O. A.* Number Restoration In the System of Residual Classes With a Minimum Number of Radices. — Engineering Simulation. 1999. V. 16. P. 329–334 (in