Автоматика и телемеханика, № 6, 2004

© 2004 г. **О. А. ФИНЬКО, канд. техн. наук**
(Краснодар)

РЕАЛИЗАЦИЯ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ БОЛЬШОЙ РАЗМЕРНОСТИ МЕТОДАМИ МОДУЛЯРНОЙ АРИФМЕТИКИ

Вводятся модулярные полиномиальные и спектральные арифметико-логические формы представления булевых функций, которые позволяют получить ряд полезных свойств, связанных с ограничением числового диапазона (решением проблемы больших коэффициентов арифметических полиномов) при реализации параллельных логических вычислений.

1. Введение

При решении задач синтеза и анализа дискретных устройств, построения систем логического управления сложными техническими объектами и процессами реального времени 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 [1].

Ключ к решению этого противоречия дают методы реализации булевых функций арифметическими полиномами, устанавливающие фундаментальную взаимосвязь между логическими и арифметическими типами данных [1–3]. В ряде работ предприняты усилия к расширению классов арифметико-логических форм булевых функций на основе представления булевых функций в спектральной области [4–7]. 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 булевых функций.

Ряд важных преимуществ, связанных с ограничением числового диапазона представления результатов промежуточных вычислений, а также распараллеливанием вычислений позволяют получить модулярные преобразования [8–10]. В настоящей статье рассматриваются особенности построения модулярных арифметических форм представления булевых функций, которые позволят распространить преимущества модулярной арифметики на область логических вычислений. Для этого в разделе 2 приводятся сведения о представлении систем булевых функций посредством арифметических полиномов и основные методы их получения, которые затем взяты за основу построения модулярных арифметико-логических форм в разделах 3 и 4. При этом в разделе 3 вводятся модулярные арифметико-логические формы, основанные на одномодульной арифметике, а в разделе 4 обсуждаются модулярные арифметико-логические формы, основанные на многомодульной арифметике (Китайской теореме об остатках – Chinese remainder theorem – CRT).

2. Представление систем булевых функций посредством арифметических полиномов. Постановка задачи

2.1. Теорема о представлении системы булевых функций одним арифметическим полиномом

Пусть дана d-выходная булева функция $f(X)$ (система булевых функций – $f_1(X)$, $f_2(X)$, ..., $f_d(X)$) от n переменных $X = x_1, x_2, \ldots, x_n$:

$$(1) \qquad \begin{cases} y_1 = f_1(X), \\ \vdots \\ y_d = f_d(X), \end{cases}$$

где y_j – значение, принимаемое j-й булевой функцией $f_j(X)$; $x_i, y_j \in \{0, 1\}$ $(i = 1, \ldots, n; j = 1, \ldots, d)$. При этом кортеж значений булевых функций $y_d * y_{d-1} * \ldots * y_1$, где $*$ – разделительный знак, интерпретируется как код целого неотрицательного числа Y, представленного в двоичной системе счисления:

$$y_d * y_{d-1} * \ldots * y_1 = Y = \sum_{j=1}^{d} y_j 2^{j-1}.$$

Пример 1. Представление Y, соответствующее системе булевых функций

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

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_2	x_1	y_2	y_1	Y (десятичная запись)
0	0	1	1	3
0	1	0	0	0
1	0	0	0	0
1	1	0	1	1

Теорема 1 ([1–3]). *Произвольный кортеж булевых функций $f_d(X) * f_{d-1}(X) * \ldots * f_1(X)$ может быть представлен арифметическим полиномом*

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

где здесь и далее по тексту статьи

$$i_1 i_2 \ldots i_n = \sum_{u=1}^{n} i_u 2^{n-u}, \quad i_u \in \{0, 1\};$$

$$x_u^{i_u} = \begin{cases} x_u, & i_u = 1, \\ 1, & i_u = 0; \end{cases} \qquad c_i \in Z \quad (i = 0, 1, \ldots, 2^n - 1)$$

и притом единственным образом.

2.2. Алгебраический метод получения арифметического полинома. Линейные арифметические полиномы

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

Алгоритм 1.

Шаг 1. Получение арифметического полинома $P_j(X)$ для каждой булевой функции $y_j = f_j(X)$, $j = 1, \ldots, d$:

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

Шаг 2. Получение арифметических полиномов, взвешенных весами 2^{j-1} ($j = 1, \ldots, d$):

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

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

Шаг 3. Получение искомого арифметического полинома $D(X)$ (3) путем суммирования коэффициентов арифметического полинома $P'_j(X)$ для всех $j = 1, \ldots, d$:

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

где $c_i = \sum\limits_{j=1}^{d} r'_{j,i}$ ($i = 0, 1, \ldots, 2^n - 1$).

Пример 2. Для системы булевых функций (2) реализация алгоритма 1 имеет вид.

Шаг 1. Используя соотношения

$$\begin{aligned}
&x_1 \wedge x_2 = x_1 x_2,\\
&x_1 \vee x_2 = x_1 + x_2 - x_1 x_2,\\
&x_1 \oplus x_2 = x_1 + x_2 - 2x_1 x_2,\\
&\overline{x} = 1 - x,
\end{aligned}$$

получим

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

Шаг 2.

$$\begin{aligned}
P'_1(X) &= 2^0(1 - x_1 - x_2 + 2x_1 x_2) = 1 - x_1 - x_2 + 2x_1 x_2,\\
P'_2(X) &= 2^1(1 - x_1 - x_2 + x_1 x_2) = 2 - 2x_1 - 2x_2 + 2x_1 x_2.
\end{aligned}$$

Шаг 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 арифметических полиномов, может значительно превосходить числовой диапазон, достаточный для представления Y. В рассмотренном случае для представления Y достаточно двух двоичных разрядов ($0 \le Y \le 2^2 - 1$). В то же время для представления коэффициентов $c_1 \dots c_4$ арифметического полинома требуются четыре двоичных разряда ($-3 \le c_{1\dots4} \le 5$), а результаты промежуточных вычислений при $x_1 = x_2 = 1$ могут принимать значения от -6 до 7.

Большое значение для представления d-выходных булевых функций $f(X)$ имеют линейные арифметические полиномы $L(X)$, которые определяются выражением

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

где коэффициенты $d_0, d_1, \ldots, d_n$ – целые числа [1, 11, 12].

При вычислении $f_j(X)$ используется оператор маскирования $\Xi^t\{U\}$ [11, 12], служащий для определения t-го двоичного разряда (выхода) представления $U = a_r 2^{r-1} + \ldots + a_t 2^{t-1} + \cdots + a_2 2^1 + a_1 2^0$, т.е. $\Xi^t\{U\} = a_t$.

Пример 3. Для линеаризации арифметического полинома $P_j(X) = x_1 + x_2 - x_1 x_2$, соответствующего булевой функции $f_j(X) = x_1 \vee x_2$, используется введение дополнительной (избыточной) булевой функции $f_j^{(1)}(X)$. При этом образуется система булевых функций:

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

Тогда $U = L(X) = 2^1 f_j^{(2)}(X) + 2^0 f_j^{(1)}(X) = 1 + x_1 + x_2$ и $f_j(X) = \Xi^2\{U\}$ [11].

Таким образом, для представления систем булевых функций (1) с помощью линейных арифметических полиномов $L(X)$ используется тот же принцип взвешивания представлений булевых функций с помощью весов 2^i ($i = 0, 1, \ldots$), что и при построении арифметических полиномов $D(X)$ (3). Однако значения i при этом выбираются с учетом введенных дополнительных булевых функций.

Пример 4 ([11]). Дана система булевых функций:

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

Для обеспечения линейности результирующего арифметического полинома добавляют вспомогательные булевы функции $f_A^{(1)}(X)$, $f_B^{(3)}(X)$, $f_C^{(5)}(X)$ и получают систему булевых функций:

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

Далее в соответствии с (7) и примером 3 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 арифметический полином:

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

Для определения t-й булевой функции 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 арифметического полинома (9) достигнута за счет введения избыточных булевых функций 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 [1, 6, 12]:

$$\mathbf{C} = \mathbf{A}_{2^n}\mathbf{Y}, \tag{10}$$

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

где $\mathbf{A}_{2^n}$ и $\mathbf{A}^{-1}_{2^n}$ – соответственно матрицы прямого и инверсного арифметического преобразования размерности $2^n \times 2^n$ (базис преобразования); $\mathbf{Y}$ – вектор истинности d-выходной булевой функции $f(X)$ такой, что $\mathbf{Y} = [\mathbf{Y}_d \,|\, \mathbf{Y}_{d-1} \,|\, \ldots \,|\, \mathbf{Y}_1]^{\mathrm{T}} = \left[Y^{(0)}Y^{(1)}\ldots Y^{(2^n-1)}\right]^{\mathrm{T}}$, где T – символ транспонирования; $Y^{(i)}$ – числовое значение, принимаемое d-выходной булевой функцией $f(X)$ на i-м наборе булевых аргументов обычной таблицы истинности (см. пример 1); $\mathbf{C} = [c_0\ c_1\ \ldots\ c_{2^n-1}]^{\mathrm{T}}$ – вектор коэффициентов арифметического полинома (3) или арифметический спектр булевой функции.

Матрица $\mathbf{A}_{2^n} = \left[\begin{array}{c|c} \mathbf{A}_{2^{n-1}} & 0 \\ \hline -\mathbf{A}_{2^{n-1}} & \mathbf{A}_{2^{n-1}} \end{array}\right]$ является n-й кронекеровской степенью $\mathbf{A}_{2^n} = \bigotimes_{j=1}^{n} \mathbf{A}_1$ базовой матрицы $\mathbf{A}_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$; $\mathbf{A}^{-1}_{2^n} = \bigotimes_{j=1}^{n} \mathbf{A}_1^{-1}$, где $\mathbf{A}_1^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ – 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 булева функция, векторы принимаемых значений, которой имеют вид:

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

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

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

Из этого примера видно, что значения вектора коэффициентов $\mathbf{C}$ лежат в интервале $-28 \le c_i \le 28$. 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 булевых функций), можно сделать вывод о том, что в результирующей матрице $\mathbf{C}$ максимальное абсолютное значение может иметь коэффициент $abs(c_{2^n-1}) = 2^{n-1}(2^d - 1)$, где $abs(a)$ – абсолютная величина a. Для его представления в двоичной системе счисления с учетом необходимости представления знака числа потребуется

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

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

Для линейных арифметических полиномов проблема больших коэффициентов является еще более критичной. Однако в этом случае причиной большой величины коэффициентов является, прежде всего, большое количество реализуемых булевых функций, что в свою очередь вызвано необходимостью введения избыточных булевых функций, имеющих вспомогательный (служебный) характер.

2.4. Задача исследований

Из теории цифровой обработки сигналов известно, что ряд преимуществ, связанных с ограничением числового диапазона представления промежуточных результатов преобразования, позволяют достичь методы модулярной арифметики [13–15]. В связи с этим рассмотрим применение методов модулярных преобразований с целью ослабления “проблемы больших коэффициентов” арифметических полиномов.

3. Модулярные арифметико-логические формы

3.1. Полиномиальные модулярные арифметико-логические формы

Одномодульной арифметикой будем называть арифметику кольца вычетов Z_m, где m – значение модуля [8–10]. Наименьший неотрицательный вычет (в дальнейшем – вычет) целого числа N по модулю m будем обозначать как $|N|_m^+$.

Теорема 2. Если $m > Y_{\max}$, где $Y_{\max}$ – максимальное значение, принимаемое Y, то произвольный кортеж булевых функций может быть представлен арифметическим полиномом:

$$Y = \mu(X) = \left| \sum_{i=0}^{2^n-1} \psi_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+, \tag{13}$$

где $\psi_i = |c_i|_m^+$ $(i = 0, 1, \dots, 2^n - 1)$.

Доказательство теоремы 2 и принципы построения алгоритмов получения (13) приведены в Приложении.

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

Определение 1. Выражение (13) *будем называть представлением булевой функции $f(X)$ на основе модулярной формы арифметического полинома.*

Сравнительный анализ арифметических полиномов $D(X)$ и $\mu(X)$ можно выполнить на примере некоторых элементарных булевых функций (табл. 2).

Таблица 2

$f(X)$	$D(X)$	$\mu(X)$
x_i	$1 - x_i$	$\|1 + (m-1)x_i\|_m^+$
$x_1 \wedge x_2$	$x_1 x_2$	$x_1 x_2$
$x_1 \vee x_2$	$x_1 + x_2 - x_1 x_2$	$\|x_1 + x_2 + (m-1)x_1 x_2\|_m^+$
$x_1 \oplus x_2$	$x_1 + x_2 - 2x_1 x_2$	$\|x_1 + x_2 + (m-2)x_1 x_2\|_m^+$
$x_1 \wedge x_2$	$1 - x_1 x_2$	$\|1 + (m-1)x_1 x_2\|_m^+$
$x_1 \vee x_2$	$1 - x_1 - x_2 + x_1 x_2$	$\|1 + (m-1)x_1 + (m-1)x_2 + x_1 x_2\|_m^+$

Принцип реализации булевых функций на основе одномодульной арифметики поясняется с помощью блок-схемы, представленной на рис. 1 (здесь и далее АП – арифметический полином).

Следствие 1. Коэффициенты арифметического полинома $\mu(X)$ (13) *лежат в области целых неотрицательных чисел, а их числовой диапазон равен значению модуля m.*

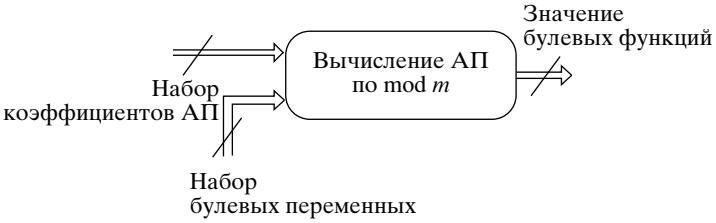

Рис. 1.

Следствие 2. Если для одной и той же системы булевых функций заданы два арифметических полинома $D(X)$ (3) и $\mu(X)$ (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 булевых функций (2), которой согласно выражению (3) (пример 2) соответствует арифметический полином

$$Y = D(X) = 3 - 3x_1 - 3x_2 + 4x_1x_2.$$

Применение теоремы 2 в общем случае дает:

$$Y = \mu(X) = |3 + (m-3)x_1 + (m-3)x_2 + 4x_1x_2|_m^+.$$

При $m = 4$ получим

$$\mu(X) = |3 + x_1 + x_2|_4^+.$$

Таким образом, следствие 2 указывает на то, что модулярная форма арифметического полинома (13) как минимум не усложняет полиномиальной формы представления систем булевых функций по показателям K_1 и K_2, а как максимум – позволяет уменьшить сложность арифметических полиномов 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 булевых функций (1) *задан линейным арифметическим полиномом* (7), *то при $m > U_{\max}$ справедлива модулярная форма линейного арифметического полинома:*

$$U = \lambda(X) = \left|\omega_0 + \sum_{i=1}^{n} \omega_i x_i\right|_m^+ = |\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n|_m^+, \tag{14}$$

где $\omega_j = |d_j|_m^+$ $(j = 0, 1, \ldots, n)$.

Доказательство леммы 1 приведено в Приложении.

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

Определение 2. Выражение (14) *будем называть представлением булевой функции на основе модулярной формы линейного арифметического полинома.*

Пример 7. Для системы булевых функций (8), заданной линейным арифметическим полиномом (9), параметр t оператора $\Xi^t\{U\}$ имеет максимальное значение $t_{\max} = 6$ и $U_{\max} = 36$. Выберем $m = 2^6 > 36$. Тогда

$$U = |20 + 60x_1 + 52x_2 + 16x_3|_{64}^+.$$

Пусть $x_1x_2x_3 = 011$. Следовательно, $U = |88|_{64}^+ = 24_{\text{dec}} = 011000$. 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:

$$\Xi^t\{U\} = \left|\left\lfloor \frac{U}{2^t} \right\rfloor\right|_2^+.$$

Замечание 3. Если для получения U используются избыточные булевы функции 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 $u = |U|^+_{2^{t_{\max}}}$, при этом $u \le U$.

Для пояснения замечания 3 рассмотрим следующий пример.

Пример 8. Для системы булевых функций

$$f_A(X) = \overline{x_1 \wedge x_2 \wedge x_3} = \Xi^3\{6 - x_1 - x_2 - x_3\},$$
$$f_B(X) = \overline{x_1 \oplus x_2 \oplus x_3} = \Xi^1\{1 + x_1 + x_2 + x_3\}$$

линейный арифметический полином $L(X)$ имеет вид:

$$U = 2^3 f_B(X) + 2^0 f_A(X) = 14 + 7x_1 + 7x_2 + 7x_3.$$

Так как $t_{\max} = 4$, то в соответствии с замечанием 3 получим $m = 16$ и

$$u = \lambda(X) = |14 + 7x_1 + 7x_2 + 7x_3|^+_{16}.$$

Пусть $x_1x_2x_3 = 111$, тогда $u = |35|^+_{16} = 2_{\text{dec}} = 0010$ и

$$f_A(X) = \Xi^3\{0010\} = 0,$$
$$f_B(X) = \Xi^4\{0010\} = 0.$$

То есть вместо шести разрядов, необходимых для представления U в соответствии с (7) и (14), замечание 3 позволяет обойтись только четырьмя разрядами.

Таким образом, основным свойством модулярной формы арифметического полинома (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 булевой функции $f(X)$ задана пара ЛДПФ (10) *и* (11) *и $m > Y_{\max}$, где $Y_{\max}$ – максимальное значение, принимаемое Y, то справедлива следующая модулярная форма преобразований:*

$$\mathbf{\Psi} = \mathbf{A}_2\mathbf{Y} (\bmod m), \tag{15}$$

$$\mathbf{Y} = \mathbf{A}^{-1}_{2^n}\mathbf{\Psi} (\bmod m), \tag{16}$$

где $\mathbf{A}_{2^n}$ и $\mathbf{A}^{-1}_{2^n}$ – соответственно матрицы прямого и инверсного арифметического преобразования; $\mathbf{Y}$ и $\mathbf{\Psi}$ – соответственно вектор истинности булевой функции $f(X)$ и вектор коэффициентов модулярной формы арифметического полинома $\mu(X)$ (13). *Запись $\bmod m$ означает, что арифметические операции, используемые при произведении матриц $\mathbf{A}_{2^n}$ и $\mathbf{A}^{-1}_{2^n}$ на вектор-столбец $\mathbf{Y}$ или $\mathbf{\Psi}$, выполняются по модулю m.*

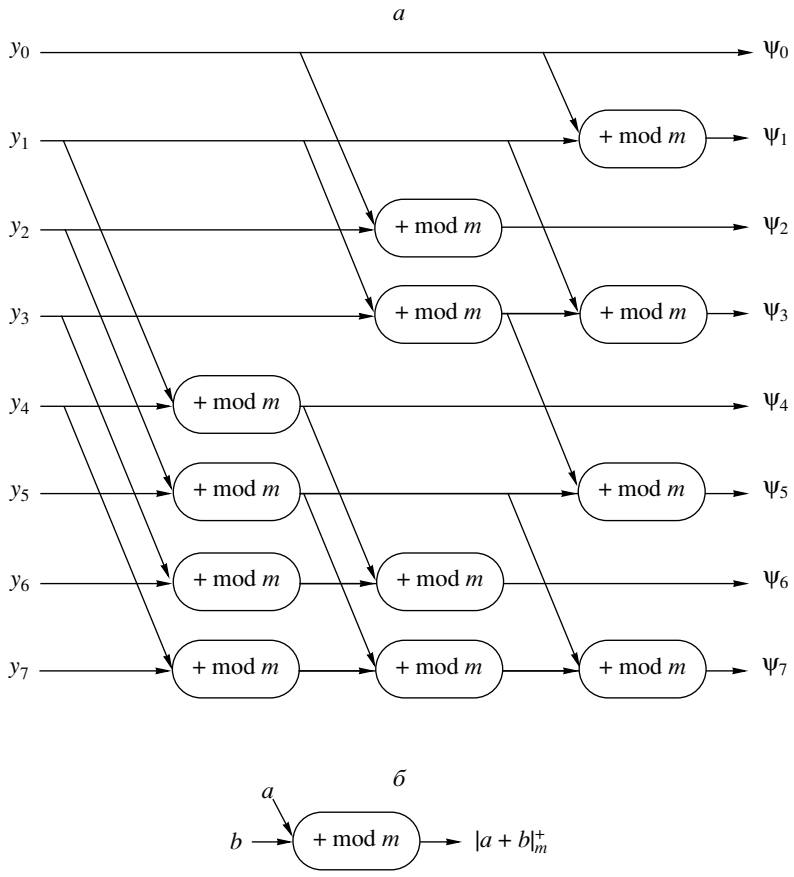

Рис. 2.

Для доказательства теоремы 3 необходимо учесть взаимооднозначность связи между матричной (10), (11) и полиномиальной (3) формами представления системы булевых функций [1]. Тогда справедливость (15) и (16) вытекает из справедливости (13).

Полученная пара преобразований имеет много общего с теоретико-числовыми преобразованиями (number theoretic transforms) методов цифровой обработки сигналов [13–15].

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 $|-1|_m^+ = m-1$, выражение (15) можно переписать в другой форме:

$$\mathbf{\Psi} = \mathbf{M}_{2^n}\mathbf{Y}(\bmod m), \tag{17}$$

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

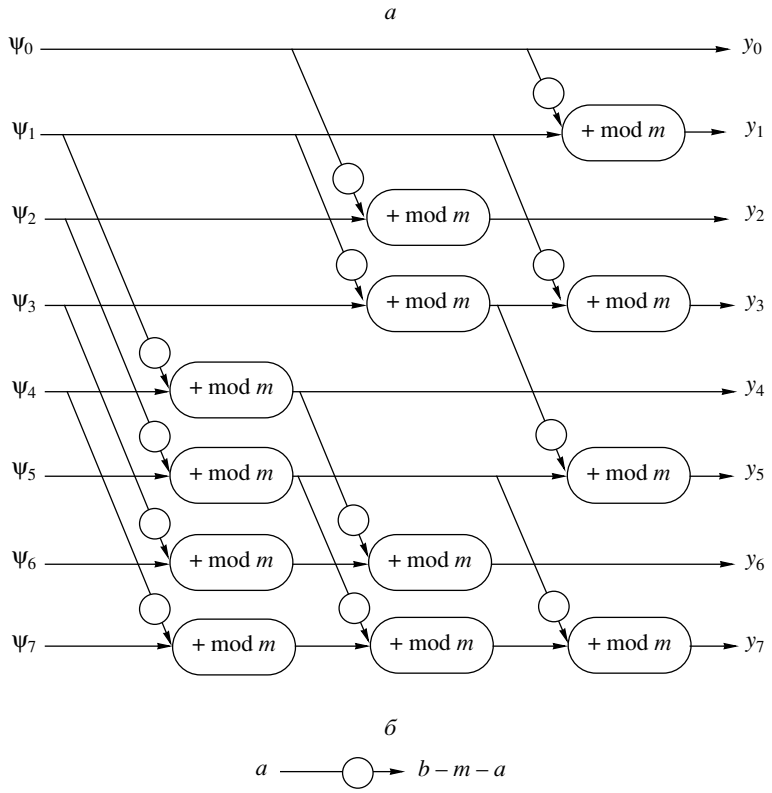

Рис. 3.

Принципы реализации прямого и обратного ЛТЧП (15) и (16) можно пояснить с помощью графов (соответственно рис. 2 и 3), структура которых аналогична структурам графов матричных преобразований, предложенных Малюгиным в [1]. Из этих графов видно, что 1) в обоих преобразованиях применяются операции модулярного сложения; 2) все результаты промежуточных преобразований неотрицательны и не превышают значения модуля m; 3) для уменьшения вычислительных затрат к (15) и (16) могут быть применены методы факторизации матриц $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$, предложенные в [1]. При этом ожидается снижение вычислительной сложности преобразования в $\xi = (3^n - 2^n)\,/(n2^{n-1})$ раз [1].

Пример 9. Продемонстрируем применение ЛТЧП (15) и (16) к двухвыходной булевой функции (2) с матрицей истинности, заданной табл. 1 (см. для сопоставления пример 2):

$$\mathbf{\Psi} = \mathbf{A}_{2^2}\mathbf{Y}(\bmod 2^2) = \left[\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ \hdashline -1 & 1 & 0 & 0 \\ 1 & -1 & -1 & 1 \end{array}\right] \left[\begin{array}{c} 3 \\ 0 \\ 0 \\ 1 \end{array}\right] (\bmod 2^2) = \left[\begin{array}{c} 3 \\ 1 \\ 1 \\ 0 \end{array}\right] \begin{array}{l} \\ x_2 \\ x_1 \\ x_1x_2 \end{array},$$

$$\mathbf{Y} = \mathbf{A}_{2^2}^{-1}\mathbf{\Psi}(\bmod 2^2) = \left[\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hdashline 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{array}\right] \left[\begin{array}{c} 3 \\ 1 \\ 1 \\ 0 \end{array}\right] (\bmod 2^2) = \left[\begin{array}{c} 3 \\ 0 \\ 0 \\ 1 \end{array}\right].$$

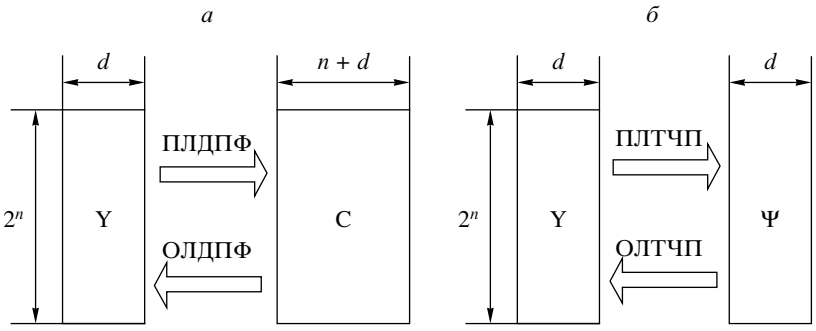

Рис. 4.

Пример 10. Применение прямого ЛТЧП (17) при $m = 2^3$ к трехвыходной булевой функции из примера 5 дает результат:

$$\mathbf{\Psi} = \mathbf{M}_{2^3}\mathbf{Y}(\bmod 2^3) = \left[\begin{array}{cccc:cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 7 & 7 & 1 & 0 & 0 & 0 & 0 \\ \hdashline 7 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 7 & 0 & 0 & 7 & 1 & 0 & 0 \\ 1 & 0 & 7 & 0 & 7 & 0 & 1 & 0 \\ 7 & 1 & 1 & 7 & 1 & 7 & 7 & 1 \end{array}\right] \left[\begin{array}{c} 0 \\ 7 \\ 6 \\ 1 \\ 5 \\ 2 \\ 3 \\ 7 \end{array}\right] (\bmod 2^3) = \left[\begin{array}{c} 0 \\ 7 \\ 6 \\ 4 \\ 5 \\ 6 \\ 0 \\ 3 \end{array}\right] \begin{array}{c} \\ x_3 \\ x_2 \\ x_2x_3 \\ x_1 \\ x_1x_3 \\ x_1x_2 \\ x_1x_2x_3 \end{array} .$$

Таким образом, значения коэффициентов вектора $\mathbf{\Psi}$ лежат в интервале $0 \le \psi_i < 8$, $i = 0, 1, \ldots, 2^3 - 1$ (в общем случае – $0 \le \psi_i < m$, $i = 0, 1, \ldots, 2^n - 1$), который сохраняется и при выполнении промежуточных вычислений (сравним с $-28 \le c_i \le 28$ в примере 5).

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

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

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

Так как $N_{\mathbf{C}}$ и $N_{\mathbf{\Psi}}$ – это максимальные размерности (количество двоичных разрядов) коэффициентов арифметических полиномов (3) и (13) соответственно, то оценка (18) применима и к арифметическому полиному (13).

На рис. 4. представлена геометрическая интерпретация получаемого выигрыша в виде представления матриц $\mathbf{Y}$, $\mathbf{C}$ и $\mathbf{\Psi}$ (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 арифметических полиномов, для которых числовой диапазон представления коэффициентов гарантированно можно уменьшить только в два раза – за счет переноса вычислений в область неотрицательных чисел (в некоторых случаях может быть использовано также замечание 3). Препятствием для дальнейшего уменьшения используемого числового диапазона является большая величина модуля m.

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

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

При моделировании реальных цифровых устройств абсолютные значения коэффициентов линейных арифметических полиномов могут превышать величину 2^{100} [11, 12]. 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 $\gcd(m_i, m_j) = 1$; $i, j = 1, \ldots, v$; $i \neq j$ (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 $\{Y\} = (\phi_1, \phi_2, \ldots, \phi_v)$, где $\phi_k = |Y|^{+}_{m_k}$ $(k = 1, \ldots, v)$ [8–10]. При этом $Y \in Z_m$. Применение для каждого вычета ϕ_k $(k = 1, \ldots, v)$ рассмотренного выше подхода позволяет получить следующие положения.

Теорема 4. Если $m > Y_{\max}$, *причем* $m = \prod\limits_{k=1}^{v} m_k$ *и* $\gcd(m_i, m_j) = 1$ $(i, j = 1, \ldots$ $\ldots, v;\ i \neq j)$, *то произвольный кортеж булевых функций может быть однозначно представлен системой модулярных форм арифметических полиномов:*

$$(19) \qquad \begin{cases} \phi_1 = \mu_1(X) = \left| \sum\limits_{i=0}^{2^n-1} \psi_{i,1} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|^{+}_{m_1}, \\ \phi_2 = \mu_2(X) = \left| \sum\limits_{i=0}^{2^n-1} \psi_{i,2} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|^{+}_{m_2}, \\ \vdots \\ \phi_v = \mu_v(X) = \left| \sum\limits_{i=0}^{2^n-1} \psi_{i,v} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \right|^{+}_{m_v}, \end{cases}$$

где $\psi_{i,k} = |c_i|^{+}_{m_k}$ $(i = 0, 1, \ldots, 2^n - 1;\ k = 1, \ldots, v)$.

Доказательство теоремы 4 и принципы построения алгоритмов получения (19) приведены в Приложении.

Определение 4. Систему арифметических полиномов (19) *будем называть полиномиальной формой представления булевых функций, основанной на Китайской теореме об остатках.*

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

$$\{Y\} = (\phi_1, \phi_2, \ldots, \phi_v),$$
$$(\psi_{i,1}, \psi_{i,2}, \ldots, \psi_{i,v}) = \{\psi_i\} = |c_i|^{+}_{m} \quad (i = 0, 1, \ldots, 2^n - 1).$$

Для каждого арифметического полинома системы (19) справедливы и следствия 1 и 2 (при этом вместо m необходимо рассматривать соответствующий модуль m_j $(j = 1, \ldots, v)$).

Лемма 2. Если кортеж булевых функций (1) *задан линейным арифметическим полиномом* $L(X)$ (7), *то при* $m > U_{\max}$, *где* $m = \prod_{k=1}^{v} m_k$, *причем* $\gcd(m_i, m_j) = 1$ $(i, j = 1, \ldots, v;\ i \neq j)$, *справедлива следующая модулярная форма линейного арифметического полинома:*

$$(20) \qquad \begin{cases} \phi_1 = \lambda_1(X) = |\omega_{0,1} + \omega_{1,1}x_1 + \cdots + \omega_{n,1}x_n|^{+}_{m_1}, \\ \phi_2 = \lambda_2(X) = |\omega_{0,2} + \omega_{1,2}x_1 + \cdots + \omega_{n,2}x_n|^{+}_{m_2}, \\ \vdots \\ \phi_v = \lambda_v(X) = |\omega_{0,v} + \omega_{1,v}x_1 + \cdots + \omega_{n,v}x_n|^{+}_{m_v}, \end{cases}$$

где $\omega_{j,k} = |d_j|^{+}_{m_k}$ $(j = 0, 1, \ldots, n;\ k = 1, 2, \ldots, v)$.

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

Определение 5. Систему арифметических полиномов (20) *будем называть линейной полиномиальной формой представления булевых функций, основанной на Китайской теореме об остатках.*

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

$$\{U\} = (\phi_1, \phi_2, \ldots, \phi_v);$$
$$(\omega_{j,1}, \omega_{j,2}, \ldots, \omega_{j,v}) = \{\omega_i\} = |d_j|^{+}_{m} \quad (j = 0, 1, \ldots, n).$$

Замечание 3 к (20) не применимо.

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

Решение системы равенств

$$\begin{cases} Y = \phi_1 (\bmod m_1), \\ Y = \phi_2 (\bmod m_2), \\ \vdots \\ Y = \phi_v (\bmod m_v) \end{cases}$$

дает Китайская теорема об остатках. Для этого будем использовать запись

$$(21) \qquad Y = \mathop{\mathbf{CRT}}_{k=1}^{v} \phi_k \ (\bmod m_k).$$

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

$$(22) \qquad Y = \mathop{\mathbf{CRT}}_{k=1}^{v} \phi_k (\bmod m_k) = |\phi_1 B_1 + \phi_2 B_2 + \ldots + \phi_v B_v|^{+}_{m},$$

где $B_k = q_k M m_k^{-1}$, q_k находится из сравнения $q_k M m_k^{-1} \equiv 1 (\bmod m_k)$ $(k = 1, \ldots, v)$ (здесь $a \equiv b (\bmod m_k)$ – a сравнимо с b по модулю m_k).

Пример 11. Рассмотрим линейный арифметический полином [11]:

$$Y = L(X) = 8 + 137x_1 - 7x_2 + 129x_3 + 136x_4 + 64x_5,$$

реализующий систему булевых функций:

$$f_1(X) = x_1 \oplus x_2 \oplus x_3,$$
$$f_2(X) = x_1 \oplus \overline{x}_2 \oplus x_3,$$
$$f_3(X) = x_5,$$
$$f_4(X) = x_1 \oplus x_3 \oplus x_4.$$

Причем

$$f_1(X) = \Xi^1\{Y\},$$
$$f_2(X) = \Xi^4\{Y\},$$
$$f_3(X) = \Xi^7\{Y\},$$
$$f_4(X) = \Xi^8\{Y\}.$$

Так как $t_{\max} = 8$ и $Y_{\max} = 474$, выберем модули $m_1 = 7$, $m_2 = 8$, $m_3 = 9$, обеспечивающие выполнение условия $m = m_1 m_2 m_3 = 504 > 474$. Тогда согласно (20):

$$\begin{cases} \lambda_1(X) = |1 + 4x_1 + 3x_3 + 3x_4 + x_5|_7^+, \\ \lambda_2(X) = |x_1 + x_2 + x_3|_8^+, \\ \lambda_3(X) = |8 + 2x_1 + 2x_2 + 3x_3 + x_4 + x_5|_9^+. \end{cases}$$

Пусть $x_1x_2x_3x_4x_5 = 10011$. Тогда

$$\begin{cases} \lambda_1(X) = 2, \\ \lambda_2(X) = 1, \\ \lambda_3(X) = 3. \end{cases}$$

Используя формулу (22) и учитывая, что $B_1 = 288$, $B_2 = 441$, $B_3 = 280$, получим

$$Y = |2 \times 288 + 1 \times 441 + 3 \times 280|_{504}^+ = |1857|_{504}^+ = 345_{\text{dec}} = 101011001.$$

Несмотря на классический вид формулы (22), она не всегда удобна для практического использования, в частности, из-за необходимости обеспечения большого числового диапазона.

Теорема 5 ([16–18][1]). *Целое неотрицательное число* $Y < m = \prod_{k=1}^{v} m_k$, *представленное вычетами* $\phi_1, \phi_2, \ldots, \phi_v$ *по системе попарно простых модулей* $m_1 < m_2 < \ldots < m_v$ *может быть однозначно восстановлено посредством рекурсии*

$$\text{(23)} \qquad \begin{cases} h_1 = \phi_2, \\ h_2 = m_1 \left|\delta_1|\phi_1 - h_2|_{M_1}^+\right|_{M_1}^+ + \phi_1, \\ h_3 = m_3 \left|\delta_2|\phi_3 - h_2|_{M_2}^+\right|_{M_2}^+ + \phi_3, \\ h_4 = m_4 \left|\delta_3|\phi_4 - h_3|_{M_3}^+\right|_{M_3}^+ + \phi_4, \\ \vdots \\ h_v = Y = m_v \left|\delta_{v-1}|\phi_v - h_{v-1}|_{M_{v-1}}^+|_{M_{v-1}}^+\right|_{M_{v-1}}^+ + \phi_v, \end{cases}$$

где

$$M_1 = m_2, \quad M_i = \prod_{j=1}^{i} m_j;$$
$$\delta_1 = \left|(M_1 - m_1)^{-1}\right|_{M_1}^+, \quad \delta_i = \left|(M_i - m_{i+1})^{-1}\right|_{M_i}^+.$$

[1] Позднее (после [16]) подобные результаты были опубликованы в [19].

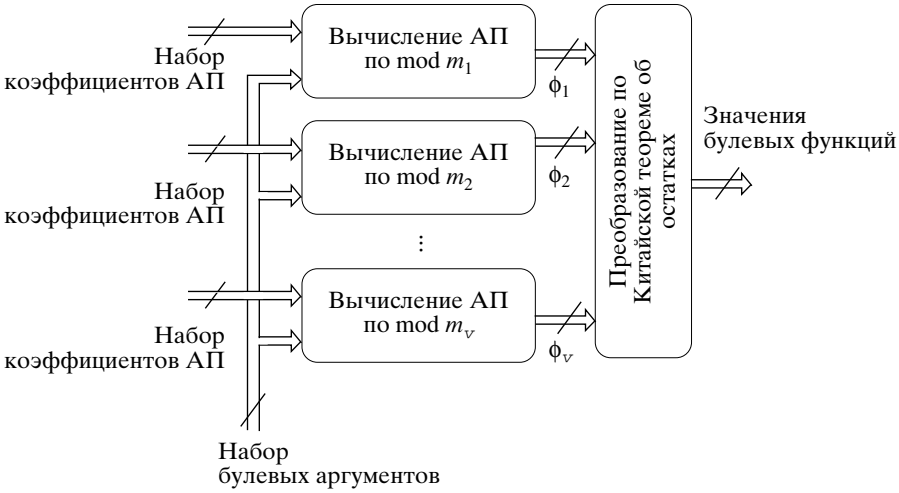

Рис. 5.

Доказательство справедливости (23) основано на обобщении случая теоремы 5 для двух модулей [17, 18] путем поэтапного перехода к составным модулям и укрупнения числового диапазона.

Для получения Y с помощью (23) потребуется v шагов. При этом промежуточные результаты не выходят за пределы диапазона M_v. При обеспечении возможности распараллеливания вычислений возможен вариант теоремы 5, позволяющий получить $\lceil \log_2 v \rceil$ шагов преобразования [17, 18].

Примитивная блок-схема, поясняющая принцип реализации булевых функций посредством модулярных форм арифметических полиномов, основанных на Китайской теореме об остатках, представлена на рис. 5.

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

Лемма 3. Если для d-выходной булевой функции $f(X)$ задана пара ЛТЧП (15) *и* (16) *и $m > Y_{\max}$, причем $m = \prod_{k=1}^{v} m_k$ и $\gcd(m_i, m_j) = 1$ $(i, j = 1, \ldots, v;\ i \neq j)$, то справедлива следующая модулярная арифметико-логическая форма преобразований:*

$$(24)\qquad \begin{cases} \mathbf{\Psi}_1 = \mathbf{A}_{2^n}\mathbf{\Phi}_1(\bmod m_1), \\ \mathbf{\Psi}_2 = \mathbf{A}_{2^n}\mathbf{\Phi}_2(\bmod m_2), \\ \vdots \\ \mathbf{\Psi}_v = \mathbf{A}_{2^n}\mathbf{\Phi}_v(\bmod m_v); \end{cases}$$

$$(25)\qquad \begin{cases} \mathbf{\Phi}_1 = \mathbf{A}_{2^n}^{-1}\mathbf{\Psi}_1(\bmod m_1), \\ \mathbf{\Phi}_2 = \mathbf{A}_{2^n}^{-1}\mathbf{\Psi}_2(\bmod m_2), \\ \vdots \\ \mathbf{\Phi}_v = \mathbf{A}_{2^n}^{-1}\mathbf{\Psi}_v(\bmod m_v); \end{cases}$$

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

$$\mathbf{\Phi}_k = \left[\phi_k^{(0)}, \phi_k^{(1)}, \ldots, \phi_k^{(2^n-1)}\right]^{\mathrm{T}}, \quad \phi_k^{(r)} = \left|Y^{(i)}\right|_{m_k}^{+}, \quad k = 1, \ldots, v;$$
$$\mathbf{\Psi}_k = [\psi_{0,k}, \psi_{1,k}, \ldots, \psi_{2^n-1,k}]^{\mathrm{T}} \quad (k = 1, \ldots, v).$$

Справедливость (24) и (25) следует: 1) из взаимооднозначности связи матричной (10) и (11) и полиномиальной (3) форм представления булевых функций [1] и 2) из доказательства справедливости полиномиальной формы представления (19), основанной на Китайской теореме об остатках.

Определение 6. Пару систем матричных преобразований (24) *и* (25) *будем называть ЛТЧП, основанными на Китайской теореме об остатках (ЛТЧП КТО).*

Замечание 6. ЛТЧП КТО (24) и (25) связаны с ЛТЧП (15) и (16) следующими отношениями

$$\mathbf{\Psi} = \underset{k=1}{\overset{v}{\mathbf{CRT}}}\, \mathbf{\Psi}(\bmod m_k),$$
$$\mathbf{Y} = \underset{k=1}{\overset{v}{\mathbf{CRT}}}\, \mathbf{\Phi}_k(\bmod m_k).$$

Пример 12. Рассмотрим пару ЛТЧП КТО применительно к условиям, используемым в примерах 5 и 10. При этом выберем значения модулей $m_1 = 3$ и $m_2 = 5$, что должно обеспечить числовой диапазон $M = m_1 m_2 = 15 \geq 2^3$. Тогда

$$|\mathbf{Y}|_3^+ = \left|\begin{bmatrix} 0&0&0\\1&1&1\\1&1&0\\0&0&1\\1&0&1\\0&1&0\\0&1&1\\1&1&1 \end{bmatrix}\right|_3^+ = \left|\begin{bmatrix} 0\\7\\6\\1\\5\\2\\3\\7 \end{bmatrix}\right|_3^+ = \begin{bmatrix} 0\\1\\0\\1\\2\\2\\0\\1 \end{bmatrix};$$

$$|\mathbf{Y}|_5^+ = \left|\begin{bmatrix} 0&0&0\\1&1&1\\1&1&0\\0&0&1\\1&0&1\\0&1&0\\0&1&1\\1&1&1 \end{bmatrix}\right|_5^+ = \left|\begin{bmatrix} 0\\7\\6\\1\\5\\2\\3\\7 \end{bmatrix}\right|_5^+ = \begin{bmatrix} 0\\2\\1\\1\\0\\2\\3\\2 \end{bmatrix}.$$

Преобразование (24) примет вид:

$$\mathbf{\Psi}_1 = \mathbf{A}_{2^3}\mathbf{\Phi}_1(\bmod 3) = \mathbf{A}_{2^3}[0\,1\,0\,1\,2\,2\,0\,1]^{\mathrm{T}}(\bmod 3) = [0\,1\,0\,0\,2\,2\,1\,1]^{\mathrm{T}},$$
$$\mathbf{\Psi}_2 = \mathbf{A}_{2^3}\mathbf{\Phi}_2(\bmod 5) = \mathbf{A}_{2^3}[0\,2\,1\,1\,0\,2\,3\,2]^{\mathrm{T}}(\bmod 5) = [0\,2\,1\,3\,0\,0\,2\,4]^{\mathrm{T}},$$

Для получения Y используем (23) для случая двух модулей [17, 18, 20]:

$$Y^{(i)} = m_1\left|\delta_1|\phi_1^{(i)} - \phi_2^{(i)}|_{m_2}^{+}\right|_{m_2}^{+} + \phi_1^{(i)} = 2\left|2|\phi_1^{(i)} - \phi_2^{(i)}|_5^{+}\right|_5^{+} + \phi_1^{(i)}, \quad i = 0, 1, \ldots, 2^n - 1.$$

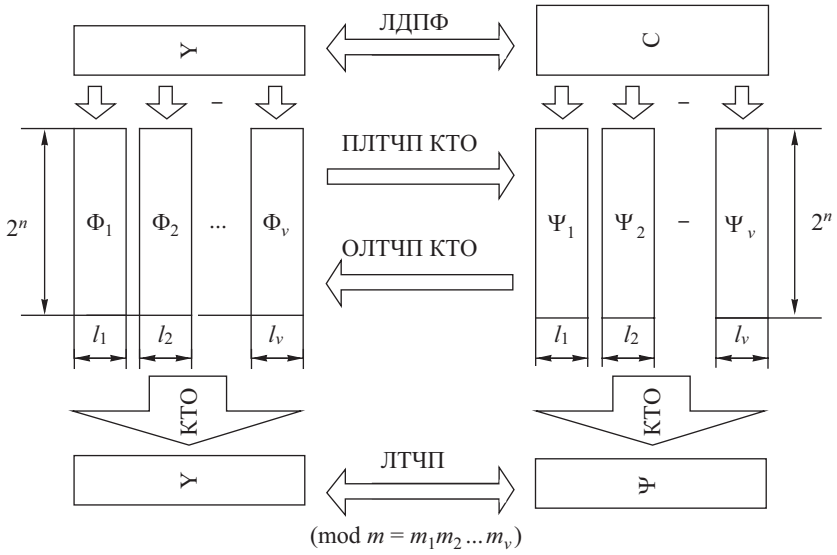

Рис. 6.

В результате получим:

$$
\begin{aligned}
Y^{(0)} &= 2\left|2|0-0|_5^+\right|_5^+ + 0 = 0,\\
Y^{(1)} &= 2\left|2|1-2|_5^+\right|_5^+ + 1 = 7,\\
Y^{(2)} &= 2\left|2|0-1|_5^+\right|_5^+ + 0 = 6,\\
Y^{(3)} &= 2\left|2|1-1|_5^+\right|_5^+ + 1 = 1,\\
Y^{(4)} &= 2\left|2|2-0|_5^+\right|_5^+ + 2 = 5,\\
Y^{(5)} &= 2\left|2|2-2|_5^+\right|_5^+ + 2 = 2,\\
Y^{(6)} &= 2\left|2|0-3|_5^+\right|_5^+ + 0 = 3,\\
Y^{(7)} &= 2\left|2|1-2|_5^+\right|_5^+ + 1 = 7.
\end{aligned}
$$

Таким образом:

$$
\begin{aligned}
\mathbf{\Psi} &= \underset{k=1}{\overset{2}{\mathbf{CRT}}}\left[\psi_{0,k}, \psi_{1,k}, \ldots, \psi_{2^3-1,k}\right]^{\mathrm{T}} (\bmod m_k) = [0\,7\,6\,8\,5\,0\,2\,9]^{\mathrm{T}},\\
\mathbf{Y} &= \underset{k=1}{\overset{2}{\mathbf{CRT}}}[\phi_{0,k}, \phi_{1,k}, \ldots, \phi_{2^3-1,k}]^{\mathrm{T}} (\bmod m_k) = [0\,7\,6\,1\,5\,2\,3\,7]^{\mathrm{T}}.
\end{aligned}
$$

Структура графов матричных преобразований для каждого номера k модуля m_k ЛТЧП КТО аналогична структурам графов, представленным на рис. 2 и рис. 3. Следовательно, к ЛТЧП КТО применимы методы факторизации матриц $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ (методы быстрых конъюнктивных преобразований), применимые и к ЛДПФ [1] и ЛТЧП.

На рис. 6 показаны геометрическая интерпретация ЛТЧП КТО и его взаимосвязь с ЛДПФ и ЛТЧП.

Таблица 3

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}	m_{11}	m_{12}	m_{13}	m_{14}	m_{15}	m_{16}	m_{17}
67	71	73	79	83	89	91	97	101	103	107	109	111	113	115	127	128

Согласно этой диаграмме смысл ЛТЧП КТО сводится к разложению каждой из матриц $\mathbf{Y}$ и $\mathbf{C}$ на v матриц меньшей "ширины" – $\ell_1, \ell_2, \ldots, \ell_v$, где $\ell_k = \lceil \log_2 m_k \rceil$, что позволяет упростить преобразование для каждой из полученных матриц $\mathbf{\Psi}_k$ или $\mathbf{\Phi}_k$ $(k = 1, 2, \ldots, v)$ в отдельности. Полученные результаты затем восстанавливаются с помощью Китайской теоремы об остатках. При этом спектр $\mathbf{\Psi}$ является матрицей ЛТЧП по модулю $m = \prod_{k=1}^{v} m_k$.

Будем исходить из предположения, что преобразования для всех модулей ЛТЧП КТО выполняются параллельно. Тогда наибольшую сложность будет иметь преобразование ЛТЧП КТО для наибольшего модуля m_v. Максимальная "ширина" (необходимое количество двоичных разрядов для представления элементов матрицы) соответствует матрице $\mathbf{\Psi}_v$ по наибольшему модулю m_v и составит $\ell_v = \lceil \log_2 m_v \rceil$ двоичных разрядов. Учитывая, что для большинства практических задач значение ℓ_v не превышает $6 \div 7$, выигрыши в сравнении с ЛДПФ ЛТЧП соответственно составят

$$\frac{N_{\mathbf{C}}}{\ell_v} \approx \frac{n+d}{6 \div 7} \quad \text{и} \quad \frac{N_{\mathbf{\Psi}}}{\ell_v} \approx \frac{d}{6 \div 7} \text{ раз.}$$

Например, при $n = d = 40$ и $m_v = 128$ выигрыши будут соответственно 11,4 и 5,7 раз. Для восстановления окончательного результата в соответствии с (23) потребуется v итераций. Например, набор из 17 модулей (табл. 3) обеспечивает представление коэффициентов арифметического полинома (3) или (7) с верхней границей (округляя до наименьшей степени числа 2) 2^{105}.

Полученные оценки сохраняют силу и для модулярных форм полиномиальных преобразований, основанных на Китайской теореме об остатках. При этом для сравнения с линейными арифметическим полиномом необходимо использовать отношение $\dfrac{d^*}{6 \div 7}$, где d^* – общее количество (с учетом избыточных) реализуемых булевых функций или максимальное количество разрядов, необходимых для представления коэффициентов полинома. Относительно $d^* = 2^{100}$ линейного арифметического полинома выигрыш в количестве используемых двоичных разрядных цифр в пределах одного канала (модуля) преобразования составит 14,3 раза.

5. Заключение

Классификация предложенных модулярных форм представления булевых функций показана на рис. 7, согласно которой наряду с модулярными формами арифметических полиномов (нелинейных и линейных) впервые рассмотрены логические теоретико-числовые преобразования.

Главное преимущество модулярных форм представления булевых функций, основанных на одномодульной арифметике, – уменьшение числового диапазона представления промежуточных результатов преобразований, которое достигается как за счет ограничения величины коэффициентов (и их сумм) арифметических полиномов значением модуля преобразования (преимущественно для нелинейных арифметических полиномов), так и за счет перевода коэффициентов в область положительных чисел. Однако для линейных арифметических полиномов одномодульная арифметика не позволяет получить заметных преимуществ. Радикальное уменьшение

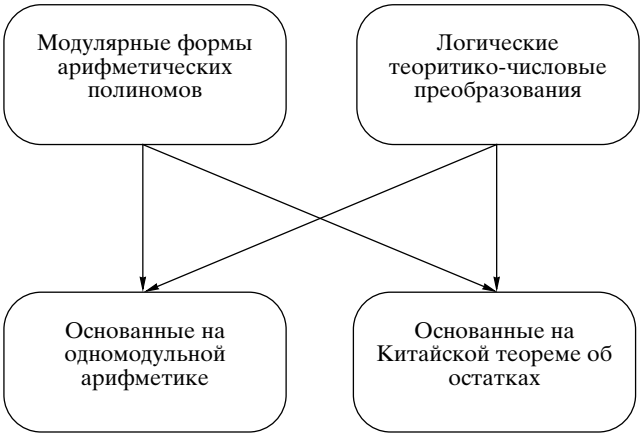

Рис. 7.

требуемого числового диапазона позволяет получить модулярные формы представления булевых функций, основанные на Китайской теореме об остатках, которые наиболее эффективны для реализации больших систем булевых функций (больших значениях d) при больших значениях коэффициентов арифметических полиномов ($2^{100} \div 2^{1000}$ и более). Рассмотрен вариант Китайской теоремы об остатках для восстановления числа по его остаткам, удовлетворяющий требованиям минимальности используемого числового диапазона. Однако эти преимущества имеют силу только при организации параллельных вычислений для групп или всех используемых модулей преобразования. Это обстоятельство хотя и сужает область применения данных форм, однако позволяет использовать развитый аппарат и средства цифровой обработки сигналов для реализации интенсивных логических вычислений.

Можно ожидать, что еще более высокую эффективность рассмотренные методы могут дать при реализации функций алгебры многозначной логики за счет ускорения выполнения операций умножения. При этом их можно рассматривать как методы вычисления функций k-значной логики для произвольных значений k программными или аппаратурными средствами с другими заданными значностями логики (значениями модулей). Дальнейшим направлением исследований также может быть использование модулярных форм для организации контроля ошибок при логических вычислениях [21].

Основные результаты этой статьи апробированы и одобрены на Международных конференциях [18, 22–26].

ПРИЛОЖЕНИЕ

Доказательство теоремы 2. Рассмотрим два варианта доказательств, которые определят два варианта алгоритма получения (13).

а. Пусть дан арифметический полином $D(x)$ (3). Тогда согласно теории сравнений [27] справедливо:

$$(\text{П.1}) \qquad |Y|_m^+ = \left| \sum_{i=0}^{2^n-1} c_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+ = \left| \sum_{i=0}^{2^n-1} |c_i|_m^+ \, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+ .$$

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

$$(\text{П.2}) \qquad Y = \left| \sum_{i=0}^{2^n-1} |c_i|_m^+ \, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+ = \left| \sum_{i=0}^{2^n-1} \psi_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+, \quad \text{где} \quad \psi_i = |c_i|_m^+.$$

Теорема доказана.

Из этого доказательства вытекает алгоритм получения (13), заключающийся в выполнении следующих шагов:

Шаг 1. Построение (3) посредством алгоритма 1.

Шаг 2. Определение (13) посредством выражения (П.2).

б. Так как $f_j(X) \in \{0, 1\}$ и $m > Y$ с учетом предыдущих рассуждений, полином (4) можно представить в виде:

$$(\text{П.3}) \qquad f_j(X) = \mu'_j(X) = \left| \sum_{i=0}^{2^n-1} \psi'_{j,i} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+, \quad j = 1, \dots, d,$$

где $\psi'_{j,i} = |r_{j,i}|_m^+$ ($j = 1, \dots, d$; $i = 0, 1, \dots, 2^n - 1$). Далее приведением (5) и (6) по модулю m получим:

$$(\text{П.4}) \qquad \mu''_j(X) = \sum_{i=0}^{2^n-1} \psi''_{j,i} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad j = 1, \dots, d,$$

где $\psi''_{j,i} = |\psi'_{j,i} b_j|_m^+$, $b_j = |2^{j-1}|_m^+$ ($j = 1, \dots, d$; $i = 0, 1, \dots, 2^n - 1$);

$$(\text{П.5}) \qquad Y = \mu(X) = \left| \sum_{i=0}^{2^n-1} \left| \sum_{j=1}^{d} \psi''_{j,i} \right|_m^+ x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+ = \left| \sum_{i=0}^{2^n-1} \psi_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right|_m^+.$$

Теорема доказана.

Таким образом, второй вариант алгоритма получения (13) состоит в выполнении трех шагов, заключающихся соответственно в построении (П.3), (П.4) и (П.5).

Доказательство леммы 1. Рассмотрим арифметический полином

$$U = \left| \omega_0^* + \sum_{i=1}^{s} \omega_i^* z_i \right|_m^+ = |\omega_0^* + \omega_1^* z_1 + \ldots + \omega_n^* z_n|_m^+,$$

который при подстановке $\omega_0^* = \omega_0$, $\omega_i^* = \omega_i$, $z_i = x_i$, $s = n$ соответствует полиному (14). Пусть $U = Y$, $\omega_0^* = \psi_0$, $\omega_i^* = \psi_i$, $z_i = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$, $s = 2^n - 1$, тогда доказательство (14) сводится к повторению доказательства теоремы 2 п.а.

Доказательство теоремы 4. По аналогии с доказательством теоремы 2 рассмотрим два варианта доказательств, определяющих два варианта построения алгоритма получения (19).

а. Так как (П.1) справедливо для любых значений модуля $m > 1$, то справедливы и v записей П.1 для различных значений модуля $m > 1$:

$$
\text{(П.6)}\qquad
\begin{aligned}
|Y|^{+}_{m_1} &= \left|\sum_{i=0}^{2^n-1} c_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_1} = \left|\sum_{i=0}^{2^n-1} |c_i|^{+}_{m_1} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_1},\\
|Y|^{+}_{m_2} &= \left|\sum_{i=0}^{2^n-1} c_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_2} = \left|\sum_{i=0}^{2^n-1} |c_i|^{+}_{m_2} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_2},\\
&\vdots\\
|Y|^{+}_{m_v} &= \left|\sum_{i=0}^{2^n-1} c_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_v} = \left|\sum_{i=0}^{2^n-1} |c_i|^{+}_{m_v} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_v}.
\end{aligned}
$$

На основании Китайской теоремы об остатках система

$$\phi_1 = |Y|^{+}_{m_1},\ \phi_2 = |Y|^{+}_{m_2},\ \dots,\ \phi_v = |Y|^{+}_{m_v}$$

имеет единственное решение Y, если выполнены условия:

$$Y_{\max} < \prod_{k=1}^{v} m_k; \quad \gcd(m_i, m_j) = 1, \quad i, j = 1, \dots, v; \quad i \neq j.$$

Так как эти условия в теореме 4 определены, то и (19) имеет единственное решение Y.

Теорема доказана.

Из данного доказательства следует, что построить (19) можно посредством выполнения двух шагов:

Шаг 1. Построение (3) посредством алгоритма 1.

Шаг 2. Построение системы (19) посредством (П.6).

б. Используем (П.3) для построения системы арифметических полиномов по v заданным модулям, отвечающим требованиям однозначности представления (19):

$$
\text{(П.7)}\qquad
P_j(X) = \begin{cases}
\mu'_{j,1}(X) = \left|\sum\limits_{i=0}^{2^n-1} \psi'_{j,i,1} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_1},\\
\mu'_{j,2}(X) = \left|\sum\limits_{i=0}^{2^n-1} \psi'_{j,i,2} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_2},\\
\vdots\\
\mu'_{j,v}(X) = \left|\sum\limits_{i=0}^{2^n-1} \psi'_{j,i,v} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\right|^{+}_{m_v},
\end{cases}
$$

где $\psi'_{j,i,k} = |r_{j,i}|^{+}_{m_k}$ $(j = 1, \dots, d;\ i = 0, 1, \dots, 2^n - 1;\ k = 1, \dots, v)$.

Аналогично используя (П.4), получим:

$$(\text{П.8}) \qquad \begin{cases} \mu''_{j,1}(X) = \sum\limits_{i=0}^{2^n-1} \psi''_{j,i,1} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \\ \mu''_{j,2}(X) = \sum\limits_{i=0}^{2^n-1} \psi''_{j,i,2} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \\ \vdots \\ \mu''_{j,v}(X) = \sum\limits_{i=0}^{2^n-1} \psi''_{j,i,v} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \end{cases}$$

где $\psi''_{j,i,k} = |\psi'_{j,i,k} b_{j,k}|^+_{m_k}$; $b_{j,1} = \left|2^{j-1}\right|^+_{m_1}, b_{j,2} = \left|2^{j-1}\right|^+_{m_2}, \dots, b_{j,s} = \left|2^{j-1}\right|^+_{m_s}$ $(j = 1, \dots, d;\ i = 0, 1, \dots, 2^n - 1;\ k = 1, \dots, v)$.

Окончательно, обобщая (П.4) для модулей $m_1, m_2, \dots, m_v$, получают (19) с помощью выражений

$$(\text{П.9}) \qquad \psi_{i,k} = \left| \sum_{j=1}^{d} \psi''_{j,i,k} \right|^+_{m_k} \qquad (i = 0, 1 \dots, 2^n - 1;\ k = 1, \dots, v).$$

Теорема доказана.

Алгоритм получения (19) состоит в выполнении трех шагов, заключающихся соответственно в построении (П.7), (П.8) и собственно (19) при помощи (П.9).

Достоинством первых вариантов реализации алгоритмов формирования арифметических полиномов (13) и (19) являются простота и наглядность. Особенностью вторых вариантов является формирование соответствующих арифметических полиномов, обеспечивающих модулярность преобразований на всех этапах реализации алгоритма, что дает "удержание" промежуточных результатов вычислений в заданном числовом диапазоне.

СПИСОК ЛИТЕРАТУРЫ

1. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов. М.: Наука. Физматлит, 1997.
2. *Малюгин В.Д.* Реализация булевых функций арифметическими полиномами // АиТ. 1982. № 4. С. 84–93.
3. *Малюгин В.Д.* Реализация кортежей булевых функций посредством линейных арифметических полиномов // АиТ. 1984. № 2. С. 114–121.
4. *Thornton M.A., Dreschler R., Miller D.M.* Spectral Techniques in VLSI CAD. Kluwer Academic Publishers, 2002.
5. *Heidtmann K.D.* Arithmetic Spectrum Applied to Fault Detection for Combinational Natworks // IEEE Trans. Comput. 1991. V. 40. № 3. P. 320–324.
6. *Шмерко В.П.* Синтез арифметических форм булевых функций посредством преобразования Фурье // АиТ. 1989. № 5. С. 134–142.
7. *Кухарев Г.А., Шмерко В.П., Зайцева Е.Н.* Алгоритмы и систолические процессоры для обработки многозначных данных. Минск: Наука и техника, 1990.
8. *Акритас А.* Основы компьютерной алгебры с приложениями: Пер. с англ. М.: Мир, 1994 / Akritas A.G. Elements of computer algebra. John Wiley & Sons, 1989.
9. *Кнут Д.Э.* Искусство программирования. Т. 2. Получисленные алгоритмы, 3-е изд.: Пер. с англ.: Уч. пос. М.: Издат. дом "Вильямс", 2000.

10. *Амербаев В.М.* Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976.
11. *Yanushkevich S., Shmerko V., Dziurzanski P.* Word Level Decision Diagrams Upon the Conditions of Linearity // IEEE Trans. Comput. Design of Integrated Syst. 2001. V. XX. No. Y. month. P. 1–40.
12. *Шмерко В.П.* Теоремы Малюгина: новое понимание в логическом управлении, проектировании СБИС и структурах данных для новых технологий // АиТ. 2004. № 6.
13. *Soderstrand M.A., Jenkins W.K., Jullien G.A. and Tailor F.J.* Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. N.Y.: IEEE Press, 1986.
14. *Макклеллан Дж., Рейдер Ч.М.* Применение теории чисел в цифровой обработке сигналов: Пер. с англ. / Под ред. Ю.И. Манина. М.: Радио и связь, 1983. / *Maclellan J.H. and Rader C.M.* Number Theory in Digital Signal Processing. Prentice-Hall, Englewood Cliffs. N.J., 1979. (In USA).
15. *Кравченко В.Ф., Крот А.М.* Методы и микроэлектронные средства цифровой фильтрации сигналов и изображений на основе теоретико-числовых преобразований // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1997. № 6. С. 3–31.
16. *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.
17. *Финько О.А.* Восстановление числа в системе остаточных классов с минимальным количеством оснований // Электронное моделирование. 1998. Т. 20. № 3. С. 56–61.
18. *Финько О.А.* Варианты Китайской теоремы об остатках, ориентированные на техническую реализацию // Междунар. конгресс "Мат. в XXI в. Роль ММФ НГУ в науке, образовании и бизнесе." 25–28 июня 2003. Новосибирск, Академгородок. http://www.sbras.ru/ws/MMF-21/.
19. *Ноден П., Китте К.* Алгебраическая алгоритмика: Пер. с франц. М.: Мир, 1999.
20. *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.
21. *Финько О.А.* Контроль и реконфигурация аналого-цифровых устройств, функционирующих в системе остаточных классов // Электронное моделирование. 2000. Т. 22. № 4. С. 92–103.
22. *Fin'ko 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). Divnomorskoe, September 5–10, 2002. P. 453–454. (In USA).
23. *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.
24. *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. 611–619.
25. *Финько О.А.* Параллельные логические вычисления, использующие избыточные представления чисел // Тр. II Междунар. конф. "Идентификация систем и задачи управления" (SICPRO'03). М.: ИПУ им. Трапезникова РАН, Москва, 29–31 января 2003. С. 1716–1728.
26. *Финько О.А.* Логические вычисления на основе теоретико-числовых преобразований // Тр. II Междунар. конф. по проблемам управления (МКПУ II). М.: ИПУ им. Трапезникова РАН, Москва, 16–20 июня 2003.
27. *Бухштаб А.А.* Теория чисел. М.: Просвещение, 1966.

Статья представлена к публикации членом редколлегии П.П. Пархоменко.

Поступила в редакцию 17.12.2003