АРИФМЕТИЗАЦИЯ ЛОГИЧЕСКОГО РАЗЛОЖЕНИЯ ПОСПЕЛОВА ДЛЯ ОПТИМИЗАЦИИ СТРУКТУРЫ МАТЕМАТИЧЕСКОГО СОПРОЦЕССОРА

Щербаков А.В., Финько О.А.

Краснодарское высшее военное училище
Россия, 350035, Краснодар, Красина ул., 4
E-mail: ofinko@yandex.ru

Рассмотрен арифметический аналог логического разложения Поспелова (обобщенного разложения Шеннона), который позволяет оптимизировать структуру реализующего его математического сопроцессора.

Математические, в частности логические, сопроцессоры (ЛС) широко применяются для получения требуемых характеристик шифрования информации в защищенных информационных системах. Проблемой построения таких вычислителей является трудность обеспечения ряда противоречивых требований: высокой функциональной гибкости, производительности и достоверности функционирования.

Решить данную проблему позволяют ЛС, основанные на реализации арифметико-логических моделей (АЛМ) типовых криптографических функций [1, 2].

Если считать, что максимальная вычислительная мощность ЛС устанавливается исходя из максимальной сложности реализуемых АЛМ, то архитектура ЛС будет оптимальной при условии, если сложность всех реализуемых АЛМ всегда одинакова. Однако это противоречит требованиям к гибкости функционирования ЛС. В реальных условиях значительная часть оборудования ЛС будет *простаивать*.

В теории автоматов в таких случаях применяют методы *логической* декомпозиции булевых функций, например основанных на разложении Шеннона [3] или его обобщении — разложении Поспелова [4]. Однако для ЛС, реализующих АЛМ, эти положения нельзя применить *напрямую*.

Ц е л ь р а б о т ы : построение арифметического аналога логического разложения Поспелова и исследование его свойств для оптимизации структуры ЛС.

Арифметизация логических разложений Шеннона и Поспелова. Под арифметическим представлением системы булевых функций:

$$F(X)=\begin{cases} f_1(x_1,\ldots,x_n),\\ f_2(x_1,\ldots,x_n),\\ \ldots\\ f_i(x_1,\ldots,x_n), \end{cases}$$

где $f_i(X)\in\{0,1\}$; $x_j\in\{0,1\}$, будем понимать арифметический полином:

$$D(X)=c_0+c_1x_1+c_2x_2+\ldots+c_{2^n-1}x_1x_2\ldots x_n;\ \ c_i\in\mathbf{Z}.$$

Разложение Шеннона по одной переменной имеет вид [3]:

$$f(X)=x_i f_1^{(i)}(X)\vee\bar{x}_i f_0^{(i)}(X). \qquad (1)$$

Обобщение (1) на произвольное количество переменных дает разложение Поспелова [4]:

$$f(x_1,\ldots,x_i,x_{i+1},\ \ldots,x_n)=\bigvee x_1^{a_1}x_2^{a_2}\ldots x_i^{a_i}f(a_1,a_2,\ldots,a_i,x_{i+1},\ldots,x_n), \qquad (2)$$

где $x_i^{a_i}$ — степень аргумента x_i, a_i — двоичная переменная величина такая, что

$$x_i^{a_i}=\begin{cases} x_i, & \text{если}\quad a_i=1,\\ \bar{x}_i, & \text{если}\quad a_i=0. \end{cases}$$

Обобщим (1) на случай АЛМ. Для этого в (1) произведем подстановку:

$$\begin{aligned} &\bar{x}=1-x,\quad F(x_1,\ldots,x_n)=D(x_1,\ldots,x_n),\\ &F_{\,|\,x_i=1}(x_1,\ldots,x_n)=D_{\,|\,x_i=1}(x_1,\ldots,x_{i-1},1,x_{i+1},\ldots,x_n),\\ &F_{\,|\,x_i=0}(x_1,\ldots,x_n)=D_{\,|\,x_i=0}(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n):\\ &F(x_1,\ldots,x_n)=x_iF_{\,|\,x_i=1}(x_1,\ldots,x_n)+(1-x_i)F_{\,|\,x_i=0}(x_1,\ldots,x_n)=\\ &=x_iD_{\,|\,x_i=1}(x_1,\ldots,x_{i-1},1,x_{i+1},\ldots,x_n)+(1-x_i)D_{\,|\,x_i=0}(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n), \end{aligned} \qquad (3)$$

где с учетом $x_i=1$:

$$D_{|x_i=1}(x_1,\ldots,x_n)=c_0+\sum_{j=1}^{2^n-1}c_j x_1x_2\ldots x_{i-1}\,1\,x_{i+1}\ldots x_n\ ,$$

а с учетом $x_i=0$:

$$D_{|x_i=0}(x_1,\ldots,x_n)=c_0+\sum_{j=1}^{2^n-1}c_j x_1x_2\ldots x_{i-1}\,0\,x_{i+1}\ldots x_n.$$

Разложение (3) будем называть ***арифметическим аналогом логического разложения Шеннона*** (термин заимствован у В.П. Шмерко) графическая интерпретация которого, представлена на рис. 1.

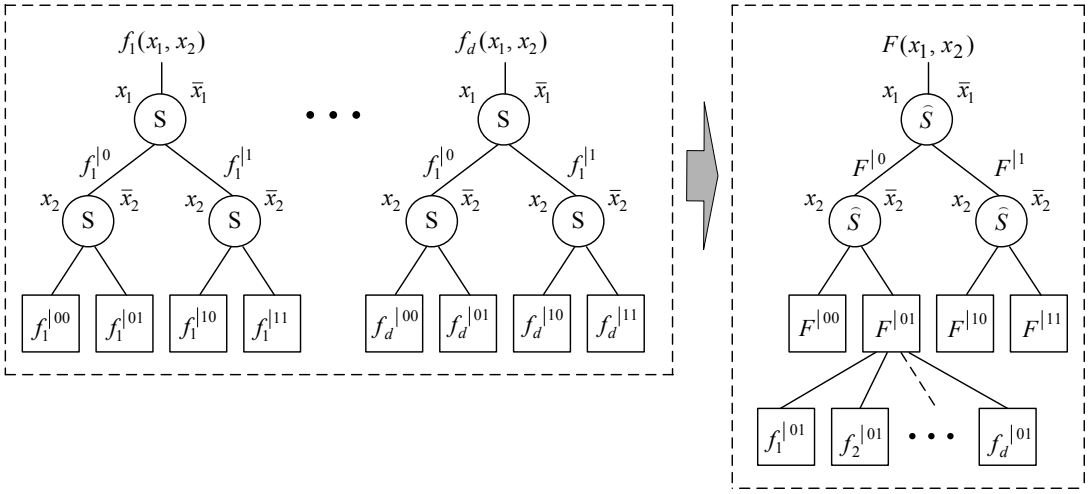


Рис. 1. Демонстрация (граф) логического (часть рисунка слева) разложения **Шеннона** и его арифметического аналога (справа) применительно к *системе* булевых функций

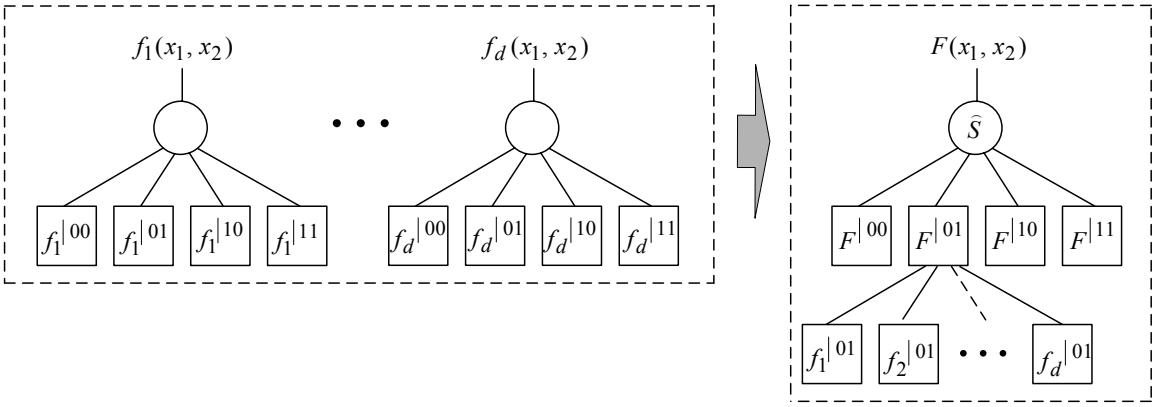


Рис. 2. Демонстрация (граф) логического (часть рисунка слева) разложения **Поспелова** и его арифметического аналога (справа) применительно к *системе* булевых функций

Произведем те же действия и для логического разложения Поспелова. Обобщим (4) на случай АЛМ. Для этого в (2) произведем подстановку:

$$F(x_1,\ldots,x_i,x_{i+1},\ldots,x_n)=D(x_1,\ldots,x_i,x_{i+1},\ldots,x_n);$$

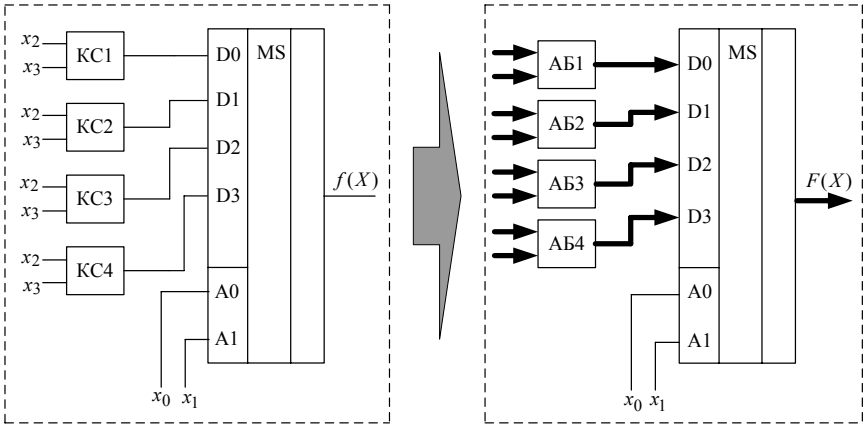
$$\boxed{\begin{aligned}F(x_1,\ldots,x_i,x_{i+1},\ldots,x_n)&=\bigvee x_1^{a_1}x_2^{a_2}\ldots x_i^{a_i}F(a_1,a_2,\ldots,a_i,x_{i+1},\ldots,x_n)=\\&=\bigvee x_1^{a_1}x_2^{a_2}\ldots x_i^{a_i}D(a_1,a_2,\ldots,a_i,x_{i+1},\ldots,x_n),\end{aligned}} \qquad (4)$$

где

$$D(x_1,\ldots,x_i,x_{i+1},\ldots,x_n)=c_0+\sum_{j=1}^{2^n-1}c_j a_1a_2\ldots a_i x_{i+1}\ldots x_n\ .$$

Разложение (4) будем называть ***арифметическим аналогом логического разложения Поспелова*** графическая интерпретация которого, поясняется с помощью рис. 2.

Идентификация и оптимизация структуры ЛС. При схемной реализации структура неоптимизированного ЛС выглядит следующим образом (рис. 3):



(а) (б)

КС – комбинационная схема, АБ – арифметический блок

Рис. 3. Традиционное применение логического разложения Поспелова для декомпозиции логической схемы (а) и «прямое» применение его арифметического аналога для декомпозиции ЛС, реализующего АЛМ (б)

Структура неоптимизированного ЛС (рис. 3 б), основанная на арифметическом разложении Поспелова, состоит из *идентичных* арифметических блоков (АБ) и мультиплексора. Эта особенность может быть использована для оптимизации ЛС.

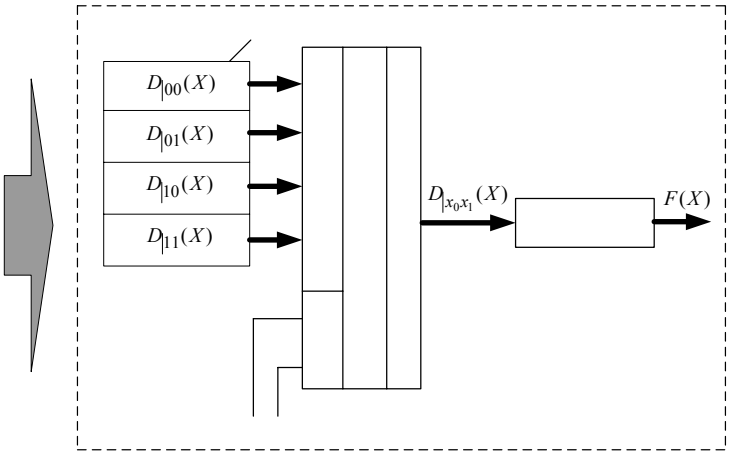


Рис. 4. Структура ЛС, учитывающая специфику «арифметизированного» разложения Поспелова

Структура ЛС, учитывающего особенности «арифметизированного» разложения Поспелова, представлена на рис. 4. В отличие от ЛС, представленного на рис. 3, этот ЛС содержит только один арифметический блок. Сокращение числа арифметических блоков стало возможным благодаря новым свойствам АЛМ. Если традиционный способ аппаратурной реализации булевых функций предполагал их уникальное отражение в схеме устройства, то при использование АЛМ уникальность булевых функций (систем) отражается в значениях коэффициентов арифметических полиномов, которые имеют каноническую форму. Таким образом, для смены реализуемой функции не требуется изменения реализующей ее аппаратной части, а достаточно изменить набор коэффициентов арифметического полинома.

ЛИТЕРАТУРА

1. Финько О.А. Модулярная арифметика параллельных логических вычислений: Монография / Под ред. В.Д. Малюгина. — М.: ИПУ РАН, 2003. — 224 с.
2. Малюгин В.Д. Параллельные логические вычисления посредством арифметических полиномов. — М.: Наука. Физматлит, 1997. — 192 с.

3. Шеннон К. Синтез двухполюсных переключательных схем. В кн.: Шеннон К. Работы по теории информации и кибернетике. — М.: Иностранная литература, 1963.
4. Поспелов Д.А. Логические методы анализа и синтеза схем. — М.: Энергия, 1964.

ARITHMETIZATION OF LOGICAL EXPANSION OF POSPELOV FOR OPTIMIZATION OF STRUCTURE OF THE MATH COPROCESSOR

ShCherbakov A., Finko O.

Krasnodar higher military school
Russia, 350035, Krasnodar, street Krasina, 4
E-mail: ofinko@yandex.ru

Abstract. The arithmetical analog of logical expansion of Pospelov (the generalized expansion of Shannon) which allows to optimize structure of the math coprocessor realizing it is considered.

In the protected intelligence systems mathematical (logical) coprocessors (LC) are widely applied to reaching required performances of encoding of the information. A problem of construction such вычислителей is difficulty of security of some contradictory requirements: high functional flexibility, efficiency and reliability of operation.

T h e p u r p o s e : construction of arithmetical analog of logical expansion of Pospelov (the generalized expansion of Shannon) and research of his properties for optimization of structure LC.

Under arithmetical representation of a system of Boolean functions: $F(X) = f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_i(x_1, \ldots, x_n),$ where $f_i(X) \in \{0, 1\}; x_j \in \{0, 1\}$, we shall understand an arithmetical polynomial: $D(X) = c_0 + c_1 x_1 + c_2 x_2 + \ldots + c_{2^n-1} x_1 x_2 \ldots x_n; c_i \in \mathbf{Z}$.

Expansion $F(x_1, \ldots, x_n) = x_i F_{|x_i=1}(x_1, \ldots, x_n) + (1 - x_i) F_{|x_i=0}(x_1, \ldots, x_n) =$

$= x_i D_{|x_i=1}(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) + (1 - x_i) D_{|x_i=0}(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$

let's name ***as arithmetical analog of logical expansion of Shannon*** (the term is borrowed for V.P. Shmerko), where with the registration $x_i = 1$:

$$D_{|x_i=1}(x_1, \ldots, x_n) = c_0 + \sum_{j=1}^{2^n-1} c_j x_1 x_2 \ldots x_{i-1}\, 1\, x_{i+1} \ldots x_n$$

and with the registration $x_i = 0$:

$$D_{|x_i=0}(x_1, \ldots, x_n) = c_0 + \sum_{j=1}^{2^n-1} c_j x_1 x_2 \ldots x_{i-1}\, 0\, x_{i+1} \ldots x_n.$$

Expansion

$$\begin{aligned} F(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n) &= \bigvee x_1^{a_1} x_2^{a_2} \ldots x_i^{a_i} F(a_1, a_2, \ldots, a_i, x_{i+1}, \ldots, x_n) = \\ &= \bigvee x_1^{a_1} x_2^{a_2} \ldots x_i^{a_i} D(a_1, a_2, \ldots, a_i, x_{i+1}, \ldots, x_n), \end{aligned} \qquad (1)$$

where $D(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n) = c_0 + \sum_{j=1}^{2^n-1} c_j a_1 a_2 \ldots a_i x_{i+1} \ldots x_n$; $x_i^{a_i} = \begin{cases} x_i, & \text{если} \quad a_i = 1, \\ \bar{x}_i, & \text{если} \quad a_i = 0. \end{cases}$

let's name ***as arithmetical analog of logical expansion of Pospelov.***

Traditional application of logical expansion of Pospelov assumes decomposition of the logic circuit. LC, realizing (1) contains only one arithmetical block. Abbreviation of number of arithmetical blocks became possible due to new properties of arithmetical forms of representation of logical functions.