А. К. Вишневский, **О. А. Финько** (Краснодар, КВВУ). **Реализация систем подстановок числовыми полиномами.**

Числовые формы реализации *булевых функций* (БФ) и систем в ряде случаев имеют преимущества при технической реализации [1–3], а именно, по распараллеливанию и контролю ошибок логических вычислений [2,3]. Операция подстановки степени $k = 2^{\log k}$ является важной для области криптографии [4]. Поэтому имеет смысл рассмотреть особенности ее числовой реализации, интерпретируя одну подстановку как систему $2^{\log k}$ БФ. Конкретнее, рассмотрим систему подстановок

$$\boldsymbol{\sigma}_1 = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma_1^{(1)} & \sigma_1^{(2)} & \dots & \sigma_1^{(k)} \end{pmatrix}, \dots, \ \boldsymbol{\sigma}_s = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma_s^{(1)} & \sigma_s^{(2)} & \dots & \sigma_s^{(k)} \end{pmatrix}, \qquad (1)$$

где $\sigma_t^{(i)}$, $i=1,2,\dots,k$, $t=1,2,\dots,s$, таковы, что $\sigma_t^{(i)} \neq \sigma_t^{(j)}$ при $i \neq j$. Тогда вектор булевых значений, принимаемых σ_t, обозначим $\vec{\boldsymbol{\sigma}}_t = (f_t^{(1)}(\vec{\mathbf{x}}_t), f_t^{(2)}(\vec{\mathbf{x}}_t), \dots, f_t^{(\log k)}(\vec{\mathbf{x}}_t))$, где $f_t^{(i)}(\vec{\mathbf{x}}_t)$ — БФ, определенная на векторе существенных булевых переменных $\vec{\mathbf{x}}_t = (x_t^{(1)}, x_t^{(2)}, \dots, x_t^{(\log k)})$. Соответственно, вектор $\vec{\boldsymbol{\sigma}} = (\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \dots, \boldsymbol{\sigma}_s)$ системы (1) подстановок интерпретируется как система БФ:

$$F(\vec{\mathbf{x}}_1, \vec{\mathbf{x}}_2, \dots, \vec{\mathbf{x}}_s) = F(\vec{\mathbf{x}}) = (f_1^{(1)}(\vec{\mathbf{x}}_1), \dots, f_1^{(\log k)}(\vec{\mathbf{x}}_1), \dots, f_s^{(1)}(\vec{\mathbf{x}}_s), \dots, f_s^{(\log k)}(\vec{\mathbf{x}}_s)). \qquad (2)$$

При этом лексикографический порядок упорядоченных существенных переменных $\vec{\mathbf{x}} = (x_1^{(1)}, \dots, x_1^{(\log k)}, \dots, x_s^{(1)}, \dots, x_s^{(\log k)})$ сохраняется для каждой $\boldsymbol{\sigma}_t$ в отдельности.

Пусть $P^{(\nu)}(\vec{\mathbf{x}}_t) = \sum_{i=1}^{k} a_i^{(\nu)} x_1^{i_1} x_2^{i_2} \cdots x_{\log k}^{i_{\log k}}$ — числовая нормальная форма [4] представления ν-й БФ $f_t^{(\nu)}(\vec{\mathbf{x}}_t)$ (2), где $a_i = 0, 1, \dots, k$, $k = 2^{\log k}$, $i_j \in \{0, 1\}$ ($j = 1, 2, \dots, \log k$), $x_1^{i_1} x_2^{i_2} \cdots x_{\log k}^{i_{\log k}}$ — попарно различные элементарные конъюнкции (мономы). Тогда подсистема БФ $f_t^{(1)}(\vec{\mathbf{x}}_t), f_t^{(2)}(\vec{\mathbf{x}}_t), \dots, f_t^{(\log k)}(\vec{\mathbf{x}}_t)$, соответствующая подстановке $\boldsymbol{\sigma}_t$, может быть реализована одним числовым полиномом (ЧП): $Y_t = D_t(\vec{\mathbf{x}}_t) = \sum_{\nu=1}^{\log k} 2^{\nu} P_t^{(\nu)}(\vec{\mathbf{x}}_t) = \sum_{i=1}^{k} c_i x_{t,1}^{i_1} x_{t,2}^{i_2} \cdots x_{t,\log k}^{i_{\log k}}$, где $c_i \in \mathbf{Z}$. Вычисление $D_t(\vec{\mathbf{x}}_t)$ дает целое $Y_t \in \{0, 1, \dots, 2^{\log k}\}$, которое при представлении $Y_t = (y_t^{(1)} y_t^{(2)} \cdots y_t^{(\log k)})$ в двоичной системе счисления дает результат вычисления системы $\boldsymbol{\sigma}_t$, т. е. $y_t^{(1)} = f_t^{(\log k)}(\vec{\mathbf{x}}_t), y_t^{(2)} = f_t^{(\log k - 1)}(\vec{\mathbf{x}}_t), \dots, y_t^{(\log k)} = f_t^{(1)}(\vec{\mathbf{x}}_t)$.

Наконец, система (1) посредством (2) может быть реализована одним ЧП:

$$Y = H(\vec{\mathbf{x}}_t) = \sum_{t=1}^{s} 2^{(t-1)\log k} D_t(\vec{\mathbf{x}}_t) = \sum_{\substack{i=1,\dots,k \\ t=1,\dots,s}} d_{t,i} x_{t,1}^{i_1} x_{t,2}^{i_2} \cdots x_{t,\log k}^{i_{\log k}} \pmod m, \qquad (3)$$

где $d_{t,j} \in \mathbf{Z}_m$, $m = 2^{s \log k}$, $Y = (y_1 y_2 \dots y_{s \log k})_2$ — представление числа Y в двоичной системе счисления, в разрядах $y_1, y_2, \dots, y_{s \log k}$ которого размещены результаты вычисления БФ (2): $y_1 = f_s^{(\log k)}(\vec{\mathbf{x}}_s), y_2 = f_s^{(\log k - 1)}(\vec{\mathbf{x}}_s), \dots, y_{\log k} = f_s^{(1)}(\vec{\mathbf{x}}_s)$, $\dots, y_{(s-1)\log k + 1} = f_1^{(\log k)}(\vec{\mathbf{x}}_1), y_{(s-1)\log k + 2} = f_1^{(\log k - 1)}(\vec{\mathbf{x}}_2), \dots, y_{s \log k} = f_1^{(1)}(\vec{\mathbf{x}}_1)$.

Верхняя граница L длины ЧП (3) равна $s(2^{\log k} - 1) + 1$, что в $u = 2^{s \log k} / (s(2^{\log k} - 1) + 1)$ раз меньше максимальной длины ЧП для $s \log k$ переменных. Например, при $k = 16$, $s = 8$ (соответствует подстановке в ГОСТ 28.147-89) $L = 121$, $u \approx 35495598$.

СПИСОК ЛИТЕРАТУРЫ

1. *Малюгин В. Д.* Параллельные логические вычисления посредством арифметических полиномов. М.: Наука, 1997, 192 с.
2. *Финько О. А.* Модулярная арифметика параллельных логических вычислений. М.: ИПУ РАН, 2003, 224 с.
3. *Финько О. А.* Реализация систем булевых функций большой размерности методами модулярной арифметики. — Автомат. и телемех., 2004, № 6, с. 37-60.
4. *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004, 470 с.