УДК 519.713

ПОЛИНОМИАЛЬНОЕ РАЗЛОЖЕНИЕ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ

В. П. Супрун, А. М. Седун
Беларусь, Минск, БГУ, БГЭУ

Предлагаются методы разложения монотонной булевой функции n переменных в канонический полином Жегалкина $P(F)$ и в арифметический полином $G(F)$. Методы ориентированы на преобразование множества нижних единиц $N_1(F)$ в искомые полиномы. При этом не требуется построение таблицы истинности монотонной булевой функции F. Применение методов иллюстрируется примерами.

Введение

Известно [1], что задача построения полинома Жегалкина $P(F)$ для произвольных булевых функций n переменных является весьма трудоемкой. То же самое относится и к задаче построения арифметических полиномов $G(F)$. Трудоемкость универсальных методов полиномиального разложения булевых функций имеет экспоненциальную (относительно n) сложность. В этой связи является целесообразной разработка эффективных методов полиномиального разложения, ориентированных на относительно узкие классы булевых функций. В частности, в работах [2,3] предлагаются методы построения полиномов $P(F)$ и $G(F)$ для симметрических булевых функций n переменных.

В настоящей работе рассматривается класс монотонных булевых функций, зависящих от n переменных, и для таких функций предлагаются эффективные методы построения полиномов $P(F)$ и $G(F)$.

1. Основные понятия и определения

При задании монотонной булевой функции n переменных F важное значение имеет понятие нижней единицы.

Пусть $a=(a_1, a_2, \ldots, a_n)$, $b=(b_1, b_2, \ldots, b_n)$ и $c=(c_1, c_2, \ldots, c_n)$ - наборы значений переменных $x_1, x_2, \ldots, x_n$.

Набор $a=(a_1, a_2, \ldots, a_n)$ называется ***нижней единицей*** монотонной булевой функции $F=F(x_1, x_2, \ldots, x_n)$, если выполняются следующие условия: $F(a)=1$; если $a<b$, то $F(b)=1$; если $c<a$, то $F(c)=0$.

Произвольная монотонная булева функция n переменных $F=F(x_1, x_2, \ldots, x_n)$ взаимно однозначно определяется множеством всех своих нижних единиц $N_1(F)=\{a^1, a^2, \ldots, a^k\}$. Например, если $F\equiv 0$, то $N_1(F)=\varnothing$; если $F\equiv 1$, то $N_1(F)=\{00\ldots0\}$.

Далее, каждому набору $a=(a_1, a_2, \ldots, a_n)$ поставим в соответствие элементарную конъюнкцию $A=x_{i_1}x_{i_2}\ldots x_{i_m}$, где $i_1, i_2, \ldots, i_m$ – номера единичных компонент набора $a=(a_1, a_2, \ldots, a_n)$.

Множество нижних единиц $N_1(F)=\{a^1, a^2, \ldots, a^k\}$ монотонной булевой функции F определяет ее сокращенную ДНФ, т.е. имеет место $СкДНФ F = A^1 \vee A^2 \vee \ldots \vee A^k$.

2. Построение полинома Жегалкина $P(F)$

Пусть $N_1(F)=\{a^1, a^2, \ldots, a^k\}$ – множество нижних единиц монотонной булевой функции $F=F(x_1, x_2, \ldots, x_n)$. Сформируем последовательность из $k+1$ монотонных булевых функций $F_0, F_1, \ldots, F_j, \ldots, F_k$, где $N_1(F_0)=\varnothing$, $N_1(F_j)=N_1(F_{j-1})\cup\{a^j\}$ и $j=1, 2, \ldots, k$. Из определения следует, что $F_j=F_{j-1}\vee A^j$ и $F_k=F$.

Так как $F_j=F_{j-1}\vee A^j$ и известно, что $X\vee Y=X\oplus Y\oplus XY$, то

$$P(F_j)=P(F_{j-1})\oplus A^j\oplus P(F_{j-1})A^j. \qquad (1)$$

Из формулы (1) следует, что для построения полинома $P(F_j)$ необходимо: 1) занести в полином $P(F_j)$ все слагаемые полинома $P(F_{j-1})$ и конъюнкцию A^j; 2) занести в полином $P(F_j)$ результат пе-

ремножения полинома $P(F_{j-1})$ на конъюнкцию A^j; 3) удалить из полинома $P(F_j)$ попарно одинаковые слагаемые.

Предлагаемый метод построения полинома Жегалкина $P(F)$ заключается в последовательном построении полиномов $P(F_0), P(F_1), P(F_2), \ldots, P(F_j), \ldots, P(F_k)$, где $P(F_0)=0$ и $P(F_k)=P(F)$.

Применение данного метода продемонстрируем на следующем примере.

Пример 1. Пусть $F=F(x_1,x_2,\ldots,x_6)$ - монотонная булева функция и $N_1(F)=\{110000, 101110, 001101, 000111\}$. Положим, что требуется построить полином $P(F)$.

Непосредственно из множества $N_1(F)$ следует, что

$$F=A^1\vee A^2\vee A^3\vee A^4=x_1x_2\vee x_1x_3x_4x_5\vee x_3x_4x_6\vee x_4x_5x_6.$$

Далее, в соответствии с приведенным выше методом, получаем

$$P(F_0)=0,\quad P(F_1)=P(F_0)\oplus A^1\oplus P(F_0)A^1=x_1x_2,$$

$$P(F_2)=P(F_1)\oplus A^2\oplus P(F_1)A^2=x_1x_2\oplus x_1x_3x_4x_5\oplus x_1x_2x_3x_4x_5,$$

$$P(F_3)=P(F_2)\oplus A^3\oplus P(F_2)A^3=(x_1x_2\oplus x_1x_3x_4x_5\oplus x_1x_2x_3x_4x_5)\oplus x_3x_4x_6\oplus$$
$$\oplus(x_1x_2x_3x_4x_6\oplus x_1x_3x_4x_5x_6\oplus x_1x_2x_3x_4x_5x_6)=x_1x_2\oplus x_1x_3x_4x_5\oplus$$
$$\oplus x_1x_2x_3x_4x_5\oplus x_3x_4x_6\oplus x_1x_2x_3x_4x_6\oplus x_1x_3x_4x_5x_6\oplus x_1x_2x_3x_4x_5x_6,$$

$$P(F_4)=P(F_3)\oplus A^4\oplus P(F_3)A^4=(x_1x_2\oplus x_1x_3x_4x_5\oplus x_1x_2x_3x_4x_5\oplus x_3x_4x_6\oplus$$
$$\oplus x_1x_2x_3x_4x_6\oplus x_1x_3x_4x_5x_6\oplus x_1x_2x_3x_4x_5x_6)\oplus x_4x_5x_6\oplus(x_1x_2x_4x_5x_6\oplus$$
$$\oplus x_1x_3x_4x_5x_6\oplus x_1x_2x_3x_4x_5x_6\oplus x_3x_4x_5x_6\oplus x_1x_2x_3x_4x_5x_6\oplus x_1x_3x_4x_5x_6\oplus$$
$$\oplus x_1x_2x_3x_4x_5x_6=x_1x_2\oplus x_1x_3x_4x_5\oplus x_1x_2x_3x_4x_5\oplus x_3x_4x_6\oplus x_1x_2x_3x_4x_6\oplus$$
$$\oplus x_1x_3x_4x_5x_6\oplus x_4x_5x_6\oplus x_1x_2x_4x_5x_6\oplus x_3x_4x_5x_6.$$

Так как $P(F)=P(F_4)$, то искомый полином получен. Отметим, что полином $P(F)$ содержит 9 слагаемых и его степень (максимальный ранг

3. Оценка сложности полинома Жегалкина $P(F)$

Под сложностью полинома $P(F)$ понимается, как правило, число слагаемых (элементарных конъюнкций). Сложность полинома $P(F)$ обозначается через $d(P(F))$. Если F – монотонная булева функция, зависящая от n переменных, то значение $d(P(F))$ зависит не только от числа переменных n, но и от числа ее нижних единиц m.

Обозначим через $D(m)$ сложность $d(P(F))$ полинома $P(F)$ некоторой монотонной булевой функции F, число нижних единиц которой равно m. Для оценки сверху значения $D(m)$ воспользуемся формулой (1), из которой следует, что $D(m) \le 2D(m-1)+1$. Так как $D(1)=1$, то имеет место следующая цепочка неравенств:

$$D(m) \le 2D(m-1)+1 \le 2(2D(m-2)+1)+1 =$$
$$= 2^2 D(m-2)+2+1 \le 2^3 D(m-3)+2^2+2^1+2^0 \le \ldots$$
$$\ldots \le 2^{m-1}D(1)+2^{m-2}+\ldots+2^2+2^1+2^0 = 2^m-1.$$

Следовательно, доказано, что $D(m) \le 2^m - 1$. Это означает, что полином Жегалкина $P(F)$ монотонной булевой функции F из примера 1 может иметь не более 15 слагаемых.

4. Построение арифметического полинома $G(F)$

Основная идея метода построения арифметического полинома $G(F)$ позаимствована у приведенного выше метода построения полинома $P(F)$.

Поскольку $F_j = F_{j-1} \vee A^j$ и $X \vee Y = X + Y - XY$, то

$$G(F_j) = G(F_{j-1}) + A^j - G(F_{j-1})A^j. \qquad (2)$$

Согласно формуле (2) полином $G(F_j)$ формируется на основе полинома $G(F_{j-1})$ по следующим правилам: 1) занести все слагаемые по-

линома $G(F_{j-1})$ и слагаемое A^j в полином $G(F_j)$; 2) вычесть из полинома $G(F_j)$ результат умножения полинома $G(F_{j-1})$ на слагаемое A^j; 3) привести подобные слагаемые в полиноме $G(F_j)$.

По аналогии с методом построения полинома Жегалкина $P(F)$, метод построения арифметического полинома $G(F)$ заключается в последовательном построении полиномов $G(F_0)$, $G(F_1)$, $G(F_2)$, ... , $G(F_j)$, ... , $G(F_k)$, где $G(F_0)=0$ и $G(F_k)=G(F)$.

Рассмотрим пример применения метода построения полинома $G(F)$ для монотонной булевой функции F.

Пример 2. Предположим, что требуется построить арифметический полином $G(F)$ для монотонной функции $F=F(x_1,x_2,...,x_6)$, приведенной в примере 1.

Тогда $G(F_0)=0$, $G(F_1)=G(F_0)+A^1-G(F_0)A^1=x_1x_2$,

$$G(F_2)=G(F_1)+A^2-G(F_1)A^2=x_1x_2+x_1x_3x_4x_5-x_1x_2x_3x_4x_5,$$

$$G(F_3)=G(F_2)+A^3-G(F_2)A^3=(x_1x_2+x_1x_3x_4x_5-x_1x_2x_3x_4x_5)+x_3x_4x_6-$$
$$-(x_1x_2x_3x_4x_6+x_1x_3x_4x_5x_6-x_1x_2x_3x_4x_5x_6)=x_1x_2+x_1x_3x_4x_5-$$
$$-x_1x_2x_3x_4x_5+x_3x_4x_6-x_1x_2x_3x_4x_6-x_1x_3x_4x_5x_6+x_1x_2x_3x_4x_5x_6,$$

$$G(F_4)=G(F_3)+A^4-G(F_3)A^4=(x_1x_2+x_1x_3x_4x_5-x_1x_2x_3x_4x_5+x_3x_4x_6-$$
$$-x_1x_2x_3x_4x_6-x_1x_3x_4x_5x_6+x_1x_2x_3x_4x_5x_6)+x_4x_5x_6-(x_1x_2x_4x_5x_6+$$
$$+x_1x_3x_4x_5x_6-x_1x_2x_3x_4x_5x_6+x_3x_4x_5x_6-x_1x_2x_3x_4x_5x_6-x_1x_3x_4x_5x_6+$$
$$+x_1x_2x_3x_4x_5x_6)=x_1x_2+x_1x_3x_4x_5-x_1x_2x_3x_4x_5+x_3x_4x_6-x_1x_2x_3x_4x_6-$$
$$-x_1x_3x_4x_5x_6+x_4x_5x_6-x_1x_2x_4x_5x_6-x_3x_4x_5x_6+2x_1x_2x_3x_4x_5x_6.$$

Таким образом, арифметический полином $G(F)$ содержит 10 слагаемых и его степень равна 6.

Заключение

Основное достоинство предлагаемых методов состоит в том, что построение полиномов $P(F)$ и $G(F)$ монотонных булевых функций

$F = F(x_1, x_2, .., x_n)$ осуществляется на основе преобразования множества нижних единиц $N_1(F)$ и при этом знание таблицы истинности функций F совсем не обязательно. В то время как универсальные методы построения полиномов $P(F)$ и $G(F)$ оперируют непосредственно с таблицей истинности реализуемых булевых функций F.

Предлагаемые в настоящей работе методы просты и удобны для их программной реализации. Подтверждением тому является программа построения полиномов $P(F)$ и $G(F)$ для монотонных булевых функций F, написанная на языке C++ в среде разработки Borland C++ Builder. Программа состоит из трех модулей: основного модуля; модуля ввода данных; модуля дополнительной информации. Модули реализованы в виде экранных форм с расположенными на них элементами ввода и управления. Результатом выполнения программы является построение полинома $P(F)$, полинома $G(F)$, в зависимости от выбора соответствующей задачи пользователем.

В последнее время при проектировании дискретных устройств все большее внимание уделяется базисам, в которых вместо элемента ИЛИ используются элементы СЛОЖЕНИЕ ПО МОДУЛЮ ДВА [4]. Кроме того, наряду с ПЛМ типа И-ИЛИ-НЕ, возможно использование ПЛМ типа И-ИСКЛЮЧАЮЩЕЕ ИЛИ (AND-XOR) [5]. В этой связи возникают новые задачи синтеза логических схем и представляет практический интерес разработка методов логического синтеза, основанных на полиномиальном представлении реализуемых булевых функций.

Литература

1. Поспелов Д.А. Логические методы анализа и синтеза схем. М.: Энергия, 1974. –368 с.

2. Супрун В.П. Полиномиальное разложение симметрических булевых функций // Известия АН СССР. Техническая кибернетика. - 1985. - N 4. - С.123-127.

3. Супрун В.П., Мачикенас Э.К. Арифметическое разложение симметрических булевых функций. - В кн.: "Вычислительная техника", Вильнюс. - 1989. - С.148-151.

4. Закревский А.Д., Торопов Н.Р. Полиномиальная реализация частичных булевых функций и систем. - Минск: ИТК НАН Беларуси, 2001. - 200 с.

5. Sasao T., Bessiich Ph. On the complexity of MOD-2 sum PLA's // IEEE Trans. on Comput., Vol. 39, N 2, 1990, pp. 262-266.