УДК 519.714

© 1996 г. В.Н. КОНДРАТЬЕВ,
А.А. ШАЛЫТО, канд. техн. наук
(ЦНИИ НПО "АВРОРА", Санкт-Петербург)

РЕАЛИЗАЦИЯ БУЛЕВЫХ ФУНКЦИЙ ОДНИМ ЛИНЕЙНЫМ АРИФМЕТИЧЕСКИМ ПОЛИНОМОМ С МАСКИРОВАНИЕМ

Предлагаются эффективные (по трудоемкости и компактности представления) методы реализации пороговых, пороговo-линейных и линейных булевых функций одним линейным (бесповторным) арифметическим полиномом с маскированием. Рассматривается вопрос о реализации симметрических булевых функций.

1. Введение

При использовании в системах логического управления микропроцессоров и микро-ЭВМ появляется возможность применения нетрадиционных методов реализации булевых функций (БФ), базирующихся на широких арифметических возможностях указанных технических средств. Одним из таких методов является реализация БФ с помощью арифметических полиномов (АП) [1–14].

В общем случае АП для булевой функции n переменных является нелинейным (повторным) и содержит 2^n членов, и поэтому с ростом n вычисление полинома значительно усложняется.

Особую важность при этом представляет реализация БФ с помощью линейных (бесповторных) АП (ЛАП), так как вычисление ЛАП сводится к суммированию коэффициентов при переменных, значения которых равны единице.

Однако вопросы реализации БФ линейными АП исследованы далеко недостаточно.

В [7] определено условие линейности (УЛ), выполнение которого обеспечивает реализацию БФ n переменных одним безызбыточным ЛАП тех же переменных. Напомним, что ЛАП называется безызбыточным, если число разрядов в двоичном представлении максимального значения, вычисленного по этому полиному, равно числу реализуемых БФ, и избыточным, если указанное число разрядов превышает число реализуемых функций.

Однако, как показано ниже, безызбыточным ЛАП реализуются только БФ, существенно зависящие не более, чем от одной переменной.

Расширение класса функций, реализуемых ЛАП, обеспечивается при введении избыточности – реализации наряду с заданной еще и некоторых других функций [1]. При этом ЛАП вычисляет на входном наборе десятичное значение кортежа функций, при двоичном представлении которого в соответствующем разряде будет находиться значение заданной функции на этом наборе.

Операцию выделения ℓ-го разряда, считая младший разряд первым, в m-разрядном двоичном представлении десятичного числа будем называть маскированием и обозначать r_m^ℓ, а операцию преобразования десятичного числа в двоичное – символом bin.

ЛАП, к десятичному значению которого для выделения разряда в его двоичном представлении применяется операция маскирования, будем называть ЛАП с маскированием (ЛАПМ).

В [4] предложен подход к построению ЛАПМ, однако он чрезвычайно трудоемок в связи с необходимостью преобразований сложных логических формул и решения сложных логических уравнений с помощью целочисленного программирования на основе алгоритма Балаша.

В [3] изложен существенно менее трудоемкий метод реализации произвольных БФ, заданных в дизъюнктивной нормальной форме, суперпозицией двух ЛАПМ, первый из которых вычисляет все конъюнкции, а второй дизъюнкцию, получающуюся после замены в БФ каждой конъюнкции новой буквой.

Таким образом, можно утверждать, что в настоящее время неизвестны конструктивные методы введения в кортеж с заданной БФ дополнительных функций с целью реализации их одним ЛАПМ.

В настоящей работе предлагаются эффективные (по трудоемкости и компактности представления) методы реализации пороговых, порогово-линейных и линейных БФ одним ЛАПМ. Это имеет как практическое, когда ЛАМП компактнее других форм представления функций, так и теоретическое значение, так как предлагаемые методы направлены на определение взаимосвязи между такими важными математическими объектами, как булевы функции (формулы) и линейные арифметические полиномы. При разработке методов использовались, в том числе, и теоремы из [4, 6], относящиеся к классам БФ.

2. Реализация булевых функций безызбыточным линейным арифметическим полиномом

Теорема 1. *Линейным арифметическим полиномом можно безызбыточно реализовать лишь булеву функцию, существенно зависящую не более, чем от одной переменной* 0, 1, $!x$, x, *где* ! - *символ операции "инверсия".*

Доказательство. Каждое значение БФ должно быть равно 0 или 1, а коэффициенты ЛАП (кроме $a0 = 0, 1$) могут принимать только следующие значения: -1, 0, 1. Если $a0 = 0$ ($a0 = 1$), то не более одного из оставшихся коэффициентов может быть равно единице (минус единице), в то время как остальные коэффициенты должны быть равны нулю. В противном случае хотя бы на одном входном наборе значение полинома будет не равно ни нулю, ни единице, что и доказывает сформулированную теорему.

Из теоремы следует, что одна БФ, существенно зависящая от двух и более переменных, не может быть реализована безызбыточным ЛАП, и поэтому рассмотрим вопрос о реализации таких функций ЛАПМ.

3. Реализация пороговых функций

В настоящем разделе рассматриваются два метода реализации пороговых функций (ПФ), первый из которых строит ЛАПМ n переменных по пороговому представлению функции n переменных, а второй - по ЛАПМ пороговой функции $(n-1)$-й переменной.

а) *Первый метод.* Булева функция называется пороговой, если

$$(1)\qquad f = \begin{cases} 1 & \text{при} \quad \sum_{i=1}^{n} wi * xi \geqslant T, \\ 0 & \text{при} \quad \sum_{i=1}^{n} wi * xi < T, \end{cases}$$

где wi вес переменной xi; T - порог функции; $*$ символ операции "умножение".

Таким образом, можно утверждать, что пороговая функция f, зависящая от n переменных, представляет собой совокупность, состоящую из ЛАП

$$P = -T + w1 * x1 + w2 * x2 + \ldots + wn * xn$$

и условного оператора

$$\text{if } (P \geqslant 0) \text{ then } f = 1 \text{ else } f = 0.$$

В настоящем разделе ставится задача нахождения для функции f другого ЛАП

$$P = w0 + w1 * x1 + w2 * x2 + \ldots + wn * xn,$$

такого, что

$$f = r_m^m(\text{bin } P).$$

Следовательно, задача сводится, в некотором смысле, к определению возможности замены условного оператора операцией маскирования, которая программно может реализовываться проще.

Для функции f, зависящей от n переменных и принадлежащей к рассматриваемым в настоящей работе классам функций, отличных от пороговых, ищется ЛАП

$$P = a0 + a1 * x1 + a2 * x2 + \ldots + an * xn,$$

такой, что

$$f = r_m^l(\text{bin } P).$$

Возвращаясь к рассмотрению пороговых функций, отметим, что если порог равен 2^α $(\alpha = 0, 1, 2, \ldots)$, то наличие единицы хотя бы в одном разряде двоичного представления значений $\sum_{i=1}^{n} wi{*}xi$, начиная с разряда с номером $\alpha + 1$ (при нумерации разрядов с единицы), свидетельствует о том, что вычисленное значение достигло или превысило T.

Если $T \neq 2^\alpha$, то задача сводится к рассмотренной за счет увеличения порога до величины, равной ближайшей целой степени двух. Для этого необходимо добавить к левой и правой частям неравенства (1) величину $2^{]\log_2 T[} - T$:

$$2^{]\log_2 T[} - T + \sum_{i=1}^{n} wi * xi \geqslant 2^{]\log_2 T[}. \tag{2}$$

При этом новым порогом будет величина $T_1 = 2^\alpha = 2^{]\log_2 T[}$. Левая часть соотношения (2) является ЛАП вида:

$$P = 2^{]\log_2 T[} - T + \sum_{i=1}^{n} wi * xi. \tag{3}$$

Из изложенного следует, что произвольная ПФ может быть реализована следующим образом:

$$f = r_\beta^\beta(\text{bin } P) \mid r_\beta^{\beta-1}(\text{bin } P) \mid \ldots \mid r_\beta^{\alpha+1}(\text{bin } P), \tag{4}$$

где β – число разрядов в двоичном представлении максимального значения P; | – символ операции "дизъюнкция".

Пример 1. Реализовать ПФ $f = x1 \mid x2 \mid x3$.

В этом случае (1) приобретает вид: $x1 + x2 + x3 \geqslant 2^0$. Так как максимальное значение P в данном случае равно трем, то $\beta = 2$. Учитывая, что $\alpha = 0$, то из (4) следует, что

$$f = r_2^2(\mathrm{bin}\,(x1 + x2 + x3)) \mid r_2^1(\mathrm{bin}\,(x1 + x2 + x3)).$$

Рассмотрим случай, когда $\beta = \alpha + 1$ – превышение порога происходит только в одном разряде двоичного представления значения P. Для этого величина β не должна превышать числа разрядов двоичного представления величины порога T_1. Сформулированное условие можно записать в виде:

$$(5) \qquad P_{\max} < 2 * T,$$

где $P_{\max}$ – максимальное значение полинома P.

Отметим, что если для ПФ условие (5) не выполняется, то необходимо увеличить величину T_1 в два раза. Для этого требуется добавить к левой и правой частям (2) величину T_1. Если и при этом (5) не выполняется, указанная процедура повторяется до выполнения этого условия. Таким образом можно добиться выполнения (5) для любой ПФ, так как при увеличении левой и правой частей (2) правая часть неравенства (5) возрастает в два раза быстрее левой.

Таким образом, доказано, что произвольная ПФ может быть вычислена следующим образом:

$$(6) \qquad f = r_\beta^\beta(\mathrm{bin}\,P).$$

Программная реализация этого соотношения на языке высокого уровня, например СИ, чрезвычайно проста и состоит в вычислении на заданном входном наборе значения полинома P, сдвиге полученного результата на $\beta - 1$ разрядов вправо и считывании полученного результата, равного значению ПФ на этом наборе.

Для того чтобы воспользоваться предложенным подходом для заданной ПФ, необходимо предварительно определить ее пороговую реализацию (ПР) (1).

Процедура определения весов переменных и порога для ПФ весьма трудоемка [15], и поэтому рассмотрим три более простых подхода к нахождению пороговой реализации. Первый строит ПР непосредственно по описанию ПФ, второй основан на использовании для произвольных ПФ шести и менее переменных каталогов оптимальных ПР (например, [16]), а третий, изложенный в приложении, применим для бесповторных пороговых формул (БПФ), имеющих важное практическое и теоретическое значение [17].

Пример 2. Реализовать ПФ "два и более из трех", которая описывается формулой $f = (x1 \mid x2) \& x3 \mid x1 \& x2$.

Из словесного описания функции следует, что $x1 + x2 + x3 \geqslant 2$. Так как в этом случае $T = 2^\alpha$, а (5) выполняется, то

$$f = r_2^2(\mathrm{bin}\,(x1 + x2 + x3)).$$

Проиллюстрируем полученное соотношение таблицей.

Из таблицы следует, что введение избыточности (реализация полиномом двух функций вместо одной) и применение операции маскирования позволило построить ЛАПМ вместо безызбыточного (по числу объединяемых функций), но более сложного нелинейного АП (НАП) [7]:

$$f = x1 * x2 + x1 * x3 + x2 * x3 - 2 * x1 * x2 * x3.$$

Таким образом, повторной БФ соответствует бесповторный АП с маскированием, что является основной предпосылкой использования последнего для эффективной

$x1$	$x2$	$x3$	$x1 + x2 + x3$	$\mathrm{bin}\,(x1 + x2 + x3)$	
				r_2^2	r_2^1
0	0	0	0	0	0
0	0	1	1	0	1
0	1	0	1	0	1
0	1	1	2	1	0
1	0	0	1	0	1
1	0	1	2	1	0
1	1	0	2	1	0
1	1	1	3	1	1

программной реализации. Для бесповторной булевой формулы ее непосредственная программная реализация всегда более эффективна, чем реализация на основе ЛАПМ. Однако для систем пороговых формул, даже бесповторных, использование ЛАПМ может обеспечить минимальную по объему памяти программную реализацию [13].

При использовании языка СИ найденный ЛАПМ реализуется следующей программой:

$$
\begin{aligned}
&\mathrm{lapm}\ (\mathrm{int}\,x1,\ \mathrm{int}\,x2,\ \mathrm{int}\,x3)\\
&\quad \{\ \mathrm{int}\,f;\\
&\quad\ \ f = (x1 + x2 + x3) \gg 1;\},
\end{aligned}
$$

где $\gg L$ символ операции "сдвиг на L двоичных разрядов вправо".

Важно отметить, что такая реализация функции "два и более из трех" при выбранных типах переменных является простейшей (14 байт) по сравнению с другими известными авторам более шестидесяти вариантами программной реализации этой функции. Так, например, непосредственная реализация формулы

$$
\begin{aligned}
&\mathrm{for}\ (\mathrm{int}\,x1,\ \mathrm{int}\,x2,\ \mathrm{int}\,x3)\\
&\quad \{\ \mathrm{int}\ f;\\
&\quad\ \ f = (x1 \,|\, x2)\&x3 \,|\, x1\&x2;\}
\end{aligned}
$$

требует 20 байт памяти, а ПР

$$
\begin{aligned}
&\mathrm{prg}\ (\mathrm{int}\ x1,\ \mathrm{int}\ x2,\ \mathrm{int}\ x3)\\
&\quad \{\ \mathrm{int} f = 0;\\
&\quad\ \ \mathrm{if}\ \big((x1 + x2 + x3) \geqslant 2\big)\ \ f = 1;\}
\end{aligned}
$$

и того больше – двадцати четырех байт.

Пример 3. Реализовать ПФ "семь и более из десяти".

Из описания функции следует, что $\sum\limits_{i=1}^{10} xi \geqslant 7$. Увеличим порог функции до величины 2^a. При этом $1 + \sum\limits_{i=1}^{10} xi \geqslant 8$. Так как (5) выполняется, то

$$
f = r_4^4\left(\mathrm{bin}\left(1 + \sum_{i=1}^{10} xi\right)\right).
$$

Этот пример демонстрирует возможность высокой эффективности использования ЛАПМ, так как таблица истинности, булева формула или ЛАП в этом случае чрезвычайно громоздки и поэтому программируются с большими затратами памяти.

Пример 4. Реализовать ПФ $f = (x1 \mid x2 \mid x3) \& x4 \mid x1 \& x2 \& x3$.

В этом случае из [15] следует, что $x1 + x2 + x3 + 2 * x4 \geqslant 3$. В силу того, что $T \neq 2^{\alpha}$, увеличим порог функции: $1 + x1 + x2 + x3 + 2 * x4 \geqslant 4$. Так как при этом соотношения (2) и (5) выполняются, то

$$f = r_3^3\bigl(\mathrm{bin}\,(1 + x1 + x2 + x3 + 2 * x4)\bigr).$$

Пример 5. Реализовать БПФ $f = x1 \& x2$.

Используя метод, изложенный в приложении, получим $x1 + x2 \geqslant 2$. Так как в этом случае $T = 2^{\alpha}$, а (5) выполняется, то

$$f = r_2^2\bigl(\mathrm{bin}\,(x1 + x2)\bigr).$$

Пример 6. Реализовать БПФ $f = x1 \mid x2$.

Используя метод, изложенный в приложении, получим $x1 + x2 \geqslant 1$. Так как $T = 2^{\alpha}$, но (5) не выполняется, увеличим порог функции: $1 + x1 + x2 \geqslant 2$. Ввиду того, что при этом оба условия выполняются,

$$f = r_2^2\bigl(\mathrm{bin}\,(1 + x1 + x2)\bigr).$$

Пример 7. Реализовать БПФ $f = x1 \& x2 \& x3$.

Используя метод, изложенный в приложении, получим $x1 + x2 + x3 \geqslant 3$. Так как $T \neq 2^{\alpha}$, увеличим порог функции до ближайшей степени двух: $1 + x1 + x2 + x3 \geqslant 4$. Ввиду того, что при этом (5) выполняется,

$$f = r_3^3\bigl(\mathrm{bin}\,(1 + x1 + x2 + x3)\bigr).$$

Пример 8. Реализовать БПФ $f = x1 \& x2 \mid x3$.

Используя метод, изложенный в приложении, получим $x1 + x2 + 2 * x3 \geqslant 2$. В этом случае $T = 2^{\alpha}$, однако, так как (5) не выполняется ($P_{\max} = 2 * T$), то увеличим порог до следующей величины, равной степени двух: $2 + x1 + x2 + 2 * x3 \geqslant 4$. Так как при этом (5) выполняется, то

$$f = r_3^3\bigl(\mathrm{bin}\,(2 + x1 + x2 + 2 * x3)\bigr).$$

б) *Второй метод.* Метод основан на теореме, приведенной в [6].

Теорема 2. ***Если кортеж N булевых функций и переменных $f_N \# f_{N-1} \#, \ldots, \#, f_1$ реализуется линейным арифметическим полиномом P_N, то кортеж из $(N+1)$-й функции***

$$(7) \qquad (f_N \& x_{n+1}) \# (f_N \oplus x_{n+1}) \# f_{N-1} \# \ldots \# f_1$$

реализуется ЛАП вида $P_{N+1} = P_N + 2^{N-1} * x_{n+1}$, а кортеж из того же числа функций

$$(8) \qquad (f_N \mid x_{n+1}) \# (f_N \oplus x_{n+1} \oplus 1) \# f_{N-1} \# \ldots \# f_1$$

реализуется ЛАП вида $P_{N+1} = P_N + 2^{N-1} * x_{n+1} + 2^{N-1}$, где # — операция объединения в кортеж, а $\oplus$ — операция "сумма по модулю 2".

В силу установленного в [13] факта, что ЛАП реализует лишь такие кортежи функций, в которых крайняя левая функция f_N является ПФ, а в [15] показано, что если f_N — пороговая функция n переменных, то и функции $f_N \& x_{n+1}$ и $f_N \mid x_{n+1}$ также являются пороговыми, то теорема 2 определяет:

рекурсивный метод построения ЛАПМ для БПФ;

простой метод реализации ПФ вида $f_N \& x_{n+1}$ и $f_N \mid x_{n+1}$ для случая, когда ЛАПМ для f_N уже найден, например, с помощью подходов, изложенных выше.

Пример 9. Реализовать БФ $f = x1 \& x2 \& x3$.

Из примера 5 следует, что для $f1 = x1 \& x2$ $n = 2$, $N = 2$, и поэтому из (7) имеем

$$f = r_3^3\bigl(\mathrm{bin}\,(x1 + x2 + 2 * x3)\bigr).$$

Из этого соотношения и примера 7 следует, что представление БФ с помощью ЛАПМ в отличие от их представления АП [1, 7] не является единственным.

Пример 10. Реализовать БФ $f = (x1 \mid x2) \& x3 \mid x1 \& x2 \mid x4$.

Из примера 2 следует, что для $f1 = (x1 \mid x2) \& x3 \mid x1 \& x2$ $n = 2$, $N = 2$, и поэтому, исходя из (8), получим

$$f = r_3^3\bigl(\mathrm{bin}\,(2 + x1 + x2 + x3 + 2 * x4)\bigr).$$

Методы, рассмотренные выше, применимы к ПФ, представимым формулами без инверсий — положительно монотонным ПФ (ПМПФ).

При наличии в реализуемой формуле переменных типа $!xi$ первоначально ЛАПМ строится для однотипной с ней ПМПФ, а затем в ЛАПМ переменная xi заменяется соотношением $1 - xi$.

Пример 11. Реализовать ПФ $f = x1 \mid !x2$.

Из изложенного и примера 6 следует

$$f = r_2^2\bigl(\mathrm{bin}\,(2 + x1 - x2)\bigr).$$

Пример 12. Реализовать ПФ $f = (x1 \mid x2) \& x3 \mid x1 \& x2 \mid !x4$.

Из изложенного и примера 10 имеем

$$f = r_3^3\bigl(\mathrm{bin}\,(4 + x1 + x2 + x3 - 2 * x4)\bigr).$$

4. Реализация линейных функций

Линейной называется БФ, представимая формулой

$$f = c0 \oplus c1 \& x1 \oplus c2 \& x2 \oplus \ldots \oplus cn \& xn,$$

где $ci = 0, 1$.

Линейная функция реализуется ЛАПМ вида

$$f = r^1_{1+[\log_2 n]}\left(\mathrm{bin}\,(c0 * (1 - xn) + \sum_{k=1}^{n-c0} ck * xk)\right).$$

Поэтому

$$f1 = x1 \oplus x2 = r_2^1\bigl(\mathrm{bin}\,(x1 + x2)\bigr),$$

$$f2 = x1 \oplus x2 \oplus x3 = r_2^1\bigl(\mathrm{bin}\,(x1 + x2 + x3)\bigr).$$

Вторая из этих функций реализуется на языке СИ следующей программой:

```
mod (int x1, int x2, int x3)
{ int f;
  f = (x1 + x2 + x3) & 1; }.
```

Рассмотренные функции реализуются теми же ЛАПМ, что и функции $f1 = x1\&x2$; $f2 = (x1\,|\,x2)\&x3\,|\,x1\&x2$ соответственно, как и должно быть для двоичных одноразрядных полусумматора и сумматора.

5. Реализация порогово-линейных функций

Порогово-линейной функцией (ПЛФ) будем называть булеву функцию, представимую формулой вида:

$$f = f1(x1, \ldots, xN) \oplus \widetilde{xi} \oplus \ldots \oplus \widetilde{xj},$$

где $f1$ пороговая функция; i, j – целые числа; $\widetilde{xi} = \{!xi, xi\}$.

Рассмотрим методы построения ЛАПМ для ПЛФ при условии, что реализуемая функция задана в порогово-линейной форме.

Использование теоремы 2 позволяет реализовать ПЛФ, для которых $i, j > n$, а ЛАПМ для $f1$ найден с помощью методов, изложенных в разделе 3.

Пример 13. Реализовать ПЛФ $f = x1\&x2\&x3\oplus!x4$.

Из примера 7 следует, что $f1 = x1\&x2\&x3 = r_3^3(\text{bin}\,(1 + x1 + x2 + x3))$. Поэтому из соотношения (8) находим $f = x1\&x2\&x3\oplus!x4 = x1\&x2\&x3 \oplus x4 \oplus 1 = r_4^3(\text{bin}\,(5 + x1 + x2 + x3 + 4 * x4))$.

Реализуем заданную функцию другим способом. Из соотношения (7) и раздела 3 следует, что $f = x1\&x2\&x3\oplus!x4 = r_4^3(\text{bin}\,(5 + x1 + x2 + x3 - 4 * x4))$.

Это соотношение реализуется на языке СИ следующей программой:

```
plf ( int x1, int x2, int x3, int x4 )
{ int f;
  f = ((5 + x1 + x2 + x3 - 4 * x4) >> 2) & 1; }.
```

Недостаток теоремы 2 состоит в том, что ее нельзя использовать для случая, когда $i, j \leqslant n$. Этот недостаток устраняется применением следующей теоремы [4].

Теорема 3. Если $f1 = r_m^k(\text{bin}\,P_N)$, то $f = f1 \oplus xi$ реализуется в k-м разряде полинома $P_N + 2^{k-1} * xi$, где $i = \{1, 2, \ldots, n+1\}$.

Пример 14. Реализовать ПЛФ $f = x1 \oplus x2\&(!x3\,|\,x4))$.

Из примера 11 следует, что $f1 =!x3\,|\,x4 = r_2^2(\text{bin}\,(2 - x3 + x4))$.

Используя (7), получим $f2 = x2\&(!x3\,|\,x4) = r_3^3(\text{bin}\,(2 + 2*x2 - x3 + x4))$. Применяя теорему 3, находим $f = r_4^3(\text{bin}\,(2 + 4 * x1 + 2 * x2 - x3 + x4))$. При этом отметим, что в [1] эта формула реализуется существенно более сложным НАП:

$$f = 1 - x1 - x2 - x3 + 2 * x1 * x2 + 2 * x1 * x3 + 2 * x2 * x3 + x3 * x4 -$$
$$- 4 * x1 * x2 * x3 - 2 * x1 * x3 * x4 - 2 * x2 * x3 * x4 + 4 * x1 * x2 * x3 * x4.$$

Пример 15. Реализовать ПЛФ $f = (x1\,|\,x2\,|\,x3) \oplus x3$.

В силу того, что $f1 = x1\,|\,x2\,|\,x3 = r_3^3(\text{bin}\,(3 + x1 + x2 + x3))$, из теоремы 3 следует

$$f = r_4^3(\text{bin}\,(3 + x1 + x2 + 5 * x3)).$$

С другой стороны, так как $f = (x1\,|\,x2\,|\,x3) \oplus x3 = (x1\,|\,x2)\&!x3$ является БПФ, то, используя результаты раздела 3, получим

$$f = r_3^3(\text{bin}\,(3 + x1 + x2 - 2 * x3)).$$

Пример 16. Реализовать ПЛФ $f = x1\&x2 \oplus x3 \oplus x4 \oplus x5$.

Применяя многократно теорему 3, имеем $f1 = x1\&x2 = r_2^2(\mathrm{bin}(x1 + x2))$; $f2 = x1\&x2 \oplus x3 = r_3^2(\mathrm{bin}(x1 + x2 + 2 * x3))$; $f3 = x1\&x2 \oplus x3 \oplus x4 = r_3^2(\mathrm{bin}(x1 + x2 + 2 * x3 + 2 * x4))$. Таким образом,

$$f = r_4^2\big(\mathrm{bin}(x1 + x2 + 2 * x3 + 2 * x4 + 2 * x5)\big).$$

Интересным является тот факт, что в этом примере в отличие от предыдущих реализуемая функция "сдвинулась" в середину двоичного представления.

Перейдем к рассмотрению случая, когда ПЛФ задана в форме, отличной от порогово-линейной. Поиск такой формы предлагается проводить на основе соотношений [7]:

$$f = \big(!xi\&f(0) \,|\, xi\&!f(1)\big) \oplus xi; \tag{9}$$

$$f = \big(!xi\&!f(0) \,|\, xi\&f(1)\big) \oplus !xi. \tag{10}$$

Пример 17. Реализовать ПЛФ $f = !x1\&x2 \,|\, x1\&!x2\&x3$.

Используя (9), получим $f = f1 \oplus x1 = (x1\&!x3 \,|\, x2) \oplus x1$. Для БПФ $f1 = r_3^3(\mathrm{bin}(3 + x1 + 2 * x2 - x3))$. Поэтому, используя теорему 3, получим

$$f = r_4^3(\mathrm{bin}(3 + x1 + 2 * x2 - x3)).$$

Эта функция реализована в [4] с помощью алгоритма Балана более сложным полиномом:

$$f = r_6^4\big(\mathrm{bin}(5 + 12 * x1 + 6 * x2 + 14 * x3)\big).$$

Пример 18. Реализовать ПЛФ $f = (!x1 \,|\, !x2 \,|\, !x3)\&(x1 \,|\, x2 \,|\, x3))$.

Используя (9), получим $f = f1 \oplus x1 = (!x1\&(x2 \,|\, x3) \,|\, x2\&x3) \oplus x1$. Для ПЛФ $f1 = r_2^2(\mathrm{bin}(1 - x1 + x2 + x3))$. Поэтому, используя теорему 3, получим

$$f = r_3^2\big(\mathrm{bin}(1 + x1 + x2 + x3)\big).$$

Пример 19. Реализовать ПЛФ $f = x1\&!x2\&!x3\&x4 \,|\, !x1\&x2\&x3\&x4 \,|\, !x1\&!x2\&!x4 \,|\, x1\&x3\&!x4 \,|\, x2\&!x3\&!x4$.

Из (9) при $i = 4$ следует, что $f = f1 \oplus x4 = (!x1\&!x2 \,|\, x1\&x3 \,|\, x2\&!x3) \oplus x4$. Применяя (10) к функции $f1$, получим $f = f2 \oplus !x1 \oplus x4 = ((x1 \,|\, x2)\&x3 \,|\, x1\&x2) \oplus !x1 \oplus x4$.

Из примера 2 следует, что $f2 = r_2^2(\mathrm{bin}(x1 + x2 + x3))$. Поэтому, применяя теорему 3, находим $f1 = r_3^2(\mathrm{bin}(2 - x1 + x2 + x3))$. Повторно используя теорему 3, имеем

$$f = r_3^2\big(\mathrm{bin}(2 - x1 + x2 + x3 + 2 * x4)\big).$$

Полученное соотношение в отличие от других форм представления этой функции является бесповторным, что обеспечивает более простую программную реализацию.

Вид и сложность ЛАПМ, получаемого по ПЛФ, зависит от того, какое из этих соотношений применяется и какая переменная используется в качестве xi.

Пример 20. Реализовать ПЛФ $f = !x1\&!x2\&x3 \,|\, x1\&x2\&!x3$.

Полагая в (9) $xi = x1$, получим $f = f1 \oplus x1 = (!x1\&(!x2\&x3) \,|\, x1\&!(x2\&!x3)) \oplus x1 = ((x1 \,|\, x3)\&!x2 \,|\, x1\&x3) \oplus x1$.

При этом, так как $f2 = (x1 \,|\, x3)\&x2 \,|\, x1\&x3 = r_2^2(\mathrm{bin}(x1 + x2 + x3))$, то $f1 = r_2^2(\mathrm{bin}(1 + x1 - x2 + x3))$. Используя теперь теорему 3, находим

$$f = r_3^2\big(\mathrm{bin}(1 + 3 * x1 - x2 + x3)\big).$$

Применяя в качестве xi переменные $!x1$, $x2$, $!x2$, $x3$, $!x3$, получим следующие соотношения: $f = r_3^2(\text{bin}\,(4 - 3 * x1 + x2 - x3)) = r_3^2(\text{bin}\,(1 - x1 + 3 * x2 + x3)) = r_3^2(\text{bin}\,(4 + x1 - 3 * x2 - x3)) = r_3^2(\text{bin}\,(x1 + x2 + 3 * x3)) = r_3^2(\text{bin}\,(5 - x1 - x2 - 3 * x3))$.

Таким образом, простейшая реализация обеспечивается при $xi = x3$. Вопросы принадлежности функции классу ПЛФ и выбор переменной xi в соотношениях (9), (10) остаются открытыми.

6. Реализация симметрических функций

Рассмотрим класс ЛАП вида $P = \sum_{i=1}^{n} xi$. Эти ЛАП описывают работу комбинационных счетчиков, для построения которых требуется определить систему из $1 + [\log_2 n]$ булевых функций. Эти функции относятся к классу симметрических и реализуются следующим образом.

Запишем матрицу-столбец размерности $(n+1) * 1$, все элементы которой принимают значения $0, 1, \ldots, n$. Эта матрица преобразуется в двоичную матрицу размерности $(n+1) * (1 + [\log_2 n])$, i-я $(i = 0, 1, \ldots, n)$ строка которой является двоичным представлением i-го элемента матрицы-столбца. При этом j-й столбец двоичной матрицы является характеристическим числом j-й функции, единица в i-м разряде которого указывает на наличие рабочего числа в этой функции.

Пример 21. Определить симметрические функции (СФ), реализуемые ЛАП $P = x1 + x2 + x3 + x4$.

Выполняя указанные построения и преобразования, получим

$$P = \begin{vmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{vmatrix} = \left| \; S_4^4 \;\#\; S_{2,3}^4 \;\#\; S_{1,3}^4 \; \right|.$$

Рассмотрим более широкий класс ЛАП:

$$(11) \qquad P1 = c1 + c2 * \sum_{i=1}^{n} xi,$$

где $c1$, $c2$ положительные целые числа.

Этот класс ЛАП реализует СФ так же, как рассмотрено выше.

Пример 22. Определить СФ, реализуемые ЛАП $P1 = 3 + 5 * (x1 + x2 + x3 + x4)$. Искомые функции определяются следующим образом:

$$P1 = 3 + 5 * \begin{vmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{vmatrix} = \begin{vmatrix} 3 \\ 8 \\ 13 \\ 18 \\ 23 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{vmatrix} =$$

$$= \left| \; S_{3,4}^4 \;\#\; S_{1,2}^4 \;\#\; S_{2,4}^4 \;\#\; S_{0,3,4}^4 \;\#\; S_{0,2,4}^4 \; \right|.$$

Из изложенного следует, например, что

$$f = S_{2,4}^4 = r_5^3\Big(\text{bin}(3 + 5 * (x1 + x2 + x3 + x4))\Big).$$

Покажем, что такая реализация эффективнее непосредственного построения АП для СФ.

В [12] показано, что произвольная СФ n переменных реализуется АП, содержащим не более $n+1$ коэффициентов ai. Для $n=4$ справедливо соотношение:

$$f = a4 * \psi_4^4 + a3 * \psi_4^3 + a2 * \psi_4^2 + a1 * \psi_4^1 + a0,$$

где

$$\psi_4^4 = x1 * x2 * x3 * x4;$$
$$\psi_4^3 = x1 * x2 * x3 + x1 * x2 * x4 + x1 * x3 * x4 + x2 * x3 * x4;$$
$$\psi_4^2 = x1 * x2 + x1 * x3 + x1 * x4 + x2 * x3 + x2 * x4 + x3 * x4;$$
$$\psi_4^1 = x1 + x2 + x3 + x4.$$

Для функции $S_{2,4}^4$ в [12] показано, что $(a4, a3, a2, a1, a0) = (7, -3, 1, 0, 0)$.

Из изложенного следует, что выражение (11) может рассматриваться в качестве эффективного генератора СФ. Исследование показало, что все СФ двух переменных порождаются пятью ЛАП при $c1 = 0, \ldots, 4$, $c2 = 1$, а все СФ трех переменных одиннадцатью ЛАП, в которых $c1 = 0, \ldots, 5$, $c2 = 1$; $c1 = 7$, $c2 = 1$; $c1 = 0$, $c2 = 3$; $c1 = 2$, $c2 = 3$; $c1 = 4$, $c2 = 3$; $c1 = 5$, $c2 = 5$.

Рассмотренный метод является переборным и не гарантирует реализацию произвольной СФ n переменных. Конструктивные методы реализации СФ, являющихся пороговыми, порогово-линейными и линейными, рассмотрены в предыдущих разделах. Например, используя метод, изложенный в разделе 5, можно показать, что

$$S_{0,2,3}^3 = (x1 \& x3 \,|\, !x2) \oplus x1 \oplus x3 = r_4^3(\mathrm{bin}(4 + 5 * x1 - 2 * x2 + 5 * x3));$$
$$S_1^3 = (!x1 \,|\, !x3) \& x2 \oplus x1 \oplus x3 = r_4^3(\mathrm{bin}(3 + 3 * x1 + 2 * x2 + 3 * x3)).$$

Вопрос о принадлежности произвольной СФ n переменных одному из перечисленных классов остается открытым.

ПРИЛОЖЕНИЕ

Построение пороговой реализации для положительно монотонной бесповторной пороговой формулы

1. Для заданной бесповторной формулы в базисе $\{\&, |\}$ из h букв строится древовидная схема максимальной глубины из $h-1$ двухвходовых элементов И и ИЛИ. Если построенная схема "линейна" (все элементы схемы соединены последовательно – в линию), то заданная формула является положительно монотонной бесповторной пороговой формулой (ПМБПФ).

2. Для ПМБПФ строится линейный бинарный граф (ЛБГ) [17], содержащий максимальное число путей от входа до единичного и нулевого выходов [18].

3. Используя модифицированный [19] метод Акерса [20], подсчитываем число путей в ЛБГ. При этом нулевые и единичные пометки у условных вершин (УВ) устраняются и проводится новая разметка:

начало ЛБГ помечается единицей и считается, что пометки дуг, исходящих из каждой УВ, совпадают с пометкой на ее входе;

в каждой точке объединения дуг выполняется "закон Кирхгофа" – пометка дуги, исходящей из точки объединения, равна сумме пометок дуг, входящих в эту точку.

4. Пометка на входе i-й УВ равна весу переменной xi, а пометка у "нулевой" операторной вершины равна порогу функции.

Пример П1. Построить ПР для $f = (x1 \& x2 \,|\, x3) \& x4$.

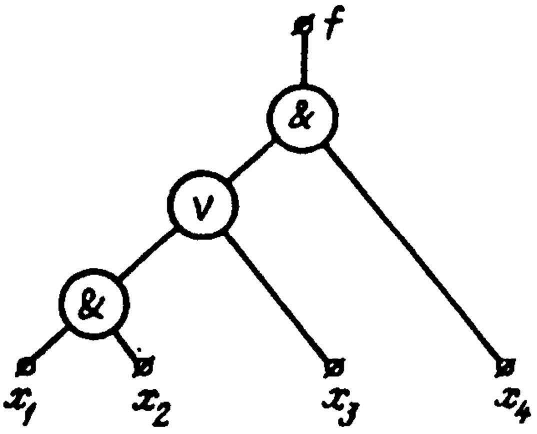

Рис. 1

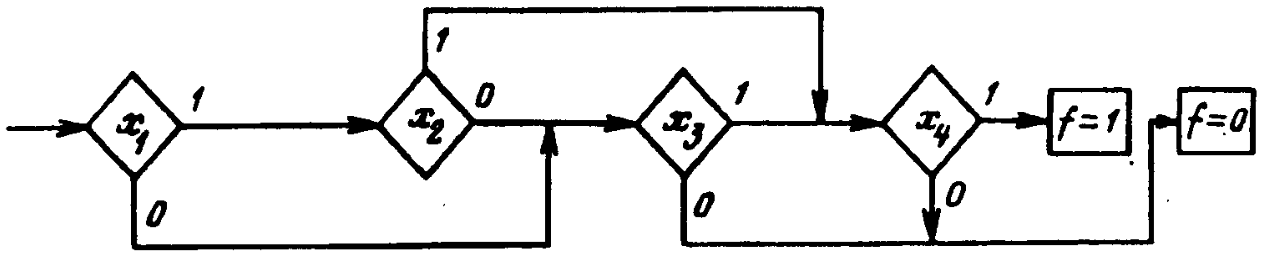

Рис. 2

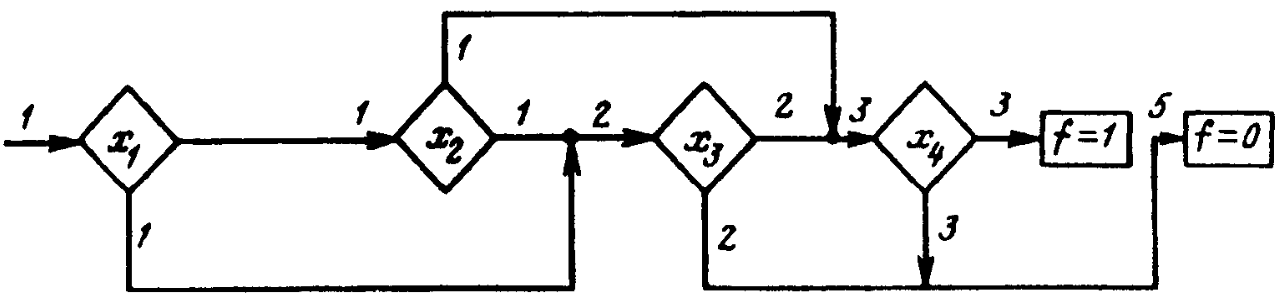

Рис. 3

В силу того, что эта формула является бесповторной, не содержит инверсий и реализуется "линейной" схемой (рис. 1), то она является ПМБПФ. На рис. 2 приведен ЛБГ с максимальным числом путей. На рис. 3 выполнена разметка ЛБГ для подсчета числа путей, из которой следует, что $w1 = 1$, $w2 = 1$, $w3 = 2$, $w4 = 3$; $T = 5$. Поэтому $x1 + x2 + 2 * x3 + 3 * x4 \geqslant 5$, а из раздела 3 следует, что $f = r_3^3(\mathrm{bin}\,(3 + x1 + x2 + 2 * x3 + 3 * x4))$.

СПИСОК ЛИТЕРАТУРЫ

1. *Малюгин В.Д.* Реализация булевых функций арифметическими полиномами // АиТ. 1982. № 4. С. 84–93.
2. *Малюгин В.Д.* О полиномиальной реализации кортежа булевых функций // Докл. АН СССР. 1982. Т. 265. № 6. С. 1338–1341.
3. *Малюгин В.Д.* Реализация кортежей булевых функций посредством линейных арифметических полиномов //АиТ. 1984. № 2. С. 114–122.

4. *Ефремов В.Д., Кузьмин А.А., Степанов В.А.* Вычисление логических функций с использованием преобразований Радемахера // АиТ. 1984. № 2. С. 105–113.
5. *Малюгин В.Д., Кухарев Г.А., Шмерко В.П.* Преобразования полиномиальных форм булевых функций. Препринт. М.: Ин-т проблем управления, 1986.
6. *Malyugin V.* Realization of logical function sets by arithmetic polynoms // Computers and Artificial Inteligence. 1987. № 6. P. 541–552.
7. *Артюхов В.Л., Кондратьев В.Н., Шалыто А.А.* Реализация булевых функций арифметическими полиномами //АиТ. 1988. № 4. С. 138–147.
8. *Осипов В.А., Шалыто А.А., Кондратьев В.Н.* Программная реализация алгоритмов логического управления в судовых системах. Методические разработки. Л.: Ин-т повышения квалификации руководящих работников и специалистов судостроительной промышленности, 1988.
9. *Шалыто А.А.* Реализация алгоритмов судовых управляющих логических систем при использовании микропроцессорной техники. Л.: Ин-т повышения квалификации руководящих работников и специалистов судостроительной промышленности, 1988.
10. *Шмерко В.П.* Синтез арифметических форм булевых функций посредством преобразования Фурье // АиТ. 1989. № 5. С. 134–142.
11. *Артюхов В.Л., Кондратьев В.Н., Шалыто А.А.* Использование линейных арифметических полиномов при реализации систем логического управления // XI Всесоюз. совещ. по проблемам управления. Тез. докл. М.: АН СССР, 1989. С. 495–496.
12. *Артюхов В.Л., Беляев Н.С., Шалыто А.А.* Методы программной реализации симметрических булевых функций // Проблемы комплексной автоматизации судов. ВНТО им. ак. А.Н. Крылова. Вып. 19. Л.: Судостроение, 1989. С. 37–51.
13. *Шалыто А.А., Кондратьев В.Н.* Методы программной реализации алгоритмов логического управления для судовых микропроцессорных систем. Л.: Ин-т повышения квалификации руководящих работников и специалистов судостроительной промышленности, 1990.
14. *Кондратьев В.Н., Шалыто А.А.* Реализация систем булевых функций с использованием линейных арифметических полиномов // АиТ. 1993. № 3. С. 135–151.
15. *Бутаков Е.А.* Методы синтеза релейных устройств из пороговых элементов. М.: Энергия, 1970.
16. *Muroga S., Toda I., Kondo M.* Majority desion function of up to six variables // Mathematics of Computation. 1962. V. 16. Oct. № 80. P. 132–150.
17. *Артюхов В.Л., Розенблюм Л.Я., Шалыто А.А.* Логические возможности некоторых типов каскадных структур // Сети связи и дискретные устройства управления. М.: Наука, 1976. С. 138–144.
18. *Кузнецов Б.П., Шалыто А.А.* Система преобразований некоторых форм представления булевых функций // АиТ. 1985. № 11. С. 120–127.
19. *Артюхов В.Л., Кузнецов Б.П., Шалыто А.А.* Настраиваемые логические устройства для судовых управляющих систем. Л.: Ин-т повышения квалификации руководящих работников и специалистов судостроительной промышленности, 1986.
20. *Akers S.B.* Binary decision diagrams // IEEE Trans. on Computers. 1978. № 6. P. 509–516.

Поступила в редакцию 15.11.94

Российская академия наук

Автоматика и Телемеханика

Журнал основан в 1936 году
Выходит 12 раз в год

1
ЯНВАРЬ
·Наука·Москва
1996