О.А. Ф и н ь к о (Краснодар, каф. КТиИБ КубГТУ). **Реализация систем булевых функций посредством мультипликативных арифметико-логических форм.**

Интенсивные логические вычисления применяются при решении задач криптографии и логического проектирования интегральных схем. В [1] параллельные логические вычисления предлагается выполнять посредством арифметических полиномов, которые в [2] развиты в модулярные полиномиальные арифметико-логические формы. Известные арифметические методы реализации систем булевых функций — полиномиальные. Рассмотрим одну из альтернатив.

Арифметическая нормальная форма произвольной булевой функции $f_k(X)$ имеет вид:

$$f_k(X) = \sum_{i=0}^{2^n-1} r_{k,\,i}\, x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}, \tag{1}$$

где $r_{k,\,i} \in \mathbb{Z}$; $X = x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$ — все произведения булевых переменных (j_1, j_2, … j_n — все двоичные представления).

Утверждение. *Произвольная система булевых функций $f_1(X)$, $f_2(X)$, …, $f_d(X)$ может быть единственным способом задана арифметическим выражением*

$$\begin{aligned} N(X) &= m_1^{f_1(X)} m_2^{f_2(X)} \dots m_d^{f_d(X)} = \\ &= \left| \nu_0 \prod_{i=1}^{2^n-1} \nu_i^{x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}} \right|_p, \end{aligned} \tag{2}$$

где

$$\begin{aligned} \nu_0 &= \left| m_1^{r_{1,\,0}} m_2^{r_{2,\,0}} \dots m_d^{r_{d,\,0}} \right|_p, \\ \nu_1 &= \left| m_1^{r_{1,\,1}} m_2^{r_{2,\,1}} \dots m_d^{r_{d,\,1}} \right|_p, \\ &\dots \\ \nu_{2^n-1} &= \left| m_1^{r_{1,\,2^n-1}} m_2^{r_{2,\,2^n-1}} \dots m_d^{r_{d,\,2^n-1}} \right|_p; \end{aligned}$$

$|\cdot|_p$ *— наименьший неотрицательный вычет $\cdot$ по модулю p; p — простое такое, что $p > m_1 m_2 \dots m_d$; m_k ($k = 1, 2, \dots, d$) — простые числа; $r_{k,\,i}$ ($k = 1, 2, \dots, d$; $i = 0, 1, \dots, 2^n - 1$) — коэффициенты арифметического полинома (1).*

Единственность (2) следует из 1) свойств разложения числа на простые множители, 2) единственности (1) и 3) соблюдения условия простоты p (вычисления (2) выполняются в простом поле).

Свойство. *Значение k-й булевой функции системы $f_1(X)$, $f_2(X)$, …, $f_d(X)$ определяется проверкой условия делимости:*

$$f_k(X) = \begin{cases} 1, & m_k | \nu(X), \\ 0, & m_k \not| \nu(X). \end{cases} \tag{3}$$

Реализация проверки (3) будет менее сложной, если учитывать признаки делимости используемого представления $\nu(X)$. Развитие (2) на область k-значных функций из-за замены проверки (3) факторизацией $\nu(X)$ не целесообразно. По отношению к полиномиальным формам представление (2) может быть предпочтительным при реализации вычислений с недвоичными представлениями данных.

СПИСОК ЛИТЕРАТУРЫ

1. *Малюгин В. Д.* Параллельные логические вычисления посредством арифметических полиномов. — М.: Наука. Физматлит, 1997.
2. *Финько О. А.* Реализация систем булевых функций большой размерности методами модулярной арифметики // Автоматика и телемеханика. 2004. № 6. С. 37–60.