

ГЛАВА 2

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ МОДУЛЯРНОЙ АРИФМЕТИКИ

Под математической моделью вычислительного устройства понимается аналитическое представление, описывающее его поведение и реализуемые им функции, а также определяющее структуру устройства в зависимости от задаваемых параметров. Математическую модель можно рассматривать как средство для последующего анализа работы и верификации устройства. Таким образом, оптимальное в том или ином смысле описание является эффективным при решении задачи логического синтеза в целом. Например, число логических выражений определяет количество структурных элементов, входящих в состав логической схемы устройства, а суммарное число переменных, входящих в эти выражения – конструктивную сложность схемы (сложность по Квайну), т.е. сумму входов всех элементов логической схемы устройства.

Для эффективной реализации функциональных блоков вычислительной системы необходимо учитывать свойства операций, реализуемых системой. Например [58–60], применение свойств симметрии булевых функций вполне обосновано при реализации коммутативных операций сложения и умножения.

Материалы, изложенные в этой главе, посвящены построению математических моделей и аналитических представлений, предназначенных для реализации модулярных операций сложения и умножения над целыми числами.

Информацию, над которой производят вычисления в устройствах МА, часто кодируют с помощью двоичных позиционных или унитарных кодов [9, 45, 45, 48, 49, 51, 67, 110].

2.1 Модулярное сложение в позиционных кодах

Произвольное целое положительное число $X \pmod{P}$ в позиционном коде можно представить с помощью δ –разрядного двоичного набора $X = (x_1, x_2, \dots, x_\delta)$ в виде

$$X \pmod{P} = \sum_{k=1}^{\delta} 2^{k-1} x_k = 2^0 x_1 + 2^1 x_2 + \dots + 2^{\delta-1} x_\delta, \quad (2.1)$$

где $x_k \in \{0, 1\}$, $\delta = \lceil \log_2 P \rceil + 1$ и $P \geq 3$.

Известны различные способы представления положительных и отрицательных целых чисел в устройствах МА [48]. Как правило, они основаны на использовании «знакового разряда» или способа со «смещением», которые описаны, например, в [34]. Однако, как отмечалось в предыдущей главе, к достоинствам МА относится небольшая разрядность представляемых в МА чисел, которая обычно не превышает восьми разрядов [36, 71]. Увеличение разрядности представляемых чисел приведет к потере основного достоинства устройств МА – быстродействия. Имеет смысл использовать способ представления целых положительных и отрицательных чисел по модулю P , который назовем дополнением до P .

Пусть $X \pmod{P}$ целое положительное число, которое представляется в виде (2.1) и $-X \pmod{P} = S \pmod{P}$. Тогда $(S + X) \pmod{P} = 0 \pmod{P}$. Иначе говоря, S является искомым числом $-X$, которое необходимо прибавить к X , что бы в результате получить $P = 0 \pmod{P}$. В таком случае получим

$$-X \pmod{P} = 2^0 s_1 + 2^1 s_2 + \dots + 2^{\delta-1} s_\delta, \quad (2.2)$$

где $S = (s_1, s_2, \dots, s_\delta)$.

Например, представим число $-3 \pmod{5}$. Тогда $-3 \pmod{5} = S \pmod{5}$. Перенесем -3 в правую часть равенства и получим $(S + 3) \pmod{5} = 0 \pmod{5}$. Откуда следует, $S = 2$ и, учитывая (2.1), $-3 \pmod{5} = (0, 1, 0)$.

2.1.1 Модулярное сложение по модулю три

Перейдем к рассмотрению операции $X_1 + X_2 + \dots + X_N = S \pmod{3}$ [4-А, 16-А]. В соответствии с выбранным модулем $P = 3$ и $\delta = [\log_2 3] + 1 = 2$, операнды $X_1, X_2, \dots, X_N$ и результат их сложения S задаются двухразрядными двоичными наборами $X_n = (x_1^n, x_2^n)$, $S = (s_1, s_2)$, где $n = \overline{1, N}$. В таком случае справедлива следующая запись:

$$\sum_{n=1}^N X_n = \sum_{n=1}^N (x_1^n + 2x_2^n) = s_1 + 2s_2 = S \pmod{3}. \quad (2.3)$$

Операнды $X_1, X_2, \dots, X_N$ и результат их сложения S принимают значения 0, 1 и 2, что соответствует двоичным наборам (00), (10) и (01).

Учитывая (2.1) и (2.2), операнд X_n может быть представлен двухразрядным набором настроенных переменных (u_1^n, u_2^n) , т.е. $X_n = u_1^n + 2u_2^n$,

где $u_1^n, u_2^n \in \{x_1^n, x_2^n\}$. Тогда при соответствующей настройке операндов может быть выполнены одна (любая) из операций $\pm X_1 \pm X_2 \dots \pm X_N = S \pmod{3}$.

В качестве примера в таблице 2.1 приведена настройка операндов на выполнение одной (любой) из четырех операций $\pm X_1 \pm X_2 = S \pmod{3}$.

Таблица 2.1 – Таблица настройки операндов на реализацию операций $\pm X_1 \pm X_2 = S \pmod{3}$

Значения разрядов операндов				Выполняемая арифметическая операция
Значение первого операнда $X_1(u_1^1, u_2^1)$		Значение второго операнда $X_2(u_1^2, u_2^2)$		
u_1^1	u_2^1	u_1^2	u_2^2	
x_1^1	x_2^1	x_1^2	x_2^2	
x_2^1	x_1^1	x_1^2	x_2^2	$X_1 + X_2$
x_1^1	x_2^1	x_2^2	x_1^2	$-X_1 + X_2$
x_2^1	x_1^1	x_2^2	x_1^2	$X_1 - X_2$
x_1^1	x_2^1	x_1^2	x_2^2	$-X_1 - X_2$

В результате выполнения операции $X_1 + X_2 + \dots + X_N = S \pmod{3}$ формируются две булевы функции $S_1 = S_1(x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N)$ и $S_2 = S_2(x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N)$, принимающие значения разрядов s_1 и s_2 результата сложения $S = (s_1, s_2)$. Тогда

$$\sum_{n=1}^N X_n = \begin{cases} 3r = 0 \pmod{3}; \\ 3r + 1 = 1 \pmod{3}; \\ 3r + 2 = 2 \pmod{3}, \end{cases} \quad (2.4)$$

где $r = 0, 1, 2, \dots$

Поскольку $S \pmod{3} = s_1 + 2s_2$, то результат сложения N операндов $S \pmod{3}$ можно представить с помощью двоичной матрицы

$$M(S) = \begin{bmatrix} s_{0,1} & s_{0,2} \\ s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (2.5)$$

где строкам матрицы соответствуют двоичные значения, которые принимает результат сложения S , а число столбцов совпадает с числом разрядов $S \pmod{3}$.

Обозначим $S^* = X_1 + X_2 + \dots + X_N$, где $S^* \in \{0, 1, 2, \dots, 2N\}$. Так как $X_1, X_2, \dots, X_N \in \{0, 1, 2\}$, то результат сложения N операндов $S^* = S \pmod{3}$ можно представить с помощью двоичной матрицы $M(S^*)$, которая имеет вид

$$M(S^*) = \begin{bmatrix} s_{0,1} & s_{0,2} \\ s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \\ \dots & \dots \\ s_{i,1} & s_{i,2} \\ \dots & \dots \\ s_{2N,1} & s_{2N,2} \end{bmatrix}, \quad (2.6)$$

где $i = \overline{0, 2N}$. Строкам матрицы соответствуют двоичные значения $S^* \pmod{3}$, а число столбцов совпадает с числом разрядов $S^* \pmod{3}$.

Функция $S_1 = 1$ тогда и только тогда, когда $s_{i,1} = 1$, т.е. когда $S^* \in \{1, 4, \dots, 3k_1 - 2\}$, где $k_1 = \left\lfloor \frac{2N+2}{3} \right\rfloor$.

Функция $S_2 = 1$ тогда и только тогда, когда $s_{i,2} = 1$, т.е. когда $S^* \in \{2, 5, \dots, 3k_2 - 1\}$, где $k_2 = \left\lfloor \frac{2N+1}{3} \right\rfloor$.

Например, в результате сложения $X_1 + X_2 + X_3 = S \pmod{3}$, где $X_1, X_2, X_3 \in \{0, 1, 2\}$, матрица $M(S^*)$ имеет вид

$$M(S^*) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad (2.7)$$

где $S^* = X_1 + X_2 + X_3$ и $S^* \in \{0, 1, 2, \dots, 6\}$. Если $s_{1,1} = s_{4,1} = 1$, то $S^* \in \{1, 4\}$ и функция $S_1 = 1$. Если $s_{2,2} = s_{5,2} = 1$, то $S^* \in \{2, 5\}$ и функция $S_2 = 1$.

Разобьем множество переменных $x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N$ на два подмножества $Y_1 = \{x_1^1, x_1^2, \dots, x_1^N\}$ и $Y_2 = \{x_2^1, x_2^2, \dots, x_2^N\}$. Тогда значения функций $S_1 = S_1(Y_1, Y_2)$ и $S_2 = S_2(Y_1, Y_2)$ инвариантны относительно любой перестановки переменных внутри каждого из подмножеств Y_1 и Y_2 , т.е. переменные $x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N$ разбиваются на два класса симметрии.

На основании процедуры симметрирования, описанной в предыдущей главе, можно утверждать, что $S_1(Y_1, Y_2) = S_1(Y_1, Y_2, Y_2)$ и $S_2(Y_1, Y_2) = S_2(Y_1, Y_2, Y_2)$ являются СБФ, которые зависят от $3N$ переменных. В таком случае функции S_1 и S_2 можно представить локальными кодами $\pi(S_1) = (\pi_0^1, \pi_1^1, \dots, \pi_{2N}^1, \pi_{2N+1}^1, \dots, \pi_{3N}^1)$ и $\pi(S_2) = (\pi_0^2, \pi_1^2, \dots, \pi_{2N}^2, \pi_{2N+1}^2, \dots, \pi_{3N}^2)$ соответственно.

Так как $0 \leq S^* \leq 2N$, то $\pi_v^1 = \pi_v^2 = 0$, где $2N+1 \leq v \leq 3N$. Тогда локальные коды функций S_1 и S_2 имеет смысл записать в виде $\pi(S_1) = (\pi_0^1, \pi_1^1, \dots, \pi_{2N}^1) = (s_{0,1}, s_{1,1}, \dots, s_{2N,1})$ и $\pi(S_2) = (\pi_0^2, \pi_1^2, \dots, \pi_{2N}^2) = (s_{0,2}, s_{1,2}, \dots, s_{2N,2})$. Другими словами, значения $\pi(S_1)$ и $\pi(S_2)$ соответствуют первому и второму столбцам матрицы $M(S^*)$ соответственно.

Из вышесказанного следует, что множества рабочих чисел СБФ S_1 и S_2 равны $A(S_1) = \{1, 4, \dots, 3k_1 - 2\}$ и $A(S_2) = \{2, 5, \dots, 3k_2 - 1\}$.

Если к СБФ S_1 и S_2 применить разложение (1.6), то получим представления этих функций посредством дизъюнкции ФСБФ. Вышесказанное относительно модулярного сложения по модулю три можно подытожить следующим утверждением.

Утверждение 2.1. Если $N \geq 2$, то

$$\begin{aligned} S_1(Y_1, Y_2) &= \bigvee_{i=0}^{2N} \pi_i^1 \cdot F_{3N}^i(Y_1, Y_2, Y_2), \\ S_2(Y_1, Y_2) &= \bigvee_{j=0}^{2N} \pi_j^2 \cdot F_{3N}^j(Y_1, Y_2, Y_2), \end{aligned} \quad (2.8)$$

где $F = F_{3N}^i(Y_1, Y_2, Y_2)$ и $F = F_{3N}^j(Y_1, Y_2, Y_2)$ – ФСБФ, зависящие от $3N$ переменных, рабочие числа которых равны $3i-2$ и $3j-1$, соответственно,

$$k_1 = \left\lceil \frac{2N+2}{3} \right\rceil, \quad k_2 = \left\lceil \frac{2N+1}{3} \right\rceil, \quad i = 1, 2, \dots, k_1 \text{ и } j = 1, 2, \dots, k_2.$$

Отсюда следует, что

$$S_1 = \begin{cases} 1, \text{ если } \sum_{n=1}^N X_n = \sum_{n=1}^N (x_1^n + 2x_2^n) = i \cdot \pi_i^1; \\ 0 - \text{ в противном случае,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ если } \sum_{n=1}^N X_n = \sum_{n=1}^N (x_1^n + 2x_2^n) = j \cdot \pi_j^2; \\ 0 - \text{ в противном случае.} \end{cases} \quad (2.9)$$

Приведенные здесь аналитические представления функций S_1 и S_2 равносильны соответствующим формулам из (2.8).

Пример 2.1. Пусть $X_1 + X_2 = S \pmod{3}$ [35-А]. В таком случае матрица $M(S^*)$ имеет вид

$$M(S^*) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix},$$

где $S^* = X_1 + X_2$.

Если $s_{1,1} = s_{4,1} = 1$, то $S^* \in \{1, 4\}$ и функция $S_1 = 1$. Если $s_{2,2} = 1$, то $S^* \in \{2\}$ и функция $S_2 = 1$.

Запишем локальные коды функций S_1 и S_2 в виде $\pi(S_1) = (0, 1, 0, 0, 1)$ и $\pi(S_2) = (0, 0, 1, 0, 0)$. Тогда представления (2.8) для СБФ S_1 и S_2 , рабочие числа которых равны $A(S_1) = \{1, 4\}$ и $A(S_2) = \{2\}$, будут выглядеть следующим образом:

$$S_1(x_1^1, x_2^1, x_1^2, x_2^2) = F_6^1(x_1^1, x_2^1, x_1^2, x_2^2) \vee F_6^4(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2),$$

$$S_2(x_1^1, x_2^1, x_1^2, x_2^2) = F_6^2(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2),$$

где

$$F_6^1 = \begin{cases} 1, \text{ если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 = 1; \\ 0 - \text{ в противном случае,} \end{cases}$$

$$F_6^2 = \begin{cases} 1, \text{ если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 = 2; \\ 0 - \text{ в противном случае,} \end{cases}$$

$$F_6^4 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 = 4; \\ 0 & - \text{в противном случае.} \end{cases}$$

Произведя перекоммутацию переменных $x_1^1, x_2^1, x_1^2, x_2^2$, как показано в таблице 2.1, может быть реализована любая из четырех операций $\pm X_1 \pm X_2 = S \pmod{3}$.

Пример 2.2. Пусть $X_1 + X_2 + X_3 = S \pmod{3}$. Для этого случая матрица $M(S^*)$ принимает вид (2.7).

Запишем локальные коды функций S_1 и S_2 в виде $\pi(S_1) = (0, 1, 0, 0, 1, 0, 0)$ и $\pi(S_2) = (0, 0, 1, 0, 0, 1, 0)$. Тогда представления (2.8) для СБФ S_1 и S_2 , рабочие числа которых равны $A(S_1) = \{1, 4\}$ и $A(S_2) = \{2, 5\}$, будут выглядеть следующим образом:

$$\begin{aligned} S_1(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3) &= F_9^1(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3) \vee \\ &\vee F_9^4(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3), \\ S_2(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3) &= F_9^2(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3) \vee \\ &\vee F_9^5(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3), \end{aligned}$$

где

$$F_9^1 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 = 1; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$F_9^2 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 = 2; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$F_9^4 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 = 4; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$F_9^5 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 = 5; \\ 0 & - \text{в противном случае.} \end{cases}$$

Пример 2.3. Пусть $X_1 + X_2 + X_3 + X_4 = S \pmod{3}$, тогда матрица $M(S^*)$, где $S^* = X_1 + X_2 + X_3 + X_4$, имеет следующий вид:

$$M(S^*) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Если $s_{1,1} = s_{4,1} = s_{7,1} = 1$, то $S^* \in \{1, 4, 7\}$ и функция $S_1 = 1$. Если $s_{2,2} = s_{5,2} = s_{8,2} = 1$, то $S^* \in \{2, 5, 8\}$ и функция $S_2 = 1$.

Локальные коды функций S_1 и S_2 имеют вид $\pi(S_1) = (0, 1, 0, 0, 1, 0, 0, 1, 0)$ и $\pi(S_2) = (0, 0, 1, 0, 0, 1, 0, 0, 1)$. Тогда представления (2.8) для СБФ S_1 и S_2 , рабочие числа которых равны $A(S_1) = \{1, 4, 7\}$ и $A(S_2) = \{2, 5, 8\}$, будут выглядеть следующим образом:

$$\begin{aligned} S_1(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4) &= F_{12}^1(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2, x_1^3, x_2^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ &\vee F_{12}^4(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2, x_1^3, x_2^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ &\vee F_{12}^7(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2, x_1^3, x_2^3, x_2^3, x_1^4, x_2^4, x_2^4); \\ S_2(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4) &= F_{12}^2(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2, x_1^3, x_2^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ &\vee F_{12}^5(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2, x_1^3, x_2^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ &\vee F_{12}^8(x_1^1, x_2^1, x_1^2, x_2^2, x_2^2, x_1^3, x_2^3, x_2^3, x_1^4, x_2^4, x_2^4), \end{aligned}$$

где

$$F_{12}^1 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 1; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$F_{12}^2 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 2; \\ 0 & - \text{в противном случае.} \end{cases}$$

$$F_{12}^4 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 4; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$F_{12}^5 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 5; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{12}^7 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 7; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{12}^8 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 8; \\ 0 & - \text{ в противном случае.} \end{cases}$$

2.1.2 Модулярное сложение для произвольного значения модуля

Перейдем к рассмотрению операции сложения $X_1 + X_2 + \dots + X_N = S \pmod{P}$, где $P \geq 3$. Тогда, в соответствии с (2.1), операнды $X_1, X_2, \dots, X_N$ и результат их сложения S принимают значения из множества $\{0, 1, \dots, P-1\}$ и задаются δ -разрядными двоичными наборами $X_n = (x_1^n, x_2^n, \dots, x_\delta^n)$ и $S = (s_1, s_2, \dots, s_\delta)$, где $n = \overline{1, N}$. В таком случае справедлива следующая запись:

$$\sum_{n=1}^N X_n = \sum_{n=1}^N (x_1^n + 2x_2^n + \dots + 2^{\delta-1}x_\delta^n) = \quad (2.10)$$

$$= 2^0 s_1 + 2^1 s_2 + \dots + 2^{\delta-1} s_\delta = S \pmod{P},$$

где $x_k^n \in \{0, 1\}$ и $k = \overline{1, \delta}$.

В результате сложения N операндов формируются δ функций $S_1 = S_1(x_1^1, \dots, x_\delta^1, \dots, x_1^N, \dots, x_\delta^N)$, $S_2 = S_1(x_1^1, \dots, x_\delta^1, \dots, x_1^N, \dots, x_\delta^N)$, ..., $S_\delta = S_\delta(x_1^1, \dots, x_\delta^1, \dots, x_1^N, \dots, x_\delta^N)$, принимающие значения разрядов $s_1, s_2, \dots, s_\delta$ результата сложения $S = (s_1, s_2, \dots, s_\delta)$. Тогда

$$\sum_{n=1}^N X_n = \begin{cases} Pr = 0 \pmod{P}; \\ Pr + 1 = 1 \pmod{P}; \\ \dots \\ Pr + t = t \pmod{P}; \\ \dots \\ Pr + P - 1 = (P - 1) \pmod{P}, \end{cases} \quad (2.11)$$

где $r = 0, 1, 2, \dots$

Поскольку $S \pmod{P} = 2^0 s_1 + 2^1 s_2 + \dots + 2^{\delta-1} s_\delta$, то результат сложения N операндов $S \pmod{P}$ можно представить с помощью двоичной матрицы

$$M(S) = \begin{bmatrix} s_{0,1} & s_{0,2} & \dots & s_{0,k} & \dots & s_{0,\delta} \\ s_{1,1} & s_{1,2} & \dots & s_{1,k} & \dots & s_{1,\delta} \\ \dots & & & & & \\ s_{t,1} & s_{t,2} & \dots & s_{t,k} & \dots & s_{t,\delta} \\ \dots & & & & & \\ s_{P-1,1} & s_{P-1,2} & \dots & s_{P-1,k} & \dots & s_{P-1,\delta} \end{bmatrix}, \quad (2.12)$$

где $t = \overline{0, P-1}$ и $k = \overline{1, \delta}$. Строкам матрицы соответствуют двоичные значения, которые принимает S , а число столбцов равно числу разрядов $S \pmod{P}$.

Обозначим $S^* = X_1 + X_2 + \dots + X_N$, т.е. $S^* \in \{0, 1, 2, \dots, (P-1)N\}$. Так как $X_1, X_2, \dots, X_N \in \{0, 1, 2, \dots, P-1\}$, то результат сложения N операндов $S^* = S \pmod{P}$ можно представить с помощью двоичной матрицы $M(S^*)$, которая имеет вид

$$M(S^*) = \begin{bmatrix} s_{0,1} & s_{0,2} & \dots & s_{0,k} & \dots & s_{0,\delta} \\ s_{1,1} & s_{1,2} & \dots & s_{1,k} & \dots & s_{1,\delta} \\ \dots & & & & & \\ s_{i,1} & s_{i,2} & \dots & s_{i,k} & \dots & s_{i,\delta} \\ \dots & & & & & \\ s_{(P-1)N,1} & s_{(P-1)N,2} & \dots & s_{(P-1)N,k} & \dots & s_{(P-1)N,\delta} \end{bmatrix}, \quad (2.13)$$

где $i = \overline{0, (P-1)N}$. Строкам матрицы соответствуют двоичные значения $S^* \pmod{P}$, а число столбцов совпадает с числом разрядов $S^* \pmod{P}$.

Функция $S_k = 1$ тогда и только тогда, когда $s_{i,k} = 1$.

Например, если $X_1 + X_2 = S \pmod{5}$, где $X_1, X_2 \in \{0, 1, 2, 3, 4\}$, то матрица $M(S)$ будет иметь вид

$$M(S) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (2.14)$$

где строкам матрицы соответствуют двоичные значения, которые может принимать результат сложения $S \pmod{5} \in \{0,1,2,3,4\}$, а число столбцов равно трем, так как $S \pmod{5} = s_1 + 2s_2 + 4s_3$.

Тогда матрица $M(S^*)$ имеет следующий вид:

$$M(S^*) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \quad (2.15)$$

где $S^* = X_1 + X_2$ и $S^* \in \{0,1,2,\dots,8\}$.

Функции S_1, S_2, S_3 принимают единичные значения при условиях:

- если $s_{1,1} = s_{3,1} = s_{6,1} = s_{8,1} = 1$, то $S^* \in \{1,3,6,8\}$ и $S_1 = 1$;
- если $s_{2,2} = s_{3,2} = s_{7,2} = s_{8,2} = 1$, то $S^* \in \{2,3,7,8\}$ и $S_2 = 1$;
- если $s_{5,3} = 1$, то $S^* \in \{4\}$ и $S_3 = 1$.

Разобьем множество переменных $\{x_1^1, x_2^1, \dots, x_\delta^1, \dots, x_1^N, x_2^N, \dots, x_\delta^N\}$ на δ подмножеств $Y_1, Y_2, \dots, Y_\delta$ следующим образом: $Y_1 = \{x_1^1, x_1^2, \dots, x_1^N\}$, $Y_2 = \{x_2^1, x_2^2, \dots, x_2^N\}$, ..., $Y_\delta = \{x_\delta^1, x_\delta^2, \dots, x_\delta^N\}$. Тогда значения функций $S_1 = S_1(Y_1, Y_2, \dots, Y_\delta)$, $S_2 = S_2(Y_1, Y_2, \dots, Y_\delta)$, ..., $S_\delta = S_\delta(Y_1, Y_2, \dots, Y_\delta)$ инвариантны относительно перестановки переменных внутри каждого из подмножеств $Y_1, Y_2, \dots, Y_\delta$, т.е. множество переменных $\{x_1^1, x_2^1, \dots, x_\delta^1, \dots, x_1^N, x_2^N, \dots, x_\delta^N\}$ разбивается на δ классов симметрии.

На основании применения процедуры симметрирования можно утверждать, что функция $S_k = S_k \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_{2^{k-1}}, \dots, \underbrace{Y_\delta, \dots, Y_\delta}_{2^{\delta-1}} \right)$ является СБФ, которая зависит от $(2^\delta - 1)N$ переменных. Тогда $S_k(Y_1, Y_2, \dots, Y_\delta) = S_k(Y_1, Y_2, Y_2, \dots, Y_k, \dots, Y_k, \dots, Y_\delta, \dots, Y_\delta)$. В таком случае функцию S_k можно представить локальным кодом $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{(P-1)N}^k, \pi_{(P-1)N+1}^k, \dots, \pi_{2^{\delta-1}N}^k)$.

Поскольку $S^* \leq (P-1)N$, то $\pi_v^k = 0$, где $v \geq (P-1)N + 1$. Тогда локальный код функции S_k будет следующим $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{(P-1)N}^k) = (s_{0,k}, s_{1,k}, s_{2,k}, \dots, s_{(P-1)N,k})$.

Если к СБФ S_k применить разложение (1.6), то получим представления этих функций посредством дизъюнкции ФСБФ. Обобщить утверждение 2.1 и подытожить вышесказанное относительно модулярного сложения в позиционных кодах можно нижеследующим утверждением.

Утверждение 2.2. Если $N \geq 2$, то

$$S_k(Y_1, Y_2, \dots, Y_\delta) = \bigvee_{i=0}^{(P-1)N} \pi_i^k \cdot F_{(2^\delta-1)N}^i \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_{2^{k-1}}, \dots, \underbrace{Y_\delta, \dots, Y_\delta}_{2^{\delta-1}} \right), \quad (2.16)$$

где $F_{(2^\delta-1)N}^i \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_{2^{k-1}}, \dots, \underbrace{Y_\delta, \dots, Y_\delta}_{2^{\delta-1}} \right)$ – ФСБФ, зависящая от $(2^\delta - 1)N$,

рабочие числа которых равны $i \cdot \pi_i^k$, где $i = \overline{0, (P-1)N}$, $k = \overline{1, \delta}$ и $Y_1 = (x_1^1, x_1^2, \dots, x_1^N)$, $Y_2 = (x_2^1, x_2^2, \dots, x_2^N)$, ..., $Y_k = \{x_k^1, x_k^2, \dots, x_k^N\}$, ..., $Y_\delta = (x_\delta^1, x_\delta^2, \dots, x_\delta^N)$.

Отсюда следует, что

$$S_k = \begin{cases} 1, & \text{если } \sum_{n=1}^N X_n = \sum_{n=1}^N (x_1^n + 2x_2^n + \dots + 2^{\delta-1}x_\delta^n) = i \cdot \pi_i^k; \\ 0 & \text{в противном случае.} \end{cases} \quad (2.17)$$

Приведенные представления функции S_k равносильны формуле (2.16).

Пример 2.4. Пусть $X_1 + X_2 = S \pmod{5}$, тогда матрицы $M(S)$ и $M(S^*)$ примут вид (2.14) и (2.15).

Локальные коды функций S_1, S_2, S_3 равны $\pi(S_1) = (0, 1, 0, 1, 0, 0, 1, 0, 1)$, $\pi(S_2) = (0, 0, 1, 1, 0, 0, 0, 1, 1)$ и $\pi(S_3) = (0, 0, 0, 0, 1, 0, 0, 0, 0)$. Представление (2.16) для СБФ S_1, S_2, S_3 , рабочие числа которых равны $A(S_1) = \{1, 3, 6, 8\}$, $A(S_2) = \{2, 3, 7, 8\}$ и $A(S_3) = \{4\}$, будут выглядеть следующим образом:

$$\begin{aligned} S_1(x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2) = & F_{14}^1(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2) \vee \\ & \vee F_{14}^3(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2) \vee \\ & \vee F_{14}^6(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2) \vee \\ & \vee F_{14}^8(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2); \end{aligned}$$

$$\begin{aligned}
S_2(x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2) &= F_{14}^2(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2) \vee \\
&\vee F_{14}^3(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2) \vee \\
&\vee F_{14}^7(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2) \vee \\
&\vee F_{14}^8(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2); \\
S_3(x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2) &= F_{14}^4(x_1^1, x_2^1, x_2^1, x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_2^2, x_2^2, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2),
\end{aligned}$$

где

$$F_{14}^1 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 1; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{14}^2 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 2; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{14}^3 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 3; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{14}^4 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 4; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{14}^6 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 6; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{14}^7 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 7; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{14}^8 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^1 + 4x_3^1 + x_1^2 + 2x_2^2 + 4x_3^2 = 8; \\ 0 & - \text{ в противном случае.} \end{cases}$$

Наряду с представлением информации в позиционных кодах при реализации модулярных вычислительных структур часто используют кодирование в унитарных кодах [48].

2.2 Арифметические операции в унитарных кодах

Произвольное целое положительное число $X \pmod{P}$ в унитарном (однопозиционном, единичном или «1 из P ») коде можно представить P – разрядным двоичным набором $X = (x_0, x_1, \dots, x_{P-1})$ в виде

$$X \pmod{P} = \sum_{k=0}^{P-1} k \cdot x_k = 0 \cdot x_0 + 1 \cdot x_1 + \dots + (P-1) \cdot x_{P-1}. \quad (2.18)$$

Основным свойством представления чисел в унитарном коде (2.18) является тот факт, что $x_0 + x_1 + \dots + x_{P-1} = 1$.

Как для случая с позиционными кодами, для представления целого положительного $X \pmod{P}$ и отрицательного $-X \pmod{P}$ числа в унитарном коде по модулю P , целесообразно использовать дополнение до P .

Пусть $-X = S \pmod{P}$, тогда $S + X = 0 \pmod{P}$. С учетом (2.18) получим $-X \pmod{P} = 0 \cdot s_0 + 1 \cdot s_1 + \dots + (P-1) \cdot s_{P-1}$, где $S = (s_0, s_1, \dots, s_{P-1})$ и $s_0 = x_0, s_1 = x_{P-1}, \dots, s_{P-1} = x_1$, т.е.

$$-X \pmod{P} = 0 \cdot x_0 + 1 \cdot x_{P-1} + \dots + (P-1) \cdot x_1. \quad (2.19)$$

Например, число $-X \pmod{5}$ в унитарном коде, на основании (2.18), можно представить в виде $-X \pmod{5} = 0 \cdot x_0 + 1 \cdot x_4 + 2 \cdot x_3 + 3 \cdot x_2 + 4 \cdot x_1$. Пусть $X = 3$, тогда $-3 \pmod{5} = (0, 0, 1, 0, 0)$.

Далее рассматриваются модулярные операции сложения $X_1 + X_2 + \dots + X_N = S \pmod{P}$ и умножения $X_1 \cdot X_2 = R \pmod{P}$.

Операнды $X_1, X_2, \dots, X_N$ и результат их сложения S и умножения R принимают целочисленные значения от 0 до $P-1$, которые соответствуют P -разрядным двоичным наборам.

В результате сложения и умножения операндов формируются функции $S_0, S_1, S_2, \dots, S_{P-1}$ и $R_0, R_1, R_2, \dots, R_{P-1}$, принимающие значения $s_0, s_1, s_2, \dots, s_{P-1}$ и $r_0, r_1, r_2, \dots, r_{P-1}$, где $S = 0 \cdot s_0 + 1 \cdot s_1 + \dots + (P-1) \cdot s_{P-1}$ и $R = 0 \cdot r_0 + 1 \cdot r_1 + \dots + (P-1) \cdot r_{P-1}$.

Учитывая (2.18) и (2.19), операнд X_n может быть представлен P -разрядным набором настроечных переменных $(u_0^n, u_1^n, u_2^n, \dots, u_{P-1}^n)$, т.е. $X_n \pmod{P} = 0 \cdot u_0^n + 1 \cdot u_1^n + \dots + (P-1) u_{P-1}^n$, где $u_0^n, u_1^n, u_2^n, \dots, u_{P-1}^n \in \{x_0^n, x_1^n, x_2^n, \dots, x_{P-1}^n\}$ и $n = \overline{1, N}$. Тогда при соответствующей настройке операндов может быть выполнена любая из операций $\pm X_1 \pm X_2 \dots \pm X_N = S \pmod{P}$.

В качестве примера в таблице 2.2 приведена настройка операндов на выполнение одной (любой) из четырех операций $\pm X_1 \pm X_2 = S \pmod{5}$ в унитарных кодах.

Таблица 2.2 – Таблица настройки операндов на реализацию операций $\pm X_1 \pm X_2 = S \pmod{5}$

Значения разрядов операндов										Выполняемая арифметическая операция
Значение первого операнда $X_1(u_0^1, u_1^1, u_2^1, u_3^1, u_4^1)$					Значение второго операнда $X_2(u_0^2, u_1^2, u_2^2, u_3^2, u_4^2)$					
u_0^1	u_1^1	u_2^1	u_3^1	u_4^1	u_0^2	u_1^2	u_2^2	u_3^2	u_4^2	
x_0^1	x_1^1	x_2^1	x_3^1	x_4^1	x_0^2	x_1^2	x_2^2	x_3^2	x_4^2	
x_0^1	x_1^1	x_2^1	x_3^1	x_4^1	x_0^2	x_1^2	x_2^2	x_3^2	x_4^2	$X_1 + X_2$
x_0^1	x_4^1	x_3^1	x_2^1	x_1^1	x_0^2	x_1^2	x_2^2	x_3^2	x_4^2	$-X_1 + X_2$
x_0^1	x_1^1	x_2^1	x_3^1	x_4^1	x_0^2	x_4^2	x_3^2	x_2^2	x_1^2	$X_1 - X_2$
x_0^1	x_4^1	x_3^1	x_2^1	x_1^1	x_0^2	x_4^2	x_3^2	x_2^2	x_1^2	$-X_1 - X_2$

2.2.1 Модулярное сложение двух операндов в унитарных кодах

Первоначально рассмотрим операцию модулярного сложения двух операндов [5-A, 13-A]. На основании (2.18) и основного свойства унитарных кодов справедлива следующая запись:

$$X_1 + X_2 = \sum_{i=0}^{P-1} \sum_{j=0}^{P-1} (i \cdot x_i^1 + j \cdot x_j^2) = \quad (2.20)$$

$$= 0 \cdot s_0 + 1 \cdot s_1 + \dots + (P-1) \cdot s_{P-1} = S \pmod{P}$$

В результате сложения $X_1 + X_2 = S \pmod{P}$ формируются функции $S_0, S_1, \dots, S_{P-1}$, принимающие значения $s_0, s_1, \dots, s_{P-1}$. Тогда

$$X_1 + X_2 = \begin{cases} Pr = 0 \pmod{P}; \\ Pr + 1 = 1 \pmod{P}; \\ \dots \\ Pr + k = k \pmod{P}; \\ \dots \\ Pr + P - 1 = (P-1) \pmod{P}, \end{cases} \quad (2.21)$$

где $r = 0, 1, 2, \dots$

Поскольку $S \pmod{P} = 0 \cdot s_0 + 1 \cdot s_1 + \dots + (P-1) \cdot s_{P-1}$, то результат сложения $S \pmod{P}$ можно представить с помощью двоичной матрицы

$$M(S) = \begin{bmatrix} s_{0,0} & s_{0,1} & \dots & s_{0,k} & \dots & s_{0,P-1} \\ s_{1,0} & s_{1,1} & \dots & s_{1,k} & \dots & s_{1,P-1} \\ \dots & & & & & \\ s_{i,0} & s_{i,1} & \dots & s_{i,k} & \dots & s_{i,P-1} \\ \dots & & & & & \\ s_{P-1,0} & s_{P-1,1} & \dots & s_{P-1,k} & \dots & s_{P-1,P-1} \end{bmatrix}, \quad (2.22)$$

где $i, k = \overline{0, P-1}$. Строкам матрицы соответствуют двоичные значения, которые принимает S , а число столбцов равно числу разрядов $S \pmod{P}$.

Обозначим $S^* = X_1 + X_2$, где $S^* \in \{0, 1, 2, \dots, 2(P-1)\}$. Так как $X_1, X_2 \in \{0, 1, 2, \dots, P-1\}$, то результат сложения операндов $S^* = S \pmod{P}$ можно представить с помощью двоичной матрицы $M(S^*)$, которая имеет вид

$$M(S^*) = \begin{bmatrix} s_{0,0} & s_{0,1} & \dots & s_{0,k} & \dots & s_{0,P-1} \\ s_{1,0} & s_{1,1} & \dots & s_{1,k} & \dots & s_{1,P-1} \\ s_{2,0} & s_{2,1} & \dots & s_{2,k} & \dots & s_{2,P-1} \\ \dots & & & & & \\ s_{t,0} & s_{t,1} & \dots & s_{t,k} & \dots & s_{t,P-1} \\ \dots & & & & & \\ s_{2(P-1),0} & s_{2(P-1),1} & \dots & s_{2(P-1),k} & \dots & s_{2(P-1),P-1} \end{bmatrix}, \quad (2.23)$$

где $t = \overline{0, 2(P-1)}$. Строкам матрицы соответствуют двоичные значения $S^* \pmod{P}$, а число столбцов совпадает с числом разрядов $S^* \pmod{P}$.

Функция $S_k = 1$ тогда и только тогда, когда $s_{t,k} = 1$.

Например, в результате выполнения операции сложения $X_1 + X_2 = S \pmod{5}$, где $X_1, X_2 \in \{0, 1, 2, 3, 4\}$, матрица $M(S)$ имеет вид

$$M(S) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad (2.24)$$

где строкам матрицы соответствуют двоичные значения, которые принимает результат сложения $S \pmod{5} \in \{0, 1, 2, 3, 4\}$, а число столбцов равно пяти, так как $S \pmod{5} = 0 \cdot s_0 + 1 \cdot s_1 + 2 \cdot s_2 + 3 \cdot s_3 + 4 \cdot s_4$.

В этом случае матрица $M(S^*)$ будет выглядеть следующим образом

$$M(S^*) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad (2.25)$$

где $S^* = X_1 + X_2$ и $S^* \in \{0, 1, 2, \dots, 8\}$.

Функции S_0, S_1, S_2, S_3, S_4 принимают единичные значения при условиях:

- если $s_{0,0} = s_{5,0} = 1$, то $S^* \in \{0, 5\}$ и $S_0 = 1$;
- если $s_{1,1} = s_{6,1} = 1$, то $S^* \in \{1, 6\}$ и $S_1 = 1$;
- если $s_{2,2} = s_{2,7} = 1$, то $S^* \in \{2, 7\}$ и $S_2 = 1$;
- если $s_{3,3} = s_{8,3} = 1$, то $S^* \in \{3, 8\}$ и $S_3 = 1$;
- если $s_{4,4} = 1$, то $S^* \in \{4\}$ и $S_4 = 1$.

Для реализации функции $S_k = S_k(x_0^1, x_1^1, \dots, x_{P-1}^1, x_0^2, x_1^2, \dots, x_{P-1}^2)$ целесообразно произвести процедуру ее симметрирования разбив множество переменных $x_0^1, x_1^1, \dots, x_{P-1}^1, x_0^2, x_1^2, \dots, x_{P-1}^2$ на P подмножеств $Y_0, Y_1, \dots, Y_{P-1}$, причем $Y_i = \underbrace{\{x_i^1, \dots, x_i^1, x_j^2, \dots, x_j^2\}}_{i+1}$, где $i + j = k \pmod{P}$.

Функция $S_k = S_k(Y_0, Y_1, \dots, Y_{P-1})$ является СБФ, которая зависит от $P(P+1)$ переменных.

Например, если $S_2 = S_2(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = S_2(Y_0, Y_1, Y_2, Y_3, Y_4)$, то $Y_0 = \{x_0^1, x_2^2, x_2^2, x_2^2, x_2^2, x_2^2\}$, $Y_1 = \{x_1^1, x_1^1, x_1^2, x_1^2, x_1^2, x_1^2\}$, $Y_2 = \{x_2^1, x_2^1, x_2^1, x_0^2, x_0^2, x_0^2\}$, $Y_3 = \{x_3^1, x_3^1, x_3^1, x_3^1, x_4^2, x_4^2\}$ и $Y_4 = \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^1, x_3^2\}$.

СБФ S_k можно представить локальным кодом $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{2(P-1)}^k, \pi_{2(P-1)+1}^k, \dots, \pi_{P(P+1)}^k)$.

На основании того, что $S^* \leq 2(P-1)$, то $\pi_v^k = 0$, где $v \geq 2(P-1)+1$. Тогда локальный код для функции S_k имеет вид $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{2(P-1)}^k) = (s_{0,k}, s_{1,k}, s_{2,k}, \dots, s_{2(P-1),k})$.

Учитывая вышесказанное, основное свойство функции $S_k = S_k(x_0^1, x_1^1, \dots, x_{P-1}^1, x_0^2, x_1^2, \dots, x_{P-1}^2)$ можно сформулировать с помощью следующего утверждения.

Утверждение 2.3. Функция $S_k = 1$ тогда и только тогда, когда $x_i^1 + x_j^2 = 2$, где $i + j = k \pmod{P}$.

Приведенное утверждение эквивалентно следующему.

Утверждение 2.4. Функция $S_k = 1$ тогда и только тогда, когда $(i + 1) \cdot x_i^1 + (P - i) \cdot x_j^2 = P + 1$, где $i + j = k \pmod{P}$.

Например, функция $S_2(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = 1$ тогда и только тогда, когда выполняется одно из следующих равенств: а) $x_0^1 + x_2^2 = 2$ и $x_0^1 + 5x_2^2 = 6$; б) $x_1^1 + x_1^2 = 2$ и $2x_1^1 + 4x_1^2 = 6$; в) $x_2^1 + x_0^2 = 2$ и $3x_2^1 + 3x_0^2 = 6$; г) $x_3^1 + x_4^2 = 2$ и $4x_3^1 + 2x_4^2 = 6$; д) $x_4^1 + x_3^2 = 2$ и $5x_4^1 + x_3^2 = 6$.

Обобщим, приведенные в утверждениях 2.3 и 2.4, представления функций S_k в следующем образом.

Утверждение 2.5. Функция $S_k = 1$ тогда и только тогда, когда

$$\sum_{i=0}^{P-1} \sum_{j=0}^{P-1} ((i + 1) \cdot x_i^1 + (P - i) \cdot x_j^2) = P + 1, \quad (2.26)$$

где $i + j = k \pmod{P}$ и $i, j, k = \overline{0, P-1}$.

Пример 2.5. Пусть $P = 5$, т.е. в результате сложения $X_1 + X_2 = S \pmod{5}$ матрицы $M(S)$ $M(S^*)$ примут вид (2.24) и (2.25).

Локальные коды функций S_0, S_1, S_2, S_3, S_4 равны $\pi(S_0) = (1, 0, 0, 0, 0, 1, 0, 0, 0)$, $\pi(S_1) = (0, 1, 0, 0, 0, 0, 1, 0, 0)$, $\pi(S_2) = (0, 0, 1, 0, 0, 0, 0, 1, 0)$, $\pi(S_3) = (0, 0, 0, 1, 0, 0, 0, 0, 1)$ и $\pi(S_4) = (0, 0, 0, 0, 1, 0, 0, 0, 0)$ соответственно.

Согласно утверждениям 2.3 и 2.4 получим следующие представления функций S_0, S_1, S_2, S_3, S_4 :

– $S_0(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = 1$, если а) $x_0^1 + x_0^2 = 2$ и $x_0^1 + 5x_0^2 = 6$; б) $x_1^1 + x_4^2 = 2$ и $2x_1^1 + 4x_4^2 = 6$; в) $x_2^1 + x_3^2 = 2$ и $3x_2^1 + 3x_3^2 = 6$; г) $x_3^1 + x_2^2 = 2$ и $4x_3^1 + 2x_2^2 = 6$; д) $x_4^1 + x_1^2 = 2$ и $5x_4^1 + x_1^2 = 6$;

– $S_1(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = 1$, если а) $x_0^1 + x_1^2 = 2$ и $x_0^1 + 5x_1^2 = 6$; б) $x_1^1 + x_0^2 = 2$ и $2x_1^1 + 4x_0^2 = 6$; в) $x_2^1 + x_4^2 = 2$ и $3x_2^1 + 3x_4^2 = 6$; г) $x_3^1 + x_3^2 = 2$ и $4x_3^1 + 2x_3^2 = 6$; д) $x_4^1 + x_2^2 = 2$ и $5x_4^1 + x_2^2 = 6$;

– условия, при которых функция $S_2(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = 1$, приведены после утверждения 2.4;

– $S_3(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = 1$, если а) $x_0^1 + x_3^2 = 2$ и $x_0^1 + 5x_3^2 = 6$; б) $x_1^1 + x_2^2 = 2$ и $2x_1^1 + 4x_2^2 = 6$; в) $x_2^1 + x_1^2 = 2$ и $3x_2^1 + 3x_1^2 = 6$; г) $x_3^1 + x_0^2 = 2$ и $4x_3^1 + 2x_0^2 = 6$; д) $x_4^1 + x_4^2 = 2$ и $5x_4^1 + x_4^2 = 6$;

– $S_4(x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2) = 1$, если а) $x_0^1 + x_4^2 = 2$ и $x_0^1 + 5x_4^2 = 6$; б) $x_1^1 + x_3^2 = 2$ и $2x_1^1 + 4x_3^2 = 6$; в) $x_2^1 + x_2^2 = 2$ и $3x_2^1 + 3x_2^2 = 6$; г) $x_3^1 + x_1^2 = 2$ и $4x_3^1 + 2x_1^2 = 6$; д) $x_4^1 + x_0^2 = 2$ и $5x_4^1 + x_0^2 = 6$.

В таком случае СБФ S_0, S_1, S_2, S_3, S_4 можно записать как

$$\begin{aligned} -S_0 &= S_0(Y_0, Y_1, Y_2, Y_3, Y_4), & \text{где} & & Y_0 &= \{x_0^1, x_0^2, x_0^2, x_0^2, x_0^2, x_0^2\}, \\ Y_1 &= \{x_1^1, x_1^1, x_4^2, x_4^2, x_4^2, x_4^2\}, & Y_2 &= \{x_2^1, x_2^1, x_2^1, x_3^2, x_3^2, x_3^2\}, & Y_3 &= \{x_3^1, x_3^1, x_3^1, x_3^1, x_2^2, x_2^2\} \text{ и} \\ Y_4 &= \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^1, x_1^2\}; \end{aligned}$$

$$\begin{aligned} -S_1 &= S_1(Y_0, Y_1, Y_2, Y_3, Y_4), & \text{где} & & Y_0 &= \{x_0^1, x_1^2, x_1^2, x_1^2, x_1^2, x_1^2\}, \\ Y_1 &= \{x_1^1, x_1^1, x_0^2, x_0^2, x_0^2, x_0^2\}, & Y_2 &= \{x_2^1, x_2^1, x_2^1, x_4^2, x_4^2, x_4^2\}, & Y_3 &= \{x_3^1, x_3^1, x_3^1, x_3^1, x_3^2, x_3^2\} \text{ и} \\ Y_4 &= \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^1, x_2^2\}; \end{aligned}$$

– $S_2 = S_2(Y_0, Y_1, Y_2, Y_3, Y_4)$, где множества Y_0, Y_1, Y_2, Y_3, Y_4 описаны выше;

$$\begin{aligned} -S_3 &= S_3(Y_0, Y_1, Y_2, Y_3, Y_4), & \text{где} & & Y_0 &= \{x_0^1, x_3^2, x_3^2, x_3^2, x_3^2, x_3^2\}, \\ Y_1 &= \{x_1^1, x_1^1, x_2^2, x_2^2, x_2^2, x_2^2\}, & Y_2 &= \{x_2^1, x_2^1, x_2^1, x_1^2, x_1^2, x_1^2\}, & Y_3 &= \{x_3^1, x_3^1, x_3^1, x_3^1, x_0^2, x_0^2\} \text{ и} \\ Y_4 &= \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^1, x_4^2\}; \end{aligned}$$

$$\begin{aligned} -S_4 &= S_4(Y_0, Y_1, Y_2, Y_3, Y_4), & \text{где} & & Y_0 &= \{x_0^1, x_4^2, x_4^2, x_4^2, x_4^2, x_4^2\}, \\ Y_1 &= \{x_1^1, x_1^1, x_3^2, x_3^2, x_3^2, x_3^2\}, & Y_2 &= \{x_2^1, x_2^1, x_2^1, x_2^2, x_2^2, x_2^2\}, & Y_3 &= \{x_3^1, x_3^1, x_3^1, x_3^1, x_1^2, x_1^2\} \text{ и} \\ Y_4 &= \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^1, x_0^2\}. \end{aligned}$$

Учитывая приведенную запись СБФ S_0, S_1, S_2, S_3, S_4 и формулу (2.26), справедливы представления этих функций

$$S_0 = \begin{cases} 1, & \text{если } x_0^1 + 5x_0^2 + 2x_1^1 + 4x_4^2 + 3x_2^1 + 3x_3^2 + 4x_3^1 + 2x_2^2 + 5x_4^1 + x_1^2 = 6; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$S_1 = \begin{cases} 1, & \text{если } x_0^1 + 5x_1^2 + 2x_1^1 + 4x_0^2 + 3x_2^1 + 3x_4^2 + 4x_3^1 + 2x_3^2 + 5x_4^1 + x_2^2 = 6; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$S_2 = \begin{cases} 1, & \text{если } x_0^1 + 5x_2^2 + 2x_1^1 + 4x_1^2 + 3x_2^1 + 3x_0^2 + 4x_3^1 + 2x_4^2 + 5x_4^1 + x_3^2 = 6; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$S_3 = \begin{cases} 1, & \text{если } x_0^1 + 5x_3^2 + 2x_1^1 + 4x_2^2 + 3x_2^1 + 3x_1^2 + 4x_3^1 + 2x_0^2 + 5x_4^1 + x_4^2 = 6; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$S_4 = \begin{cases} 1, & \text{если } x_0^1 + 5x_4^2 + 2x_1^1 + 4x_3^2 + 3x_2^1 + 3x_2^2 + 4x_3^1 + 2x_1^2 + 5x_4^1 + x_0^2 = 6; \\ 0 & - \text{в противном случае.} \end{cases}$$

Используя перекоммутации переменных $x_0^1, x_1^1, \dots, x_4^1, x_0^2, x_1^2, \dots, x_4^2$, как показано в таблице 2.2, можно реализовать любую из четырех операций вида $\pm X_1 \pm X_2 = S \pmod{5}$.

2.2.1 Модулярное сложение произвольного числа операндов в унитарных кодах

Перейдем к рассмотрению операции сложения $X_1 + X_2 + \dots + X_N = S \pmod{P}$ при $N \geq 2$ [5-А, 12-А, 18-А]. Тогда, в соответствии с (2.20), каждый из операндов $X_1, X_2, \dots, X_N$ и результат их сложения S принимает значение из множества $\{0, 1, \dots, P-1\}$ и задается P -разрядным двоичным набором $X_n = (x_0^n, x_1^n, \dots, x_{P-1}^n)$ и $S = (s_0, s_1, \dots, s_{P-1})$. В таком случае справедлива запись

$$\begin{aligned} \sum_{n=1}^N X_n &= \sum_{i_1=0}^{P-1} \sum_{i_2=0}^{P-1} \dots \sum_{i_N=0}^{P-1} (i_1 \cdot x_{i_1}^1 + i_2 \cdot x_{i_2}^2 + \dots + i_N \cdot x_{i_N}^N) = \\ &= 0 \cdot s_0 + 1 \cdot s_1 + \dots + (P-1) \cdot s_{P-1} = S \pmod{P}, \end{aligned} \quad (2.27)$$

где $x_k^n \in \{0, 1\}$ и $k = \overline{1, \delta}$.

В результате сложения $X_1 + X_2 + \dots + X_N = S \pmod{P}$ формируются функции $S_0, S_1, \dots, S_{P-1}$, принимающие значения разрядов $s_0, s_1, \dots, s_{P-1}$, где $S = (s_0, s_1, \dots, s_{P-1})$.

Тогда

$$\sum_{n=1}^N X_n = \begin{cases} Pr = 0 \pmod{P}; \\ Pr + 1 = 1 \pmod{P}; \\ \dots \\ Pr + k = k \pmod{P}; \\ \dots \\ Pr + P - 1 = (P - 1) \pmod{P}, \end{cases} \quad (2.28)$$

где $r = 0, 1, 2, \dots$.

Результат сложения N операндов $S \pmod{P}$ можно представить с помощью двоичной матрицы $M(S)$, которая совпадает с матрицей (2.22).

Матрица $M(S^*)$ формируется следующим образом. Обозначим $X_1 + X_2 + \dots + X_N = S^*$, где $S^* \in \{0, 1, 2, \dots, (P-1)N\}$. Так как $X_1, X_2, \dots, X_N \in \{0, 1, 2, \dots, P-1\}$, то результат сложения операндов $S^* = S \pmod{P}$ можно представить с помощью двоичной матрицы $M(S^*)$, которая имеет вид

$$M(S^*) = \begin{bmatrix} s_{0,0} & s_{0,1} & \dots & s_{0,k} & \dots & s_{0,P-1} \\ s_{1,0} & s_{1,1} & \dots & s_{1,k} & \dots & s_{1,P-1} \\ s_{2,0} & s_{2,1} & \dots & s_{2,k} & \dots & s_{2,P-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{t,0} & s_{t,1} & \dots & s_{t,k} & \dots & s_{t,P-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{(P-1)N,0} & s_{(P-1)N,1} & \dots & s_{(P-1)N,k} & \dots & s_{(P-1)N,P-1} \end{bmatrix}, \quad (2.29)$$

где $t = \overline{0, N(P-1)}$. Строкам матрицы соответствуют двоичные значения $S^* \pmod{P}$, а число столбцов совпадает с числом разрядов $S^* \pmod{P}$.

Функция $S_k = 1$ тогда и только тогда, когда $s_{t,k} = 1$.

Разобьем множество переменных $x_1^1, x_2^1, \dots, x_{P-1}^1, \dots, x_1^N, x_2^N, \dots, x_{P-1}^N$ на $P-1$ подмножеств $Y_1 = \{x_1^1, x_1^2, \dots, x_1^N\}$, $Y_2 = \{x_2^1, x_2^2, \dots, x_2^N\}$, ..., $Y_{P-1} = \{x_{P-1}^1, x_{P-1}^2, \dots, x_{P-1}^N\}$. Тогда значения функций $S_1 = S_1(Y_1, Y_2, \dots, Y_{P-1})$, $S_2 = S_2(Y_1, Y_2, \dots, Y_{P-1})$, ..., $S_{P-1} = S_{P-1}(Y_1, Y_2, \dots, Y_{P-1})$ инвариантны относительно перестановки переменных внутри каждого из подмножеств $Y_1, Y_2, \dots, Y_{P-1}$, т.е. множество переменных $x_1^1, x_2^1, \dots, x_{P-1}^1, \dots, x_1^N, x_2^N, \dots, x_{P-1}^N$ разбивается на $P-1$ классов симметрии. Отметим, что переменные $x_0^1, x_0^2, \dots, x_0^N$ не участвуют в указанном разбиении.

$$\text{Функция } S_k(Y_1, Y_2, \dots, Y_{P-1}) = S_k \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_k, \dots, \underbrace{Y_{P-1}, \dots, Y_{P-1}}_{P-1} \right)$$

является СБФ, которая зависит от $\frac{(P^2 - P)N}{2}$ переменных. В таком случае функцию S_k можно представить локальным кодом

$$\pi(S_k) = \left(\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{(P-1)N}^k, \pi_{(P-1)N+1}^k, \dots, \pi_{\frac{(P^2 - P)N}{2}}^k \right).$$

На основании того, что $S^* \leq (P-1)N$, то $\pi_v^k = 0$, где $v \geq (P-1)N + 1$, и тогда локальный код функции S_k можно записать $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{(P-1)N}^k) = (s_{0,k}, s_{1,k}, s_{2,k}, \dots, s_{(P-1)N,k})$.

Если к СБФ S_k применить разложение (1.6), то получим представления этих функций посредством дизъюнкции ФСБФ. Имеет место утверждение.

Утверждение 2.6. Если $n \geq 2$, то

$$S_k(x_0^1, x_1^1, x_2^1, \dots, x_{P-1}^1, \dots, x_0^N, x_1^N, x_2^N, \dots, x_{P-1}^N) = \bigvee_{t=0}^{(P-1)N} \pi_t^k \cdot F_{\frac{(P^2-P)N}{2}}^t \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_k, \dots, \underbrace{Y_{P-1}, \dots, Y_{P-1}}_{P-1} \right), \quad (2.30)$$

где $F_{\frac{(P^2-P)N}{2}}^t \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_k, \dots, \underbrace{Y_{P-1}, \dots, Y_{P-1}}_{P-1} \right)$ – ФСБФ, зависящая от $\frac{(P^2-P)N}{2}$, и рабочие числа которых равны $t \cdot \pi_t^k$, где $t = \overline{0, (P-1)N}$, $k = \overline{1, P-1}$ и $Y_k = \{x_k^1, x_k^2, \dots, x_k^N\}$.

Учитывая основное свойство унитарных кодов, справедливо следующее утверждение

Утверждение 2.7. Функция $S_k = 1$ тогда и только тогда, когда $x_{i_1}^1 + x_{i_2}^2 + \dots + x_{i_N}^N = N$, где $i_1 + i_2 + \dots + i_N = k \pmod{P}$.

Из утверждений 2.6 и 2.7 следует, что

$$S_k = \begin{cases} 1, & \text{если } \sum_{n=1}^N X_n = \sum_{i_1=0}^{P-1} \sum_{i_2=0}^{P-1} \dots \sum_{i_N=0}^{P-1} (i_1 \cdot x_{i_1}^1 + i_2 \cdot x_{i_2}^2 + \dots + i_N \cdot x_{i_N}^N) = t \cdot \pi_t^k; \\ 0 & - \text{в противном случае.} \end{cases} \quad (2.31)$$

Приведенные представления функции S_k равносильны формуле (2.30).

Пример 2.6. В результате сложения $X_1 + X_2 + X_3 + X_4 = S \pmod{3}$, где $X_1, X_2, X_3, X_4 \in \{0, 1, 2\}$, формируется три функции S_0, S_1, S_2 , принимающие значения разрядов $S \pmod{3} = 0 \cdot s_0 + 1 \cdot s_1 + 2 \cdot s_2$.

Тогда матрица $M(S)$ будет выглядеть следующим образом:

$$M(S) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

где строкам матрицы соответствуют двоичные значения, которые принимает результат сложения $S \pmod 3 \in \{0,1,2\}$. Матрица $M(S^*)$ примет вид

$$M(S^*) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

где $S^* = X_1 + X_2 + X_3 + X_4$ и $S^* \in \{0,1,2,\dots,8\}$.

Функции S_0, S_1, S_2 принимают единичные значения при условиях:

- если $s_{0,0} = s_{3,0} = s_{6,0} = 1$, то $S^* \in \{0,3,6\}$ и функция $S_0 = 1$;
- если $s_{1,1} = s_{4,1} = s_{7,1} = 1$, то $S^* \in \{1,4,7\}$ и функция $S_1 = 1$;
- если $s_{2,2} = s_{5,2} = s_{8,2} = 1$, то $S^* \in \{2,5,8\}$ и функция $S_2 = 1$.

Локальные коды СБФ S_0, S_1, S_2 равны $\pi(S_0) = (1,0,0,1,0,0,1,0,0)$, $\pi(S_1) = (0,1,0,0,1,0,0,1,0)$ и $\pi(S_2) = (0,0,1,0,0,1,0,0,1)$. Тогда представление (2.32) для функций S_0, S_1, S_2 с рабочими числами $A(S_0) = \{0,3,6\}$, $A(S_1) = \{1,4,7\}$ и $A(S_2) = \{2,5,8\}$, будет выглядеть как

$$\begin{aligned} & S_0(x_0^1, x_1^1, x_2^1, x_0^2, x_1^2, x_2^2, x_0^3, x_1^3, x_2^3, x_0^4, x_1^4, x_2^4) = \\ & \vee F_{12}^0(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ & \vee F_{12}^3(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ & \vee F_{12}^6(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4); \\ & S_1(x_0^1, x_1^1, x_2^1, x_0^2, x_1^2, x_2^2, x_0^3, x_1^3, x_2^3, x_0^4, x_1^4, x_2^4) = \\ & = F_{12}^1(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ & \vee F_{12}^4(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \\ & \vee F_{12}^7(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4); \\ & S_2(x_0^1, x_1^1, x_2^1, x_0^2, x_1^2, x_2^2, x_0^3, x_1^3, x_2^3, x_0^4, x_1^4, x_2^4) = \\ & = F_{12}^2(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_2^4) \vee \end{aligned}$$

$$\vee F_{12}^5(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_1^4, x_2^4) \vee \\ \vee F_{12}^8(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4, x_1^4, x_2^4).$$

Учитывая утверждение (2.7), функции S_0, S_1, S_2 принимают единичные значения при условиях:

- если $x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 0 \pmod{3}$, то $S_0 = 1$;
- если $x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 1 \pmod{3}$, то $S_1 = 1$;
- если $x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 + x_1^3 + 2x_2^3 + x_1^4 + 2x_2^4 = 2 \pmod{3}$, то $S_2 = 1$.

ФСБФ $F_{12}^0, F_{12}^1, \dots, F_{12}^8$ можно записать следующим образом:

$$F_{12}^0 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 0; \\ 0 & - \text{ в противном случае,} \end{cases} \quad F_{12}^1 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 1; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{12}^2 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 2; \\ 0 & - \text{ в противном случае,} \end{cases} \quad F_{12}^3 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 3; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{12}^4 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 4; \\ 0 & - \text{ в противном случае,} \end{cases} \quad F_{12}^5 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 5; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{12}^6 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 6; \\ 0 & - \text{ в противном случае,} \end{cases} \quad F_{12}^7 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 7; \\ 0 & - \text{ в противном случае,} \end{cases}$$

$$F_{12}^8 = \begin{cases} 1, & \text{если } \sum_{n=1}^4 (x_1^n + 2x_2^n) = 8; \\ 0 & - \text{ в противном случае.} \end{cases}$$

2.2.3 Модулярное умножение двух операндов в унитарных кодах

На основании (2.18) и основного свойства унитарных кодов умножение двух операндов по модулю P можно записать следующим образом [5-А, 14-А]:

$$X_1 \cdot X_2 = (0 \cdot x_0^1 + 1 \cdot x_1^1 + \dots + (P-1) \cdot x_{P-1}^1) \cdot (0 \cdot x_0^2 + 1 \cdot x_1^2 + \dots + (P-1) \cdot x_{P-1}^2) = \quad (2.32)$$

$$= 0 \cdot r_0 + 1 \cdot r_1 + \dots + (P-1) \cdot r_{P-1} = R \pmod{P},$$

где P – простое число.

В результате умножения операндов $(X_1 \pmod{P} \cdot X_2 \pmod{P}) \pmod{P} = R \pmod{P}$ формируются функции $R_0, R_1, \dots, R_{P-1}$, принимающие значения разрядов $r_0, r_1, \dots, r_{P-1}$.

Тогда

$$X_1 \cdot X_2 = \begin{cases} Pr = 0 \pmod{P}; \\ Pr + 1 = 1 \pmod{P}; \\ \dots \\ Pr + k = k \pmod{P}; \\ \dots \\ Pr + P - 1 = (P-1) \pmod{P}, \end{cases} \quad (2.33)$$

где $r = 0, 1, 2, \dots$.

Поскольку $R \pmod{P} = 0 \cdot r_0 + 1 \cdot r_1 + \dots + (P-1) \cdot r_{P-1}$, то результат умножения двух операндов $R \pmod{P}$ можно представить с помощью двоичной матрицы $M(R)$, которая совпадает с матрицей $M(S)$.

Обозначим $R^* = X_1 \cdot X_2$, где $R^* \in \{0, 1, 2, \dots, 2(P-1)\}$. Так как $X_1, X_2 \in \{0, 1, 2, \dots, P-1\}$, то результат умножения $R^* = R \pmod{P}$ можно представить с помощью двоичной матрицы $M(R^*)$, которая имеет вид

$$M(R^*) = \begin{bmatrix} r_{0,0} & r_{0,1} & \dots & r_{0,k} & \dots & r_{0,P-1} \\ r_{1,0} & r_{1,1} & \dots & r_{1,k} & \dots & r_{1,P-1} \\ r_{2,0} & r_{2,1} & \dots & r_{2,k} & \dots & r_{2,P-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_{t,0} & r_{t,1} & \dots & r_{t,k} & \dots & r_{t,P-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_{2(P-1),0} & r_{2(P-1),1} & \dots & r_{2(P-1),k} & \dots & r_{2(P-1),P-1} \end{bmatrix}, \quad (2.34)$$

где $t = \overline{0, 2(P-1)}$. Строкам матрицы соответствуют двоичные значения $R^* \pmod{P}$, а число столбцов совпадает с числом разрядов $R^* \pmod{P}$.

Функция $R_k = 1$ тогда и только тогда, когда $r_{t,k} = 1$.

Например, для $X_1 \cdot X_2 = R \pmod{5}$, где $X_1, X_2 \in \{0, 1, 2, 3, 4\}$, матрица $M(R)$ будет выглядеть следующим образом:

$$M(R) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad (2.35)$$

где строкам матрицы соответствуют двоичные значения, которые принимает результат умножения $R \pmod{5} \in \{0, 1, 2, 3, 4\}$, а число столбцов равно пяти, так как $R \pmod{5} = 0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2 + 3 \cdot r_3 + 4 \cdot r_4$.

В таком случае матрица $M(R^*)$ имеет вид

$$M(R^*) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (2.36)$$

где $R^* = R \pmod{P}$ и $R^* \in \{0, 1, 2, 3, 4, 6, 8, 9, 12, 16\}$.

Функции R_0, R_1, R_2, R_3, R_4 принимают единичные значения при условиях:

- если $r_{0,0} = 1$, то $R^* \in \{0\}$ и $R_0 = 1$;
- если $r_{1,1} = r_{6,1} = r_{16,1} = 1$, то $R^* \in \{1, 6, 16\}$ и $R_1 = 1$;
- если $r_{2,2} = r_{12,2} = 1$, то $R^* \in \{2, 12\}$ и $R_2 = 1$;
- если $r_{3,3} = r_{8,3} = 1$, то $R^* \in \{3, 8\}$ и $R_3 = 1$;
- если $r_{4,4} = r_{9,4} = 1$, то $R^* \in \{4, 9\}$ и $R_4 = 1$.

Если $R^* \notin \{5,7,10,11,13,14,15\}$, то строкам, номера которых принадлежат указанному множеству, соответствуют нулевые наборы «0 0 0 0 0».

Разобьем множество переменных $x_0^1, x_1^1, \dots, x_{P-1}^1, x_0^2, x_1^2, \dots, x_{P-1}^2$ на P подмножеств: $Y_0 = \{x_0^1, x_0^2\}$ и $Y_i = \{\underbrace{x_i^1, \dots, x_i^1}_i, \underbrace{x_j^2, \dots, x_j^2}_P\}$, где $i \cdot j = k \pmod{P}$ и

$i, j, k = \overline{1, P-1}$. Функция $R_k = R_k(Y_1, \dots, Y_{P-1})$ является СБФ, которая зависит от $P(P-1)$ переменных.

Например, для реализации функции $R_2(x_1^1, x_2^1, x_3^1, x_4^1, x_1^2, x_2^2, x_3^2, x_4^2) = R_2(Y_1, Y_2, Y_3, Y_4)$ множества Y_1, Y_2, Y_3, Y_4 будут следующими: $Y_1 = \{x_1^1, x_2^2, x_2^2, x_2^2, x_2^2\}$, $Y_2 = \{x_2^1, x_2^1, x_1^2, x_1^2, x_1^2, x_1^2\}$, $Y_3 = \{x_3^1, x_3^1, x_3^1, x_4^2, x_4^2, x_4^2\}$ и $Y_4 = \{x_4^1, x_4^1, x_4^1, x_3^2, x_3^2, x_3^2\}$.

Таким образом, СБФ R_k можно представить локальным кодом $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{(P-1)^2}^k, \pi_{(P-1)^2+1}^k, \dots, \pi_{P(P+1)}^k)$.

На основании того, что $R^* \leq (P-1)^2$, то $\pi_v^k = 0$, где $v \geq (P-1)^2 + 1$. Тогда локальный код для функции R_k можно записать в виде $\pi(S_k) = (\pi_0^k, \pi_1^k, \pi_2^k, \dots, \pi_{(P-1)^2}^k) = (r_{0,k}, r_{1,k}, r_{2,k}, \dots, r_{(P-1)^2,k})$.

Учитывая вышесказанное, свойства функций $R_0 = R_0(x_0^1, x_1^1, \dots, x_{P-1}^1, x_0^2, x_1^2, \dots, x_{P-1}^2)$ и $R_k = R_k(x_0^1, x_1^1, \dots, x_{P-1}^1, x_0^2, x_1^2, \dots, x_{P-1}^2)$ можно сформулировать с помощью следующих утверждений.

Утверждение 2.8. Функция $R_0 = 1$, тогда и только тогда, когда $x_0^1 = 1$ или $x_0^2 = 1$.

Утверждение 2.9. Функция $R_k = 1$ тогда и только тогда, когда $x_i^1 + x_j^2 = 2$, где $i \cdot j = k \pmod{P}$.

Однако это утверждение эквивалентно следующему.

Утверждение 2.10. Функция $R_k = 1$ тогда и только тогда, когда $i \cdot x_i^1 + (P-i) \cdot x_j^2 = P$, где $i \cdot j = k \pmod{P}$.

Обобщением вышесказанного служит представление, приведенное в нижеследующем утверждении.

Утверждение 2.11. Функция $R_k = 1$ тогда и только тогда, когда

$$\sum_{i=0}^{P-1} \sum_{j=0}^{P-1} ((i+1) \cdot x_i^1 + (P-i) \cdot x_j^2) = P, \quad (2.37)$$

где $i \cdot j = k \pmod{P}$.

Пример 2.7. Пусть $P=3$, т.е. в результате умножения $X_1 \cdot X_2 = R \pmod{3}$ в унитарных кодах, где $X_1, X_2 \in \{0,1,2\}$, формируются функции R_0, R_1, R_2 , принимающие значения разрядов $R \pmod{3} = 0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2$.

Матрица $M(R)$ совпадает с матрицей $M(R)$ из примера 2.6, а матрица $M(R^*)$ примет вид

$$M(R^*) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

где $R^* = R \pmod{P}$ и $R^* \in \{0,1,2,4\}$.

Функции R_0, R_1, R_2 принимают единичные значения при условиях:

- если $r_{0,0} = 1$, то $R^* \in \{0\}$ и $R_0 = 1$;
- если $r_{1,1} = r_{4,1} = 1$, то $R^* \in \{1,4\}$ и $R_1 = 1$;
- если $r_{2,2} = 1$, то $R^* \in \{2\}$ и $R_2 = 1$.

Так как $R^* \notin \{0,1,2,4\}$, то третьей строке матрицы $M(R^*)$, соответствует нулевой набор «0 0 0 0 0».

Локальные коды функций R_1 и R_2 равны $\pi(S_1) = (0,1,0,0,1)$ и $\pi(S_2) = (0,0,1,0,0)$.

На основании использования утверждений 2.8, 2.10 и процедуры симметрирования, функции R_0, R_1, R_2 принимают единичные значения при условиях:

- если $x_0^1 = 1$ и $x_0^2 = 1$, то $R_0 = 1$, где $R_0 = R_0(Y_0)$ и $Y_0 = \{x_0^1, x_0^2\}$;
- если а) $x_1^1 + x_1^2 = 2$ и $x_1^1 + 2x_1^2 = 3$; б) $x_2^1 + x_2^2 = 2$ и $2x_2^1 + x_2^2 = 3$, то $R_1 = 1$, где $R_1 = R_1(Y_1, Y_2)$ и $Y_1 = \{x_1^1, x_1^2, x_1^2\}$, $Y_2 = \{x_2^1, x_2^1, x_2^2\}$;
- если а) $x_1^1 + x_2^2 = 2$ и $x_1^1 + 2x_2^2 = 3$; б) $x_2^1 + x_1^2 = 2$ и $2x_2^1 + x_1^2 = 3$, то $R_2 = 1$, где $R_2 = R_2(Y_1, Y_2)$ и $Y_1 = \{x_1^1, x_2^2, x_2^2\}$, $Y_2 = \{x_2^1, x_2^1, x_1^2\}$.

С учетом (2.37), булевы функции R_0, R_1, R_2 можно записать следующим образом:

$$R_0 = x_0^1 \vee x_0^2;$$

$$R_1 = \begin{cases} 1, & \text{если } x_1^1 + 2x_1^2 + 2x_2^1 + x_2^2 = 3; \\ 0 & - \text{в противном случае,} \end{cases} \quad R_2 = \begin{cases} 1, & \text{если } x_1^1 + 2x_2^2 + 2x_2^1 + x_1^2 = 3; \\ 0 & - \text{в противном случае.} \end{cases}$$

Пример 2.8. В результате умножения $X_1 \cdot X_2 = R \pmod{5}$ в унитарных кодах, где $X_1, X_2 \in \{0, 1, 2, 3, 4\}$, формируются функции R_0, R_1, R_2, R_3, R_4 , принимающие значения разрядов r_0, r_1, r_2, r_3, r_4 , где $R \pmod{3} = 0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2 + 3 \cdot r_3 + 4 \cdot r_4$.

Матрицы $M(R)$ и $M(R^*)$ примут вид (2.35) и (2.36).

Локальные коды функций R_1, R_2, R_3, R_4 равны $\pi^1 = (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$, $\pi^2 = (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$, $\pi^3 = (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$, $\pi^4 = (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$.

На основании использования утверждений 2.8, 2.10 и процедуры симметрирования, функции R_0, R_1, R_2, R_3, R_4 принимают единичные значения при условиях:

- если $x_0^1 = 1$ и $x_0^2 = 1$, то $R_0 = 1$, где $R_0 = R_0(Y_0)$ и $Y_0 = \{x_0^1, x_0^2\}$;
- если а) $x_1^1 + x_1^2 = 2$ и $x_1^1 + 4x_1^2 = 5$; б) $x_2^1 + x_3^2 = 2$ и $2x_2^1 + 3x_3^2 = 5$; в) $x_3^1 + x_2^2 = 2$ и $3x_3^1 + 2x_2^2 = 5$; г) $x_4^1 + x_4^2 = 2$ и $4x_4^1 + x_4^2 = 5$, то $R_1 = 1$, где $R_1 = R_1(Y_1, Y_2, Y_3, Y_4)$ и $Y_1 = \{x_1^1, x_1^2, x_1^2, x_1^2, x_1^2\}$, $Y_2 = \{x_2^1, x_2^1, x_3^2, x_3^2, x_3^2\}$, $Y_3 = \{x_3^1, x_3^1, x_3^1, x_2^2, x_2^2\}$, $Y_4 = \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^2\}$;
- если а) $x_1^1 + x_2^2 = 2$ и $x_1^1 + 4x_2^2 = 5$; б) $x_2^1 + x_1^2 = 2$ и $2x_2^1 + 3x_1^2 = 5$; в) $x_3^1 + x_4^2 = 2$ и $3x_3^1 + 2x_4^2 = 5$; г) $x_4^1 + x_3^2 = 2$ и $4x_4^1 + x_3^2 = 5$, то $R_2 = 1$, где $R_2 = R_2(Y_1, Y_2, Y_3, Y_4)$, а множества Y_1, Y_2, Y_3, Y_4 описаны выше;
- если а) $x_1^1 + x_3^2 = 2$ и $x_1^1 + 4x_3^2 = 5$; б) $x_2^1 + x_4^2 = 2$ и $2x_2^1 + 3x_4^2 = 5$; в) $x_3^1 + x_1^2 = 2$ и $3x_3^1 + 2x_1^2 = 5$; г) $x_4^1 + x_2^2 = 2$ и $4x_4^1 + x_2^2 = 5$, то $R_3 = 1$, где $R_3 = R_3(Y_1, Y_2, Y_3, Y_4)$ и $Y_1 = \{x_1^1, x_3^2, x_3^2, x_3^2, x_3^2\}$, $Y_2 = \{x_2^1, x_2^1, x_4^2, x_4^2, x_4^2\}$, $Y_3 = \{x_3^1, x_3^1, x_3^1, x_2^2, x_2^2\}$, $Y_4 = \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^2\}$;
- если а) $x_1^1 + x_4^2 = 2$ и $x_1^1 + 4x_4^2 = 5$; б) $x_2^1 + x_2^2 = 2$ и $2x_2^1 + 3x_2^2 = 5$; в) $x_3^1 + x_3^2 = 2$ и $3x_3^1 + 2x_3^2 = 5$; г) $x_4^1 + x_1^2 = 2$ и $4x_4^1 + x_1^2 = 5$, то $R_4 = 1$, где $R_4 = R_4(Y_1, Y_2, Y_3, Y_4)$ и $Y_1 = \{x_1^1, x_4^2, x_4^2, x_4^2, x_4^2\}$, $Y_2 = \{x_2^1, x_2^1, x_2^2, x_2^2, x_2^2\}$, $Y_3 = \{x_3^1, x_3^1, x_3^1, x_3^2, x_3^2\}$, $Y_4 = \{x_4^1, x_4^1, x_4^1, x_4^1, x_4^1\}$.

Учитывая (2.37), булевы функции R_0, R_1, R_2, R_3, R_4 можно записать следующим образом:

$$R_0 = x_0^1 \vee x_0^2,$$

$$R_1 = \begin{cases} 1, & \text{если } x_1^1 + 4x_1^2 + 2x_2^1 + 3x_3^2 + 3x_3^1 + 2x_2^2 + 4x_4^1 + x_4^2 = 5; \\ 0 & \text{в противном случае,} \end{cases}$$

$$R_2 = \begin{cases} 1, & \text{если } x_1^1 + 4x_1^2 + 2x_2^1 + 3x_3^2 + 3x_3^1 + 2x_2^2 + 4x_4^1 + x_4^2 = 5; \\ 0 & \text{– в противном случае,} \end{cases}$$

$$R_3 = \begin{cases} 1, & \text{если } x_1^1 + 4x_1^2 + 2x_2^1 + 3x_3^2 + 3x_3^1 + 2x_2^2 + 4x_4^1 + x_4^2 = 5; \\ 0 & \text{– в противном случае,} \end{cases}$$

$$R_4 = \begin{cases} 1, & \text{если } x_1^1 + 4x_1^2 + 2x_2^1 + 3x_3^2 + 3x_3^1 + 2x_2^2 + 4x_4^1 + x_4^2 = 5; \\ 0 & \text{– в противном случае.} \end{cases}$$

Приведенные в этой главе математические модели модулярных операций сложения и умножения служат основой для предлагаемых в последующих главах методов синтеза и VHDL-моделей устройств МА.

2.3 Выводы

1. Аппарат СБФ является эффективным средством описания операций модулярного сложения и модулярного умножения для случая представления данных в двоичных позиционных и унитарных кодах. В общем случае предложенные математические модели имеют вид системы дизъюнкций ФСБФ.

2. Предложенные математические модели ориентированы на построение одноуровневых логических схем модулярных сумматоров и умножителей двух операндов для случая представления данных в унитарных кодах, а также двухуровневых логических схем модулярных сумматоров произвольного числа операндов для случая представления данных в унитарных и двоичных позиционных кодах.

ГЛАВА 3

МЕТОДЫ СИНТЕЗА ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ МОДУЛЯРНОЙ АРИФМЕТИКИ

Методы синтеза принято делить на два типа [27, 119]: методы синтеза двухуровневых и многоуровневых логических схем.

Идея синтеза двухуровневых логических схем связана с разложением реализуемых булевых функций в классах ДНФ и КНФ [126, 134], а также в классе полиномов [66, 79, 141]. Как правило, целью минимизации является сокращение слагаемых и переменных в ДНФ, КНФ или полиноме, реализующем булеву функцию, а критерием оптимальности схем, синтезированных на основе использования таких разложений, является число слагаемых в представлении реализуемой булевой функции и (или) число входящих в это разложение (или полином) переменных [27].

В основе методов синтеза многоуровневых схем лежат методы декомпозиции и факторизации булевых функций [2–4, 12, 17, 26, 52–54, 91, 101, 111]. Методы решения задач синтеза таких логических схем были основаны на дизъюнктивном разложении Шеннона, диаграммах двоичного выбора. Главным недостатком этих методов является ограниченность для решения задач большой размерности и низкое быстродействие схем, синтезируемых на их основе.

В этой главе будут рассмотрены методы синтеза логических схем устройств МА. Эффективность логических схем определяется числом логических элементов, сложностью схемы устройства L (суммой входов элементов схемы – сложность по Квайну), глубиной (числом уровней) T схемы и числом ее внешних выводов M .

В основу методов синтеза логических схем модулярных сумматоров и умножителей положено использование мажоритарного (порогового) представления логических элементов.

Схемы из пороговых элементов находят свое применение при реализации арифметико-логических устройств, схемах контроля и помехоустойчивого кодирования, распознавании образов, проверки четности и нечетности и др. [21, 51, 53, 54, 121, 128]. Такие схемы обладают меньшей сложностью, меньшим количеством межсоединений, однотипностью и однородностью структуры [4, 24, 51, 53, 54, 92].

В зависимости от области применения, представление логических элементов имеет смысл разделять на мажоритарное и пороговое [31, 48, 58, 64].

Если входам элементов присваиваются весовые коэффициенты, то такое представление носит название порогового. Если некоторые из входов дублируются, то все входы элемента являются равновесными и такое представление называется мажоритарным. Оба представления используются при реализации устройств МА и основаны на применении различных классов булевых функций [4, 48–50, 52–54]. Решению задач, связанных с описанием и реализацией устройств вычислительной техники на основе применения мажоритарных и пороговых элементов посвящены, например, работы [24, 49, 50, 52, 53, 58–60, 75, 92, 121, 128 и др.]. При дальнейшем описании методов синтеза будем использовать мажоритарное представление логических элементов.

Логический элемент, на входы которого поступают значения двоичных переменных $x_1, x_2, \dots, x_\delta$, а на его выходе формируется значение ФСБФ $F = F_n^a(x_1, x_2, \dots, x_\delta)$, будем называть элементом ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом a . Этот элемент описывается посредством выражения

$$F_n^a(x_1, x_2, \dots, x_\delta) = \begin{cases} 1, & \text{если } x_1 + x_2 + \dots + x_\delta = a; \\ 0 & - \text{в противном случае,} \end{cases}$$

и обозначается как показано на рисунке 3.1.

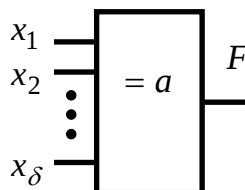


Рисунок 3.1 – Элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом a

Схемы устройств, реализующие модулярные операции сложения $X_1 + X_2 + \dots + X_N = S \pmod{P}$ и умножения $X_1 \cdot X_2 = R \pmod{P}$, будем обозначать $S(N, P)$ и $R(2, P)$, и называть модулярным сумматором и модулярным умножителем соответственно.

Предлагаемые методы синтеза таких устройств можно разделить на два этапа: построение математической модели (например, системы булевых функций) и построение логической схемы устройства в заданном элементном базисе.

В общем случае, используя полученные представления, логическая схема устройства может быть синтезирована на основании дизъюнктивного разложения СБФ.

Перейдем к описанию методов синтеза схем устройств МА.

3.1 Метод синтеза сумматоров в позиционных кодах

Рассмотрим метод синтеза модулярных сумматоров в позиционных кодах [4-А, 16-А]. Первоначально будем полагать, что $P = 3$.

На входы сумматора $S(N, 3)$ поступают операнды $X_1, X_2, \dots, X_N$ и на его выходе формируется результат их сложения S . На основании выбранного модуля и выражения (2.1), $X_1 = x_1^1 + 2 \cdot x_2^1$, $X_2 = x_1^2 + 2 \cdot x_2^2$, ..., $X_N = x_1^N + 2 \cdot x_2^N$ и $S = s_1 + 2 \cdot s_2$, где $X_1, X_2, \dots, X_N, S \in \{0, 1, 2\}$ и $x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N, s_1, s_2 \in \{0, 1\}$.

Как отмечалось, в результате сложения $X_1 + X_2 + \dots + X_N = S \pmod{P}$ формируется двухразрядный набор $S = (s_1, s_2)$ и $S^* = S \pmod{3}$, где $S^* = X_1 + X_2 + \dots + X_N$, $S^* \in \{0, 1, 2, \dots, 2N\}$. Результат сложения $S^* = S \pmod{3}$ представляется с помощью двоичной матрицы $M(S^*)$ вида (2.6).

Матрица $M(S^*)$ состоит из двух столбцов, так как результат сложения задается двухразрядным двоичным набором. Отсюда следует, что схема сумматора будет состоять из логических подсхем $S_1(N, 3)$ и $S_2(N, 3)$, на выходах которых формируются СБФ $S_1 = S_1(x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N)$ и $S_2 = S_2(x_1^1, x_2^1, x_1^2, x_2^2, \dots, x_1^N, x_2^N)$, принимающие значения разрядов s_1 и s_2 соответственно.

Каждая из подсхем, реализующих СБФ S_1 и S_2 , содержит элементы ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, число которых равно весу $|\pi(S_1)|$ и $|\pi(S_2)|$, т.е. числу единиц в $\pi(S_1)$ и $\pi(S_2)$.

Каждая из подсхем $S_1(N, 3)$ и $S_2(N, 3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и элемента ИЛИ. Если в матрице $M(S^*)$ единица содержится на пересечении i -й строки, где $i = \overline{0, 2N}$, и первого столбца, т.е. если $s_{i,1} = 1$, то элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом i принадлежит подсхеме $S_1(N, 3)$. Если же $s_{i,2} = 1$, то элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом i принадлежит подсхеме $S_2(N, 3)$.

Таким образом, если $S^* \in \{1, 4, \dots, 3k_1 - 2\}$, где $k_1 = \left\lceil \frac{2N + 2}{3} \right\rceil$, то $S_1 = 1$; если $S^* \in \{2, 5, \dots, 3k_2 - 1\}$, где $k_2 = \left\lceil \frac{2N + 1}{3} \right\rceil$, то $S_2 = 1$.

Выходы элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, принадлежащих подсхемам $S_1(N, 3)$ и $S_2(N, 3)$, соединены с входами первого и второго элементов ИЛИ, на выходе которых формируются значения функций S_1 и S_2 .

При условии, что $N = 3r + 1$, где $r = 0, 1, 2, \dots$, подсистемы $S_1(N, 3)$ и $S_2(N, 3)$ содержат одинаковое число логических элементов $k_1 = k_2$. Если же $N = 3r - 1$, то $k_1 = k_2 + 1$, т.е. подсистема $S_1(N, 3)$ будет содержать на один логический элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом больше, чем $S_2(N, 3)$.

Каждый из логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом имеет по $3N$ входов, на N из которых поступают значения разрядов $x_1^1, x_1^2, \dots, x_1^N$ и на $2N$ – попарно значения разрядов $x_2^1, x_2^2, \dots, x_2^N$.

Таким образом, логическая схема сумматора $S(N, 3)$ будет содержать $\left\lceil \frac{2N+2}{3} \right\rceil + \left\lceil \frac{2N+1}{3} \right\rceil$ логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и два элемента ИЛИ. При этом сложность схемы $L(S(N, 3))$ по Квайну вычисляется по формуле

$$L(S(N, 3)) = k_1(3N + 1) + k_2(3N + 1) = (3N + 1) \cdot \left(\left\lceil \frac{2N+2}{3} \right\rceil + \left\lceil \frac{2N+1}{3} \right\rceil \right). \quad (3.1)$$

Пример 3.1. При $P = 3$ и $N = 3$ сумматор $S(3, 3)$ реализует операцию $X_1 + X_2 + X_3 = S \pmod{3}$.

На шесть входов сумматора поступают значения разрядов операндов $x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3$, где $X_1 = x_1^1 + 2x_2^1$, $X_2 = x_1^2 + 2x_2^2$ и $X_3 = x_1^3 + 2x_2^3$. На его выходах реализуются значения СБФ $S_1 = S_1(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3)$ и $S_2 = S_2(x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3)$, принимающие значения разрядов s_1 и s_2 , где $S = s_1 + 2s_2$. Функции S_1 и S_2 , локальные коды которых равны $\pi(S_1) = (0, 1, 0, 0, 1, 0, 0)$ и $\pi(S_2) = (0, 0, 1, 0, 0, 1, 0)$ (из матрицы $M(S^*)$ примера 2.2), вычисляются в соответствие с дизъюнктивными разложениями, приведенными в примере 2.2.

Сумматор $S(3, 3)$ состоит из двух подсистем $S_1(3, 3)$ и $S_2(3, 3)$. Так как веса локальных кодов равны $|\pi(S_1)| = |\pi(S_2)| = 2$, то каждая из подсистем содержит по два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и одному элементу ИЛИ.

Каждый из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом содержит по девять входов, на три входа из которых поступают значения разрядов x_1^1, x_1^2, x_1^3 , а на остальные шесть – попарно значения разрядов x_2^1, x_2^2, x_2^3 .

Подсистема $S_1(3, 3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 1 и 4, выходы которых соединены с входами первого элемента ИЛИ. Подсистема $S_2(3, 3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 2 и 5, выходы которых соединены с входами второго элемента ИЛИ.

На рисунке 3.2 изображена схема сумматора $S(3, 3)$, синтезированная в соответствии с представлениями, приведенными в примере 2.2.

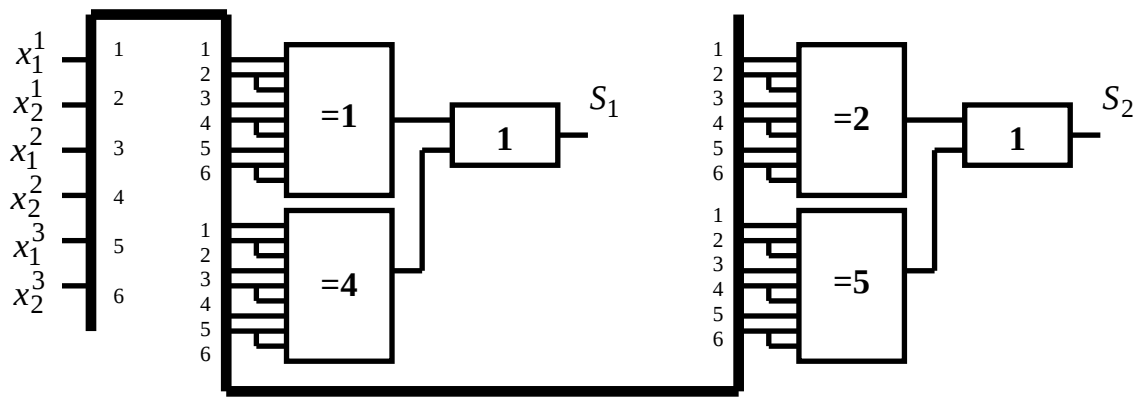


Рисунок 3.2 – Схема сумматора $S(3, 3)$

Из формулы (3.1) следует, что сложность схемы сумматора составляет $L(S(3, 3)) = 40$, число уровней и число внешних выводов схемы равны $T(S(3, 3)) = 2$ и $M(S(3, 3)) = 8$.

Пример 3.2. При $P = 3$ и $N = 4$ сумматор $S(4, 3)$ реализует операцию $X_1 + X_2 + X_3 + X_4 = S \pmod{3}$.

На восемь входов сумматора поступают значения разрядов операндов $x_1^1, x_1^2, x_1^3, x_1^4, x_2^1, x_2^2, x_2^3, x_2^4$, где $X_1 = x_1^1 + 2x_1^2$, $X_2 = x_1^2 + 2x_2^2$, $X_3 = x_1^3 + 2x_2^3$ и $X_4 = x_1^4 + 2x_2^4$. На выходах $S(4, 3)$ реализуются значения СБФ $S_1 = S_1(x_1^1, x_1^2, x_1^3, x_2^1, x_2^2, x_2^3, x_1^4, x_2^4)$ и $S_2 = S_2(x_1^1, x_1^2, x_1^3, x_2^1, x_2^2, x_2^3, x_1^4, x_2^4)$, принимающие значения разрядов s_1 и s_2 , где $S = s_1 + 2s_2$. Функции S_1 и S_2 , локальные коды которых равны $\pi(S_1) = (0, 1, 0, 0, 1, 0, 0, 1, 0)$ и $\pi(S_2) = (0, 0, 1, 0, 0, 1, 0, 0, 1)$ (из матрицы $M(S^*)$ примера 2.3), вычисляются в соответствии с дизъюнктивными разложениями, приведенными в примере 2.3.

Сумматор $S(4, 3)$ состоит из двух подсхем $S_1(4, 3)$ и $S_2(4, 3)$. Так как $|\pi(S_1)| = |\pi(S_2)| = 3$, то каждая из подсхем содержит по три элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и одному элементу ИЛИ.

Каждый из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом содержит по двенадцать входов, на четыре входа из которых поступают значения разрядов $x_1^1, x_1^2, x_1^3, x_1^4$, а на остальные восемь – попарно значения разрядов $x_2^1, x_2^2, x_2^3, x_2^4$.

Подсхема $S_1(4, 3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 1, 4 и 7, выходы которых соединены с входами первого элемента ИЛИ. Подсхема $S_2(4, 3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 2, 5 и 8, выходы которых соединены с входами второго элемента ИЛИ.

На рисунке 3.3 изображена схема сумматора $S(4, 3)$, синтезированная в соответствии с представлениями, приведенными в примере 2.3.

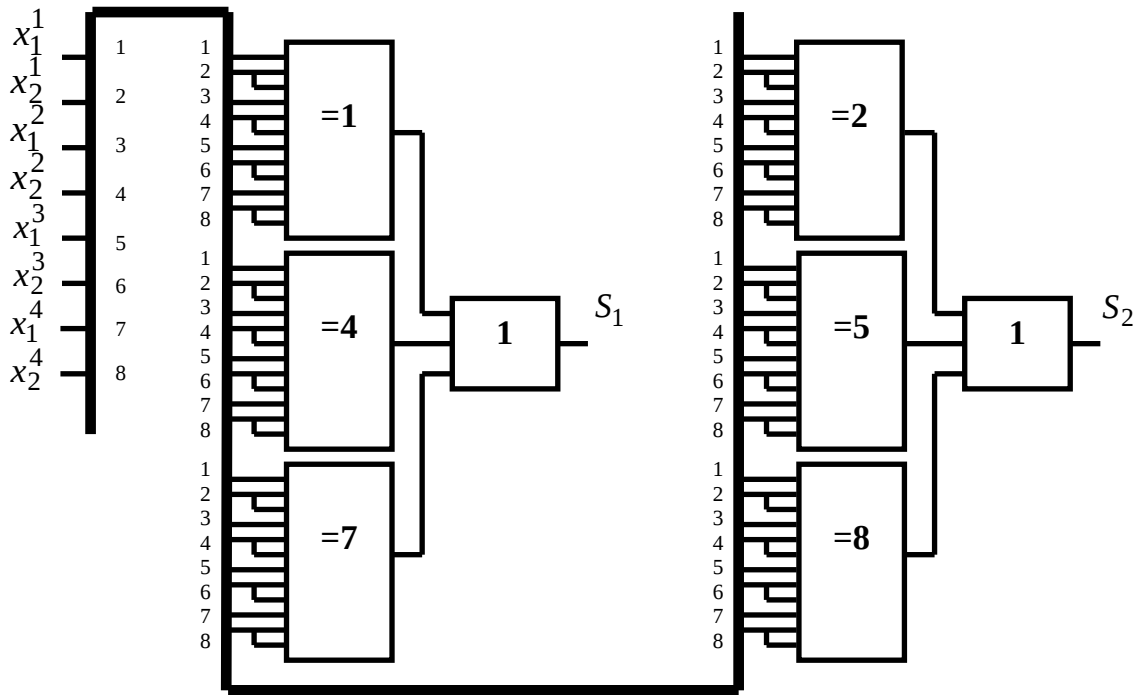


Рисунок 3.3 – Схема сумматора $S(4, 3)$

Из формулы (3.1) следует, что сложность схемы сумматора составляет $L(S(4, 3)) = 78$, а число уровней и число внешних выводов равны $T(S(4, 3)) = 2$ и $M(S(4, 3)) = 10$.

Пусть далее $P \geq 3$, т.е. на входы сумматора $S(N, P)$ поступают операнды $X_1, X_2, \dots, X_N$ и на его выходе формируется результат их сложения S . Входные и выходной операнды задаются δ -разрядными двоичными наборами $X_n = 2^0 \cdot x_1^n + 2^1 \cdot x_2^n + \dots + 2^{\delta-1} \cdot x_\delta^n$ и $S = 2^0 \cdot s_1 + 2^1 \cdot s_2 + \dots + 2^{\delta-1} \cdot s_\delta$, где $x_1^n, x_2^n, \dots, x_\delta^n, s_1, s_2, \dots, s_\delta \in \{0, 1\}$, $X_1, X_2, \dots, X_N, S \in \{0, 1, 2, \dots, P-1\}$, $\delta = \lceil \log_2 P \rceil + 1$ и $n = \overline{1, N}$.

Результат сложения $S^* = S \pmod{P}$, где $X_1 + X_2 + \dots + X_N = S \pmod{P}$, и $S^* \in \{0, 1, 2, \dots, N(P-1)\}$, представляется с помощью двоичной матрицы $M(S^*)$ вида (2.14).

Матрица $M(S^*)$ имеет δ столбцов. В этой связи схема сумматора будет состоять из логических подсхем $S_1(N, P), S_2(N, P), \dots, S_\delta(N, P)$. На выходе подсхемы $S_k(N, P)$ формируется СБФ $S_k = S_k(x_1^1, \dots, x_\delta^1, x_1^2, \dots, x_\delta^2, \dots, x_1^n, \dots, x_\delta^n)$, принимающая значение разряда s_k , где $S = (s_1, s_2, \dots, s_k, \dots, s_\delta)$ и $k = \overline{1, \delta}$.

Подсхема $S_k(N, P)$, реализующая функцию S_k , содержит $|\pi(S_k)|$ элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом.

Каждая из подсхем состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и элемента ИЛИ. Если в матрице $M(S^*)$ единица содержится на

пересечении i – й строки, где $i = \overline{0, N(P-1)}$, и k – го столбца, т.е. если $s_{i,k} = 1$, матрицы, то элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом i принадлежит подсхеме $S_k(N, P)$.

В отличие от двоичной матрицы для случая при $P = 3$, строки $M(S^*)$ для $P > 3$ могут содержать более одной единицы. Это значит, что элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом может принадлежать сразу нескольким подсхемам.

Например, в результате сложения двух операндов по модулю 17 двоичная матрица $M(S^*)$ будет состоять из 5 столбцов и 33 строк, т.е.

$$M(S^*) = \begin{bmatrix} s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} \\ \dots & & & & \\ s_{13,1} & s_{13,2} & s_{13,3} & s_{13,4} & s_{13,5} \\ \dots & & & & \\ s_{32,1} & s_{32,2} & s_{32,3} & s_{32,4} & s_{32,5} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ \dots & & & & \\ 1 & 0 & 1 & 1 & 0 \\ \dots & & & & \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Из матрицы видно, что если сумма $X_1 + X_2 = S \pmod{17} = 13 \pmod{17}$, то двоичный набор результата сложения будет равен $S \pmod{17} = (s_1, s_2, s_3, s_4, s_5) = (1, 0, 1, 1, 0)$, чему соответствует четырнадцатая строка, т.е. $s_{13,1} = s_{13,3} = s_{13,4} = 1$. Таким образом, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом 13 принадлежит подсхемам $S_1(2, 17)$, $S_3(2, 17)$ и $S_4(2, 17)$.

В общем случае подсхема $S_k(N, P)$ состоит из двух уровней. Выходы элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, принадлежащих $S_k(N, P)$ соединены с входами элемента ИЛИ, на выходе которого формируется значение функции S_k .

Следует отметить, что подсхема $S_\delta(2, P)$ является одноуровневой и состоит из единственного элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом $P-1$, если $P = 2^m + 1$, где $m \in N$.

Каждый из логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом имеет по $N(2^\delta - 1)$ входов, на $2^k \cdot N$ из которых поступают значения переменных $x_k^1, x_k^2, \dots, x_k^N$.

Таким образом, логическая схема сумматора $S(N, P)$ будет содержать $N(P-1) - \left\lfloor \frac{N(P-1)}{P} \right\rfloor$ логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и $\delta - 1$ элементов ИЛИ, если $P = 2^m + 1$ и $N = 2$, и δ элементов ИЛИ

в противном случае. При этом сложность схемы сумматора $L(S(N,P))$ по Квайну вычисляется посредством формулы

$$L(S(N,P)) = \left(N(P-1) - \left\lfloor \frac{N(P-1)}{P} \right\rfloor \right) \cdot (2^\delta - 1)N + \sum_{k=1}^{\delta} |\pi(S_k)|. \quad (3.2)$$

Предлагаемый метод позволяет синтезировать логические схемы превосходящие по глубине свои аналоги синтезированные известными методами [4].

Пример 3.3. При $N=2$ сумматор $S(2,5)$ реализует операцию $X_1 + X_2 = S \pmod{5}$.

На шесть входов сумматора поступают значения разрядов операндов $x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2$, где $X_1 = x_1^1 + 2x_2^1 + 4x_3^1$ и $X_2 = x_1^2 + 2x_2^2 + 4x_3^2$. На его выходах реализуются значения СБФ $S_1(x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2)$, $S_2(x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2)$ и $S_3(x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2)$, принимающие значения разрядов s_1, s_2 и s_3 , где $S = s_1 + 2s_2 + 4s_3$. Функции S_1, S_2 и S_3 , локальные коды которых равны $\pi(S_1) = (0, 1, 0, 1, 0, 0, 1, 0, 1)$, $\pi(S_2) = (0, 0, 1, 1, 0, 0, 0, 1, 1)$ и $\pi(S_3) = (0, 0, 0, 0, 1, 0, 0, 0, 0)$ (из матрицы $M(S^*)$ примера 2.4), вычисляются в соответствии с дизъюнктивными разложениями, приведенными в примере 2.4.

Сумматор $S(2,5)$ состоит из трех подсхем $S_1(2,5), S_2(2,5)$ и $S_3(2,5)$. Так как $|\pi(S_1)| = |\pi(S_2)| = 4$ и $|\pi(S_3)| = 1$, а также $P=5$, то подсхемы $S_1(2,5)$ и $S_2(2,5)$ содержат по четыре элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и одному элементу ИЛИ, а подсхема $S_3(2,5)$ состоит из одного элемента – элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом.

Каждый из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом содержит по четырнадцать входов, на два входа из которых поступают значения разрядов x_1^1, x_1^2 , на четыре входа – попарно значения x_2^1, x_2^2 и на остальные восемь входов – четырежды значения разрядов x_3^1, x_3^2 .

Подсхема $S_1(2,5)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 1, 3, 6 и 8, выходы которых соединены с входами первого элемента ИЛИ. Подсхема $S_2(2,5)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 2, 3, 7 и 8, выходы которых соединены с входами второго элемента ИЛИ. Подсхема $S_3(2,5)$ состоит из элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом 4.

На рисунке 3.4 изображена схема сумматора $S(2,5)$, синтезированная в соответствии с представлениями, приведенными в примере 2.4.

Из формулы (3.2) следует, что сложность схемы сумматора составляет $L(S(2, 5)) = 106$, а число уровней и число внешних выводов равны, соответственно, $T(S(2, 5)) = 2$ и $M(S(2, 5)) = 9$.

3.2 Метод синтеза арифметических устройств в унитарных кодах

Далее излагается метод синтеза схем модулярных сумматоров $S(N, P)$ и умножителей $R(2, P)$ для случая представления данных в унитарных кодах [5-А, 12-А–13-А, 18-А].

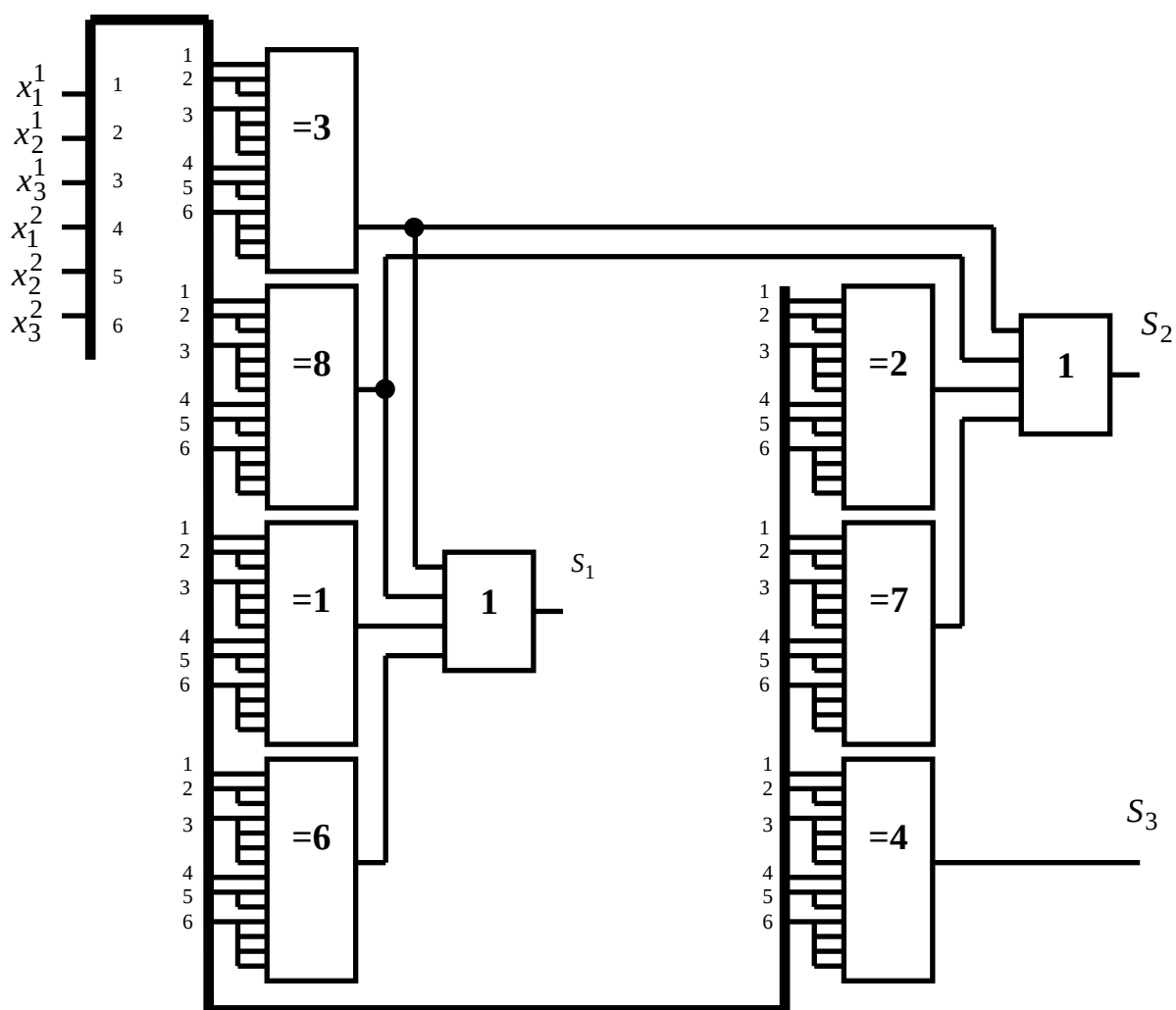


Рисунок 3.4 – Схема сумматора $S(2, 5)$

На основании (2.18) входные операнды $X_1, X_2, \dots, X_N$ и результаты их сложения S и умножения R по модулю P задаются P -разрядными двоичными наборами. Каждый из операндов можно представить следующим образом: $U \pmod{P} = (u_0, u_1, \dots, u_{P-1})$ и $U \pmod{P} = a_0 \cdot u_0 + a_1 \cdot u_1 + \dots + a_{P-1} \cdot u_{P-1}$, где

$U \in \{X_1, X_2, \dots, X_N, S, R\}$, $X_1, X_2, \dots, X_N, S, R \in \{0, 1, \dots, P-1\}$ и $u_0, u_1, \dots, u_{P-1} \in \{0, 1\}$. Напомним, что основным свойством унитарного кода является тот факт, что $u_0 + u_1 + \dots + u_{P-1} = 1$.

Как в предыдущей главы, имеет смысл отдельно рассматривать случай при $N = 2$ и $N \geq 2$.

3.2.1 Метод синтеза сумматоров в унитарных кодах

Рассмотрим случай при $N = 2$ [5-A, 13-A], т.е. когда модулярный сумматор $S(2, P)$ выполняет операцию

$$X_1 + X_2 = \sum_{i=0}^{P-1} \sum_{j=0}^{P-1} (i \cdot x_i^1 + j \cdot x_j^2) = S \pmod{P}.$$

Иначе говоря, входные X_1, X_2 и выходной S операнды в унитарных кодах представляются в виде $X_1 = a_0^1 \cdot x_0^1 + a_1^1 \cdot x_1^1 + \dots + a_{P-1}^1 \cdot x_{P-1}^1$, $X_2 = a_0^2 \cdot x_0^2 + a_1^2 \cdot x_1^2 + \dots + a_{P-1}^2 \cdot x_{P-1}^2$ и $S = a_0 \cdot s_0 + a_1 \cdot s_1 + \dots + a_{P-1} \cdot s_{P-1}$. Как отмечалось выше, $x_k^1 = 1$, $x_k^2 = 1$ и $s_k = 1$ тогда и только тогда, когда $X_1 \pmod{P} = k$, $X_2 \pmod{P} = k$, $S \pmod{P} = k$ и $X_1, X_2, S \in \{0, 1, \dots, P-1\}$, $a_0^1, \dots, a_{P-1}^1, a_0^2, \dots, a_{P-1}^2, a_0, \dots, a_{P-1}, k \in \{0, 1, \dots, P-1\}$, $x_0^1, \dots, x_{P-1}^1, x_0^2, \dots, x_{P-1}^2, s_0, \dots, s_{P-1} \in \{0, 1\}$.

В таком случае результат сложения $S \pmod{P} = S^*$, где $X_1 + X_2 = S \pmod{P}$, и $S^* \in \{0, 1, 2, \dots, N(P-1)\}$, представляется с помощью двоичной матрицы $M(S^*)$ вида (2.23).

Из того, что матрица $M(S^*)$ состоит из P столбцов, т.е. в результате сложения формируется P -разрядный двоичный набор, следует, что схема сумматора будет состоять из логических подсхем $S_0(2, P), S_1(2, P), \dots, S_{P-1}(2, P)$. На выходе подсхемы $S_k(2, P)$ формируются СБФ $S_k = S_k(Y_0, Y_1, \dots, Y_{P-1})$, которая зависит от $P(P+1)$ переменных и принимает значение s_k , где $Y_i = \{\underbrace{x_i^1, \dots, x_i^1}_{i+1}, \underbrace{x_j^2, \dots, x_j^2}_{P+1}\}$ и $i + j = k \pmod{P}$.

Подсхема $S_k(2, P)$ содержит один элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом.

На основании утверждений 2.4 и 2.5 элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, содержащийся в подсхеме $S_k(2, P)$, содержит $P(P+1)$ входов, на

которые поступают значения разрядов $x_0^1, \dots, x_{P-1}^1, x_0^2, \dots, x_{P-1}^2$, и один выход, на котором формируется СБФ S_k .

Таким образом, логическая схема сумматора $S(2, P)$ будет содержать P логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом $P+1$. Сложность схемы $L(S(2, P))$ по Квайну вычисляется по формуле

$$L(S(2, P)) = P^2 (P + 1). \quad (3.3)$$

Пример 3.4. При $P=5$ сумматор $S(2, 5)$ в унитарных кодах реализует операцию $X_1 + X_2 = S \pmod{5}$ [49-A].

На десять входов сумматора поступают значения разрядов операндов $x_0^1, x_1^1, x_2^1, x_3^1, x_4^1, x_0^2, x_1^2, x_2^2, x_3^2, x_4^2$, где $X_1 = 0 \cdot x_0^1 + 1 \cdot x_1^1 + 2 \cdot x_2^1 + 3 \cdot x_3^1 + 4 \cdot x_4^1$ и $X_2 = 0 \cdot x_0^2 + 1 \cdot x_1^2 + 2 \cdot x_2^2 + 3 \cdot x_3^2 + 4 \cdot x_4^2$. На его выходах формируются значения СБФ S_0, S_1, S_2, S_3, S_4 , принимающих значения разрядов s_0, s_1, s_2, s_3, s_4 , где $S = 0 \cdot s_0 + 1 \cdot s_1 + 2 \cdot s_2 + 3 \cdot s_3 + 4 \cdot s_4$.

Сумматор состоит из пяти подсхем $S_0(2, 5), S_1(2, 5), S_2(2, 5), S_3(2, 5)$ и $S_4(2, 5)$ – пяти элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом шесть. На выходах элементов формируются значения СБФ

$$\begin{aligned} - S_0 &= S_0(Y_0, Y_1, Y_2, Y_3, Y_4), \text{ где } Y_0 = \{x_0^1, x_0^2\}, Y_1 = \{x_1^1, x_4^2\}, Y_2 = \{x_2^1, x_3^2\}, \\ Y_3 &= \{x_3^1, x_2^2\} \text{ и } Y_4 = \{x_4^1, x_1^2\}; \\ - S_1 &= S_1(Y_0, Y_1, Y_2, Y_3, Y_4), \text{ где } Y_0 = \{x_0^1, x_1^2\}, Y_1 = \{x_1^1, x_0^2\}, Y_2 = \{x_2^1, x_4^2\}, \\ Y_3 &= \{x_3^1, x_3^2\} \text{ и } Y_4 = \{x_4^1, x_2^2\}; \\ - S_2 &= S_2(Y_0, Y_1, Y_2, Y_3, Y_4), \text{ где } Y_0 = \{x_0^1, x_2^2\}, Y_1 = \{x_1^1, x_1^2\}, Y_2 = \{x_2^1, x_0^2\}, \\ Y_3 &= \{x_3^1, x_4^2\} \text{ и } Y_4 = \{x_4^1, x_3^2\}; \\ - S_3 &= S_3(Y_0, Y_1, Y_2, Y_3, Y_4), \text{ где } Y_0 = \{x_0^1, x_3^2\}, Y_1 = \{x_1^1, x_2^2\}, Y_2 = \{x_2^1, x_1^2\}, \\ Y_3 &= \{x_3^1, x_0^2\} \text{ и } Y_4 = \{x_4^1, x_4^2\}; \\ - S_4 &= S_4(Y_0, Y_1, Y_2, Y_3, Y_4), \text{ где } Y_0 = \{x_0^1, x_4^2\}, Y_1 = \{x_1^1, x_3^2\}, Y_2 = \{x_2^1, x_2^2\}, \\ Y_3 &= \{x_3^1, x_1^2\} \text{ и } Y_4 = \{x_4^1, x_0^2\}. \end{aligned}$$

Каждый из элементов содержит по 30 входов, на которые поступают значения переменных из множеств Y_0, Y_1, Y_2, Y_3, Y_4 , приведенных в примере 2.5.

На рисунке 3.5 изображена схема сумматора унитарных кодов $S(2, 5)$, синтезированная согласно представлениями, приведенным в примере 2.5.

Из формулы (3.3) следует, что сложность схемы сумматора составляет $L(S(2, 5))=150$, а число уровней и число внешних выводов схемы равны $T(S(2, 5))=1$ и $M(S(2, 5))=15$.

Пусть далее $N \geq 2$, т.е. сумматор в унитарных кодах $S(N, P)$ реализует операцию $X_1 + X_2 + \dots + X_N = S \pmod{P}$. Входные и выходные операнды

задаются P –разрядными унитарными кодами, причем $x_k^n = 1$ и $s_k = 1$ тогда и только тогда, когда $X_n \pmod{P} = k$ и $S \pmod{P} = k$, где $k = \overline{0, P-1}$, $n = \overline{1, N}$, $X_n, S \in \{0, 1, \dots, P-1\}$, $X_n = a_0^n \cdot x_0^n + a_1^n \cdot x_1^n + \dots + a_{P-1}^n \cdot x_{P-1}^n$, $S = a_0 \cdot s_0 + a_1 \cdot s_1 + \dots + a_{P-1} \cdot s_{P-1}$, $a_0^n, a_1^n, \dots, a_{P-1}^n, a_0, \dots, a_{P-1}, k \in \{0, 1, \dots, P-1\}$, $x_0^n, x_1^n, \dots, x_{P-1}^n, s_0, \dots, s_{P-1} \in \{0, 1\}$.

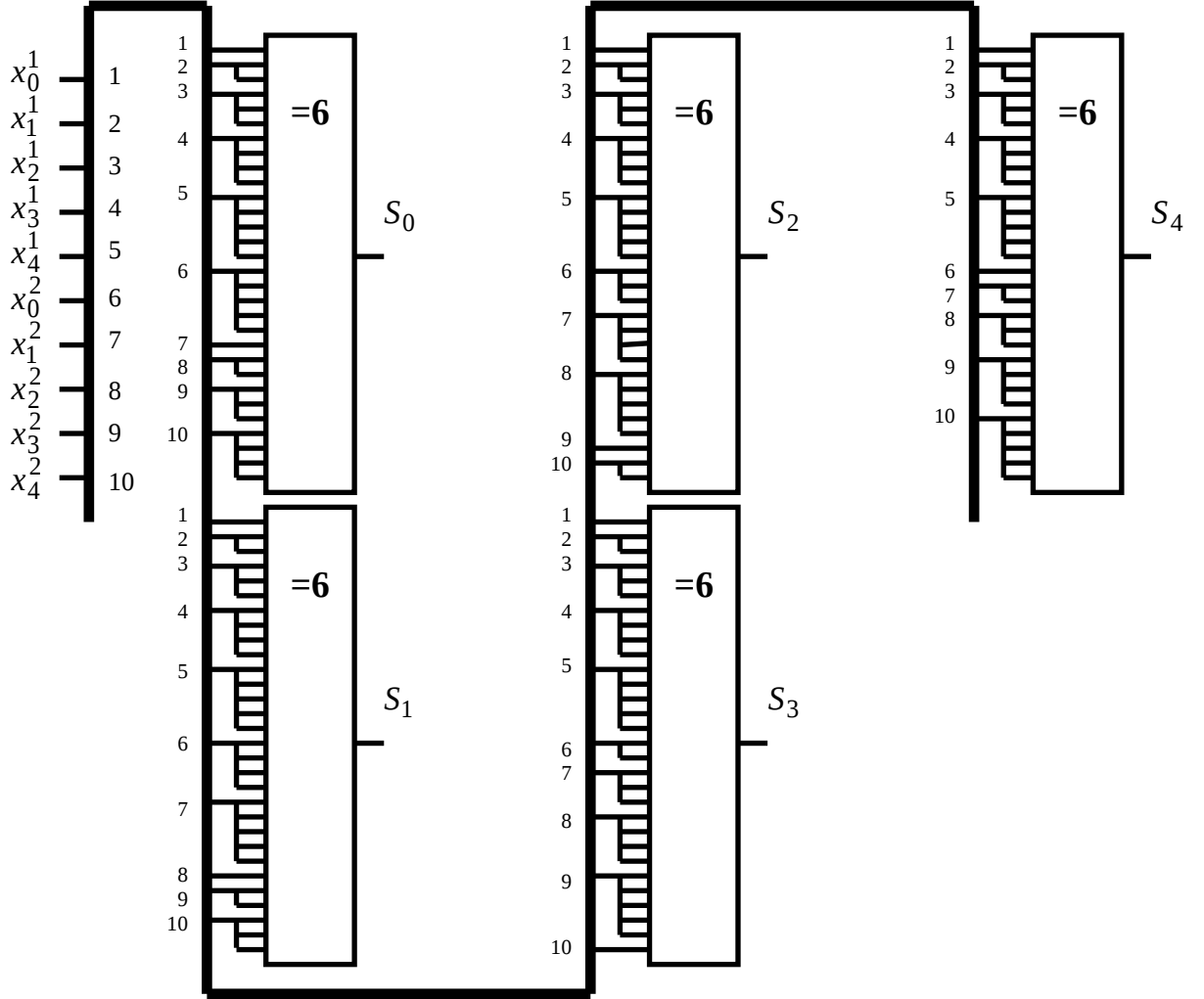


Рисунок 3.5 – Схема сумматора $S(2, 5)$

В таком случае результат сложения $S \pmod{P} = S^*$, где $X_1 + X_2 + \dots + X_N = S \pmod{P}$ и $S^* \in \{0, 1, 2, \dots, N(P-1)\}$, представляется с помощью двоичной матрицы $M(S^*)$ вида (2.29).

Как и в предыдущем случае, матрица $M(S^*)$ содержит P столбцов, значит, схема сумматора будет состоять из логических подсхем $S_0(N, P), S_1(N, P), \dots, S_{P-1}(N, P)$. На выходе подсхемы $S_k(N, P)$ формируются

$$\text{СБФ} \quad S_k = S_k \left(Y_1, Y_2, Y_2, \dots, \underbrace{Y_k, \dots, Y_k}_k, \dots, \underbrace{Y_{P-1}, \dots, Y_{P-1}}_{P-1} \right), \quad \text{которая зависит от}$$

$\frac{(P^2 - P)N}{2}$ переменных и принимает значение разряда s_k , где $Y_i = \underbrace{\{x_i^1, \dots, x_i^1, x_j^2, \dots, x_j^2\}}_{i+1}^{P+1}$ и $i + j = k \pmod{P}$.

Подсхема $S_k(N, P)$ содержит элементы ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, число которых равно $|\pi(S_k)|$.

Каждая из подсхем состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и элемента ИЛИ. Если в матрице $M(S^*)$ единица содержится на пересечении i -й строки, где $t = \overline{0, N(P-1)}$, и k -го столбца, т.е. если $s_{t,k} = 1$, то элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом t принадлежит подсхеме $S_k(N, P)$.

Из определения унитарного кода следует, что каждая строка матрицы (2.22) содержит ровно одну единицу. Это означает, что элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом принадлежит ровно одной подсхеме.

В общем случае подсхема $S_k(N, P)$ состоит из двух уровней. Выходы элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, принадлежащих $S_k(N, P)$, соединены с входами элемента ИЛИ, на выходе которого формируется значение функции S_k .

Отметим, что подсхема $S_{P-1}(N, P)$ является одноуровневой, если $N = 2$, и состоит из единственного элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом $P-1$. Однако, на основании вышеприведенного метода для $N = 2$, каждая из подсхем сумматора будет одноуровневой и использовать описываемый метод для такого случая неэффективно.

Каждый из логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом имеет по $\frac{(P-1) \cdot P}{2} N$ входов, на $k \cdot N$ из которых поступают значения разрядов $x_k^1, x_k^2, \dots, x_k^N$, где $k = \overline{0, P-1}$, каждый из которых дублируется k раз.

Таким образом, логическая схема сумматора унитарных кодов $S(N, P)$ будет содержать $N \cdot (P-1) + 1$ логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и P элементов ИЛИ. При этом сложность схемы сумматора $L(S(N, P))$ по Квайну вычисляется по формуле

$$\begin{aligned} L(S(N, P)) &= \frac{(P-1) \cdot P}{2} N \cdot ((P-1) \cdot N + 1) + (P-1) \cdot N + 1 = \\ &= ((P-1) \cdot N + 1) \cdot \left(\frac{(P-1) \cdot P}{2} N + 1 \right). \end{aligned} \quad (3.4)$$

Наиболее эффективный из известных методов с точки зрения конструктивной сложности приводит к логическим схемам модулярных сумматоров в унитарных кодах со сложностью $L(S(N,P)) = P^N(N+1)$ [74]. Очевидно, сложность этих сумматоров значительно превышает сложность модулярных сумматоров, синтезированных приведенным выше методом. Глубина схем, синтезируемых обоими методами, совпадает.

Пример 3.5. При $N=4$ и $P=3$ сумматор $S(4,3)$ реализует операцию $X_1 + X_2 + X_3 + X_4 = S \pmod{3}$.

На рисунке 3.6 изображена схема сумматора $S(4,3)$, синтезированная в соответствии с представлениями, приведенными в примере 2.6.

На входы сумматора $S(4,3)$ поступают значения разрядов операндов $x_1^1, x_2^1, x_1^2, x_2^2, x_1^3, x_2^3, x_1^4, x_2^4$, где $X_1 = 0 \cdot x_0^1 + 1 \cdot x_1^1 + 2 \cdot x_2^1$, $X_2 = 0 \cdot x_0^2 + 1 \cdot x_1^2 + 2 \cdot x_2^2$, $X_3 = 0 \cdot x_0^3 + 1 \cdot x_1^3 + 2 \cdot x_2^3$ и $X_4 = 0 \cdot x_0^4 + 1 \cdot x_1^4 + 2 \cdot x_2^4$.

Сумматор состоит из трех подсхем $S_0(4,3)$, $S_1(4,3)$ и $S_2(4,3)$, на выходах которых формируются СБФ S_0, S_1, S_2 , принимающие значения разрядов s_0, s_1, s_2 , где $S = 0 \cdot s_0 + 1 \cdot s_1 + 2 \cdot s_2$.

Из примера 2.6 следует, что локальные коды СБФ S_0, S_1, S_2 равны $\pi(S_0) = (1, 0, 0, 1, 0, 0, 1, 0, 0)$, $\pi(S_1) = (0, 1, 0, 0, 1, 0, 0, 1, 0)$ и $\pi(S_2) = (0, 0, 1, 0, 0, 1, 0, 0, 1)$. Откуда следует, что $|\pi(S_0)| = |\pi(S_1)| = |\pi(S_2)| = 3$. В таком случае каждая из подсхем сумматора содержит по три элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и одному элементу ИЛИ.

Элементы ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом содержат двенадцать входов, на четыре входа из которых поступают значения разрядов $x_1^1, x_1^2, x_1^3, x_1^4$ и на остальные восемь входов дважды поступают значения $x_2^1, x_2^2, x_2^3, x_2^4$.

Подсхема $S_0(4,3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 0, 3 и 6, выходы которых соединены с входами первого элемента ИЛИ. Подсхема $S_1(4,3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 1, 4 и 7, выходы которых соединены с входами второго элемента ИЛИ. Подсхема $S_2(4,3)$ состоит из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогами 2, 5 и 8.

Сложность схемы сумматора составляет $L(S(4,3)) = 117$, а число уровней и число внешних выводов схемы равны $T(S(4,3)) = 2$ и $M(S(4,3)) = 11$.

3.2.2 Метод синтеза умножителей в унитарных кодах

Модулярный умножитель унитарных кодов $R(2,P)$ выполняет операцию умножения $[5-A, 14-A]$, которую запишем следующим образом:

$$X_1 \cdot X_2 = \sum_{i=0}^{P-1} (i \cdot x_i^1) \cdot \sum_{j=0}^{P-1} (j \cdot x_j^2) = R \pmod{P}.$$

Входные операнды умножителя представляются по аналогии с входными операндами сумматора. Результат умножения $R \pmod{P}$ представляется P -разрядным двоичным набором и $R = a_0 \cdot r_0 + a_1 \cdot r_1 + \dots + a_{P-1} \cdot r_{P-1}$, где $r_k = 1$, $R \pmod{P} = k$, $R \in \{0, 1, \dots, P-1\}$, $a_0, \dots, a_{P-1}, k \in \{0, 1, \dots, P-1\}$ и $r_0, \dots, r_{P-1} \in \{0, 1\}$.

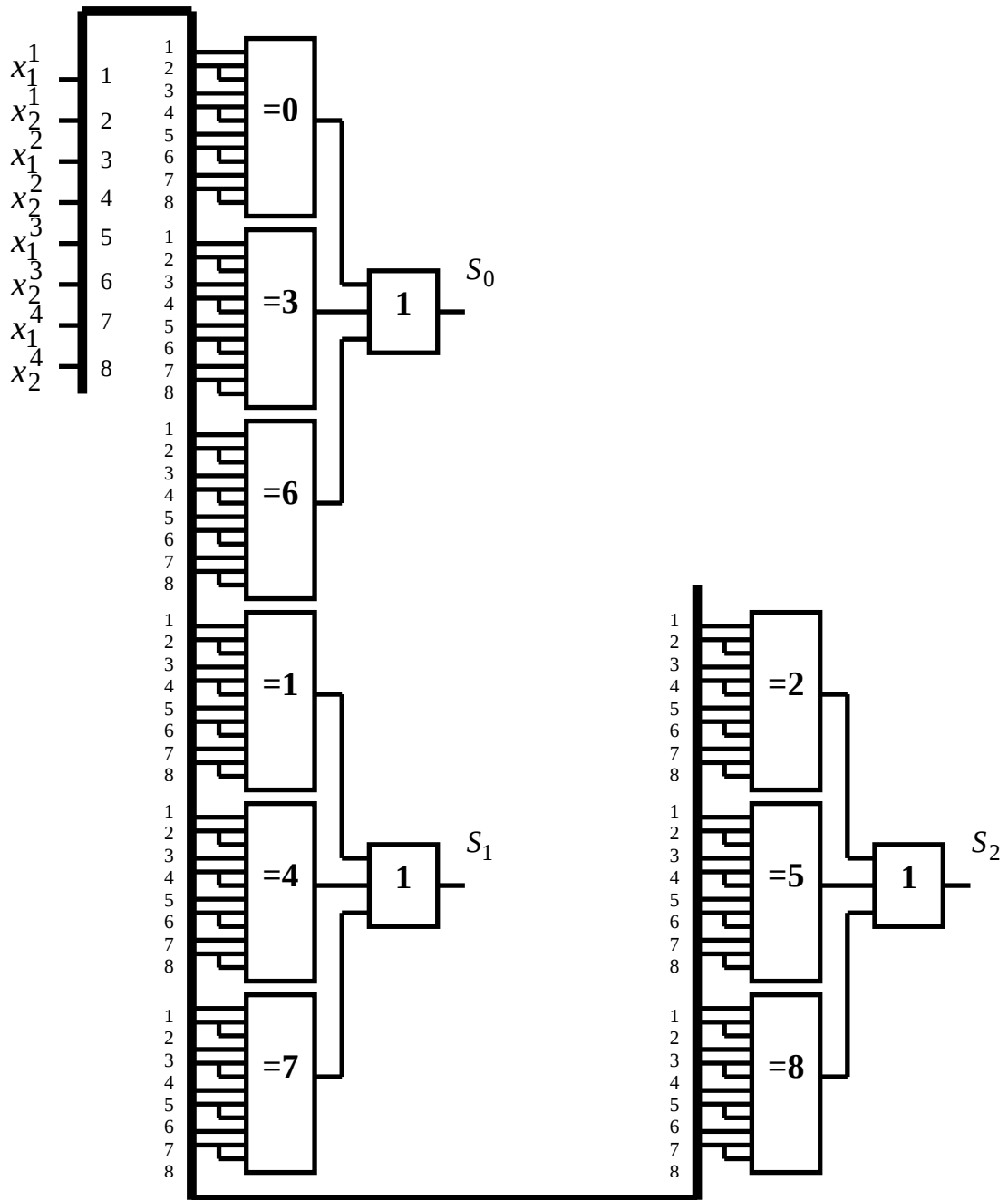


Рисунок 3.6 – Схема сумматора $S(4,3)$

Результат умножения $R^* = R \pmod{P}$, где $X_1 \cdot X_2 = R \pmod{P}$ и $R^* \in \{0, 1, 2, \dots, 2(P-1)\}$. Представляется с помощью двоичной матрицы $M(R^*)$ вида (2.34).

Поскольку матрица $M(R^*)$ состоит из P столбцов, т.е. в результате умножения формируется P – разрядный двоичный набор, то схема умножителя будет состоять из логических подсхем $R_0(2, P), R_1(2, P), \dots, R_{P-1}(2, P)$.

Из утверждения 2.8 следует, что на выходе подсхемы $R_0(2, P)$ формируется функция $R_0 = R_0(x_0^1, x_0^2)$, которая зависит от двух переменных и принимает значение r_0 . Функция $R_0 = 1$ в том случае, если $x_0^1 \vee x_0^2 = 1$.

На выходе подсхемы $R_k(2, P)$, формируется СБФ $R_k = R_k(Y_1, \dots, Y_{P-1})$, зависящая от $P(P-1)$ переменных, где $Y_i = \underbrace{\{x_i^1, \dots, x_i^1, x_i^2, \dots, x_i^2\}}_P$,

$i \cdot j = k \pmod{P}$ и $i, j, k = \overline{1, P-1}$.

Подсхема $R_k(2, P)$ содержит один элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом P .

На основании применения утверждений 2.10 и 2.11 элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом, принадлежащий подсхеме $R_k(2, P)$, содержит $P(P-1)$ входов, на которые поступают значения разрядов $x_0^1, \dots, x_{P-1}^1, x_0^2, \dots, x_{P-1}^2$, и один выход, на котором формируется СБФ S_k .

Таким образом, логическая схема модулярного умножителя унитарных кодов $R(2, P)$ будет состоять из элемента ИЛИ и $P-1$ логических элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом P . Сложность по Квайну схемы умножителя $L(R(2, P))$ вычисляется по формуле

$$L(R(2, P)) = P(P-1)^2 + 2. \quad (3.5)$$

Пример 3.6. Пусть умножитель $R(2, 3)$ в унитарных кодах реализует операцию $X_1 \cdot X_2 = R \pmod{3}$ [34-А].

На шесть входов умножителя поступают значения разрядов операндов $x_0^1, x_1^1, x_2^1, x_0^2, x_1^2, x_2^2$, где $X_1 = 0 \cdot x_0^1 + 1 \cdot x_1^1 + 2 \cdot x_2^1$ и $X_2 = 0 \cdot x_0^2 + 1 \cdot x_1^2 + 2 \cdot x_2^2$. На его выходах формируются значения булевых функций R_0, R_1, R_2 , принимающих значения разрядов r_0, r_1, r_2 , где $R = 0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2$.

Умножитель $R(2, 3)$ состоит из трех подсхем. Подсхема $R_0(2, 3)$ состоит из элемента ИЛИ, а подсхемы $R_1(2, 3)$ и $R_2(2, 3)$ – из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом три.

На выходе элемента ИЛИ формируется значение булевой функции $R_0 = R_0(Y_0)$, где $x_0^1, x_0^2 \in Y_0$. На выходах элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом три формируются значения СБФ

- $R_1 = R_1(Y_1, Y_2)$, где $Y_1 = \{x_1^1, x_1^2\}$ и $Y_2 = \{x_2^1, x_2^2\}$;
- $R_2 = R_2(Y_1, Y_2)$, где $Y_1 = \{x_1^1, x_2^2\}$ и $Y_2 = \{x_2^1, x_1^2\}$.

Таким образом, на входы элемент ИЛИ поступают значения разрядов x_0^1, x_0^2 , а на входы элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом три – значения разрядов $x_1^1, x_1^2, x_2^1, x_2^2$.

На рисунке 3.7 изображена схема умножителя унитарных кодов $S(2,3)$, синтезированная в соответствии с представлениями, приведенными в примере 2.7.

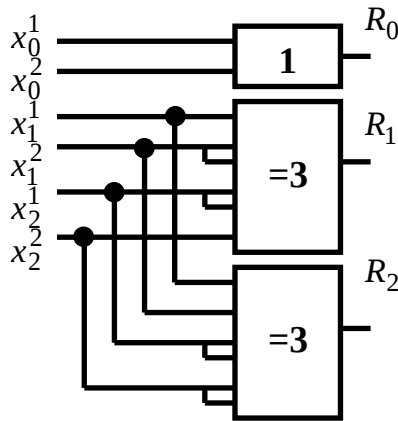


Рисунок 3.7 – Схема умножителя $R(2, 3)$

Сложность по Квайну схемы умножителя составляет $L(R(2,3))=14$, а число уровней и внешних выводов равны $T(R(2,3))=1$ и $M(R(2,3))=9$.

Пример 3.7. Модулярный умножитель $R(2,5)$ в унитарных кодах реализует операцию $X_1 \cdot X_2 = R \pmod{5}$ [48-А].

На десять входов умножителя поступают значения разрядов операндов $x_0^1, x_1^1, x_2^1, x_3^1, x_4^1, x_0^2, x_1^2, x_2^2, x_3^2, x_4^2$, где $X_1 = 0 \cdot x_0^1 + 1 \cdot x_1^1 + 2 \cdot x_2^1 + 3 \cdot x_3^1 + 4 \cdot x_4^1$ и $X_2 = 0 \cdot x_0^2 + 1 \cdot x_1^2 + 2 \cdot x_2^2 + 3 \cdot x_3^2 + 4 \cdot x_4^2$. На его выходах формируются значения СБФ R_0, R_1, R_2, R_3, R_4 , принимающих значения разрядов r_0, r_1, r_2, r_3, r_4 , где $R = 0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2 + 3 \cdot r_3 + 4 \cdot r_4$.

Умножитель $R(2,5)$ состоит из пяти подсхем. Подсхема $R_0(2,5)$ состоит из элемент ИЛИ, а подсхемы $R_1(2,5), R_2(2,5), R_3(2,5)$ и $R_4(2,5)$ – из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять.

На выходе элемента ИЛИ формируется значение функции $R_0 = R_0(Y_0)$, где $x_0^1, x_0^2 \in Y_0$. На выходах элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять формируются значения СБФ

– $R_1 = R_1(Y_1, Y_2, Y_3, Y_4)$, где $Y_1 = \{x_1^1, x_1^2\}$, $Y_2 = \{x_2^1, x_2^2\}$, $Y_3 = \{x_3^1, x_3^2\}$ и $Y_4 = \{x_4^1, x_4^2\}$;

– $R_2 = R_2(Y_1, Y_2, Y_3, Y_4)$, где $Y_1 = \{x_1^1, x_2^2\}$, $Y_2 = \{x_2^1, x_1^2\}$, $Y_3 = \{x_3^1, x_4^2\}$ и $Y_4 = \{x_4^1, x_3^2\}$;

– $R_3 = R_3(Y_1, Y_2, Y_3, Y_4)$, где $Y_1 = \{x_1^1, x_3^2\}$, $Y_2 = \{x_2^1, x_4^2\}$, $Y_3 = \{x_3^1, x_2^2\}$ и $Y_4 = \{x_4^1, x_2^2\}$;

– $R_4 = R_4(Y_1, Y_2, Y_3, Y_4)$, где $Y_1 = \{x_1^1, x_4^2\}$, $Y_2 = \{x_2^1, x_2^2\}$, $Y_3 = \{x_3^1, x_3^2\}$, $Y_4 = \{x_4^1, x_1^2\}$.

На входы элемента ИЛИ поступают значения разрядов x_0^1, x_0^2 , а на входы элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять – значения разрядов $x_1^1, x_2^1, x_3^1, x_4^1, x_1^2, x_2^2, x_3^2, x_4^2$.

На рисунке 3.8 изображена схема умножителя унитарных кодов $R(2, 5)$, синтезированная в соответствии с представлениями, приведенными в примере 2.8.

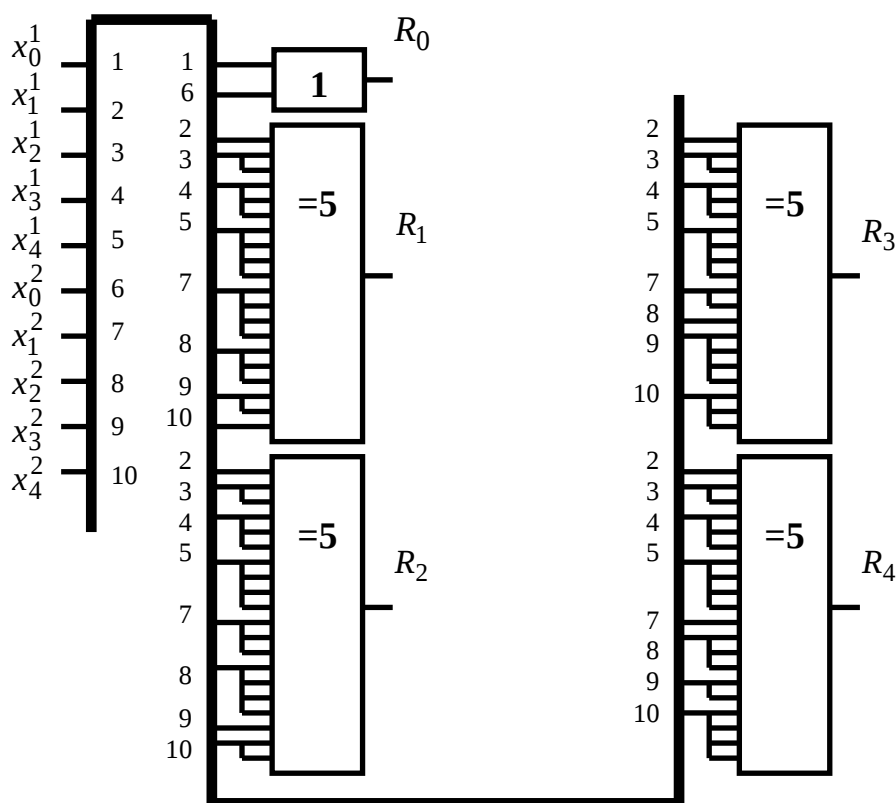


Рисунок 3.8 – Схема умножителя $R(2, 5)$

Сложность схемы модулярного умножителя составляет $L(R(2,5))=82$, а число уровней и внешних выводов схемы равны, соответственно, $T(R(2,5))=1$ и $M(R(2,5))=15$.

3.3 Метод блочно-структурного синтеза устройств модулярной арифметики

Метод блочно-структурного синтеза логических схем вычислительных устройств МА основан на использовании заранее разработанных «блоков» – схем устройств МА [2-А, 7-А–11-А, 19-А], которые будем обозначать $\odot_1, \odot_2, \dots, \odot_n$. Эти «блоки» предназначены для реализации арифметических операций МА сложения $X_1 + X_2 = S \pmod{P}$, умножения $X_1 \cdot X_2 = R \pmod{P}$ и возведения в степень $X_1^{X_2} = Q \pmod{P}$.

Метод ориентирован на синтез схем устройств МА $\odot$, реализующих произвольную суперпозицию трех указанных выше операций. Схемы, предназначенные для выполнения операций МА по модулю P и синтезированные с помощью блочно-структурного метода синтеза, будем обозначать $H(\odot, P)$.

Общая идея метода состоит в следующем. Первоначально необходимо построить структуру устройства, состоящую из модулярных «блоков» сложения, умножения и возведения в степень. Синтез устройства, предназначенного для вычисления суперпозиции указанных операций, предлагается начинать с выбора «блока», реализующего операцию, встречающуюся чаще остальных в рассматриваемой суперпозиции. Это связано с тем, что эти «блоки» потенциально чаще остальных будут участвовать в объединении с другими «блоками».

Затем необходимо подобрать логические схемы «блоков» такие, что после их подстановки в структуру устройства можно было бы «на стыках» объединять одноименные логические элементы, обладающие свойством ассоциативности (например, элементы И, ИЛИ и СЛОЖЕНИЕ ПО МОДУЛЮ ДВА), уменьшая тем самым сложность и (или) глубину логической схемы вычислительного устройства, реализующего первоначально заданную суперпозицию операций. Кроме того, если на этом этапе использовать логические схемы «блоков», например, с меньшим числом внешних выводов, то появляется возможность удалить из логической схемы часть логических элементов.

Очевидно, что для повышения эффективности применения метода блочно-структурного синтеза требуется иметь широкую номенклатуру логических схем «блоков», отличающихся друг от друга типом использованных

логических элементов, сложностью, глубиной и (или) числом внешних выводов.

Например, пусть необходимо синтезировать устройство $\odot$, реализующее в унитарных кодах арифметическую операцию $X_1 \cdot X_2 + X_3 \cdot X_4 = F \pmod{3}$, которое обозначим $H(\odot, \mathbb{Z}_3)$.

Для этого необходимо рассмотреть устройства, предназначенные для вычисления модулярных операций $X_1 + X_2 = S \pmod{3}$ и $X_1 \cdot X_2 = R \pmod{3}$. Операнды X_1 и X_2 , а также результаты вычислений S и R представляются в унитарных кодах, т.е. $X_1 = (x_0^1, x_1^1, x_2^1)$, $X_2 = (x_0^2, x_1^2, x_2^2)$, $S = (s_0, s_1, s_2)$ и $R = (r_0, r_1, r_2)$, где $x_k^1 = 1$, $x_k^2 = 1$, $s_k = 1$ и $r_k = 1$ тогда и только тогда, когда $X_1 \pmod{3} = k$, $X_2 \pmod{3} = k$, $S \pmod{3} = k$, $R \pmod{3} = k$ и $k = 0, 1, 2$.

Обозначим логическую схему сумматора с наименьшей конструктивной сложностью среди известных аналогов – $V_1(\odot, \mathbb{Z}_3)$ [75], а схему сумматора с минимальным числом внешних выводов – $V_2(\odot, \mathbb{Z}_3)$. Схемы $V_1(\odot, \mathbb{Z}_3)$ и $V_2(\odot, \mathbb{Z}_3)$ представлены, соответственно, на рисунке 3.9 а) и б). На выходах сумматора реализуются функции S_0, S_1, S_2 , принимающие значения разрядов s_0, s_1, s_2 .

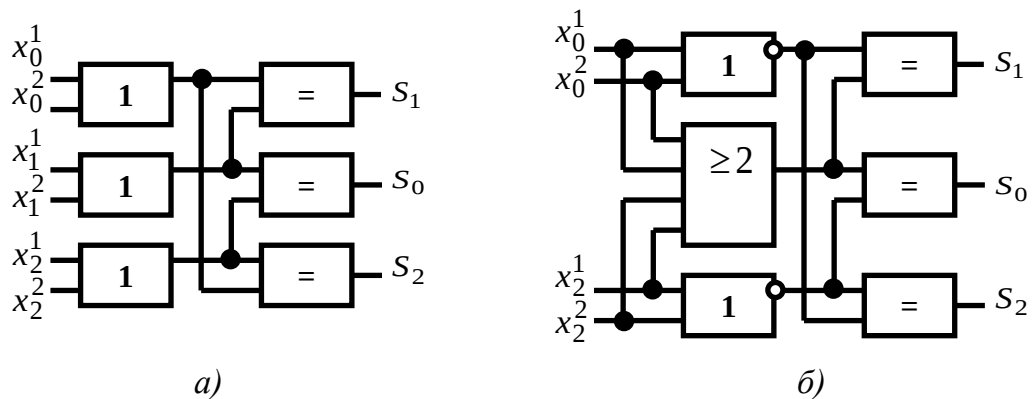


Рисунок 3.9 – Логические схемы сумматоров:
а) схема $V_1(\odot, \mathbb{Z}_3)$; б) схема $V_2(\odot, \mathbb{Z}_3)$

Логическую схему умножителя, синтезированную на основе применения ДНФ функций R_0, R_1, R_2 , обозначим $W_1(\odot, \mathbb{Z}_3)$, а схему умножителя с минимальным числом внешних выводов и наименьшей сложностью по числу логических элементов – $W_2(\odot, \mathbb{Z}_3)$ [88]. Схемы $W_1(\odot, \mathbb{Z}_3)$ и $W_2(\odot, \mathbb{Z}_3)$ представлены, соответственно, на рисунке 3.10 а) и б). На выходах умножителя реализуются функции R_0, R_1, R_2 , принимающие значения разрядов r_0, r_1, r_2 .

Структура устройства $H(\odot, \mathbb{Z}_3)$ содержит два «блока» умножителя, выходы каждого из которых соединены с входами «блока» сумматора.

На выходах устройства $H(\odot, \mathbb{Z}_3)$ формируются функции F_0, F_1, F_2 , принимающие значения разрядов f_0, f_1, f_2 , где $F = (f_0, f_1, f_2)$.

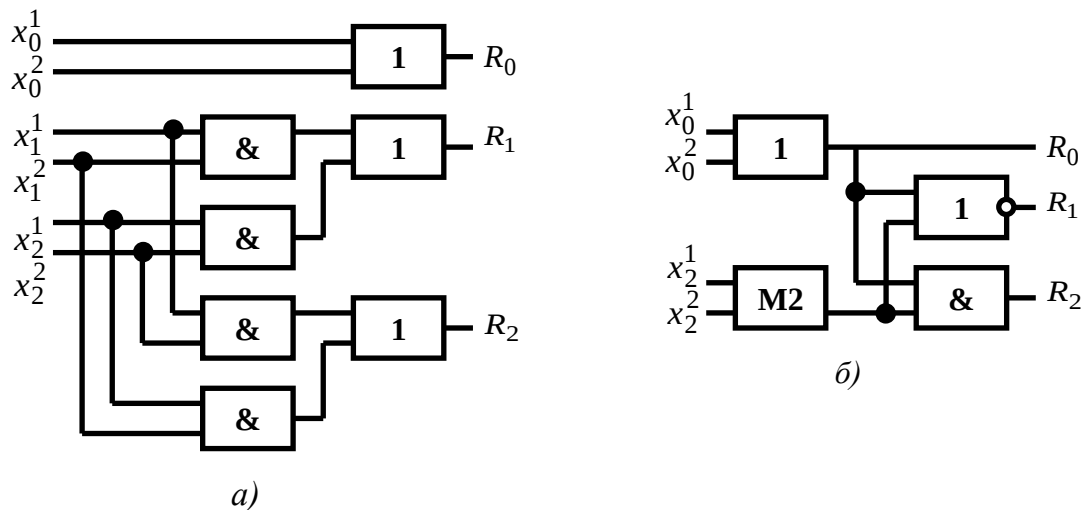


Рисунок 3.10 – Логические схемы умножителей:
а) схема $W_1(\otimes, 3)$; б) схема $W_2(\otimes, 3)$

В результате объединения «блоков» $W_1(\otimes, 3)$ и $V_1(\otimes, 3)$ получим промежуточную логическую схему устройства $H_1^*(\otimes, 3)$. Так как второй и третий уровни схемы $H_1^*(\otimes, 3)$ составляют логические элементы ИЛИ, то после их объединения получаем логическую схему $H_1(\otimes, \boxplus)$ [21-A], приведенную на рисунке 3.11.

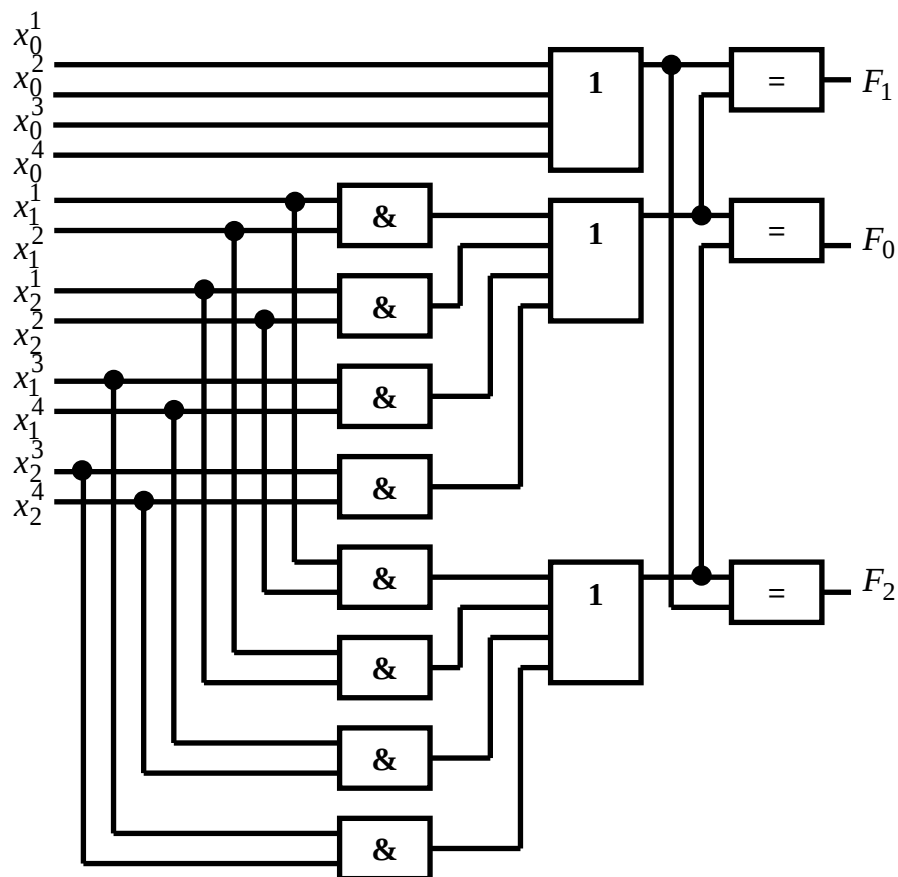


Рисунок 3.11 – Логическая схем устройства $H_1(\otimes, \boxplus)$

Обозначим через $H_2(\odot, 3)$ устройство, реализующее операцию $X_1 \cdot X_2 + X_3 \cdot X_4 = F \pmod{3}$ и состоящее из двух умножителей $W_2(\odot, 3)$, приведенных на рисунке 3.10 б), и сумматора $V_2(\odot, 3)$, приведенного на рисунке 3.9 б). В результате объединения «блоков» $W_2(\odot, 3)$ и $V_2(\odot, 3)$ получим промежуточную логическую схему устройства $H_2^*(\odot, 3)$. Так как в логической схеме $V_2(\odot, 3)$ отсутствуют входы, на которые подаются значения разрядов x_1^1 и x_1^2 , то из схемы $H_2^*(\odot, 3)$ можно удалить два элемента ИЛИ-НЕ, на выходах которых в схеме $W_2(\odot, 3)$ реализуется логическая функция R_1 . Полученная в результате таких преобразований схема $H_2(\odot, 3)$ представлена на рисунке 3.12.

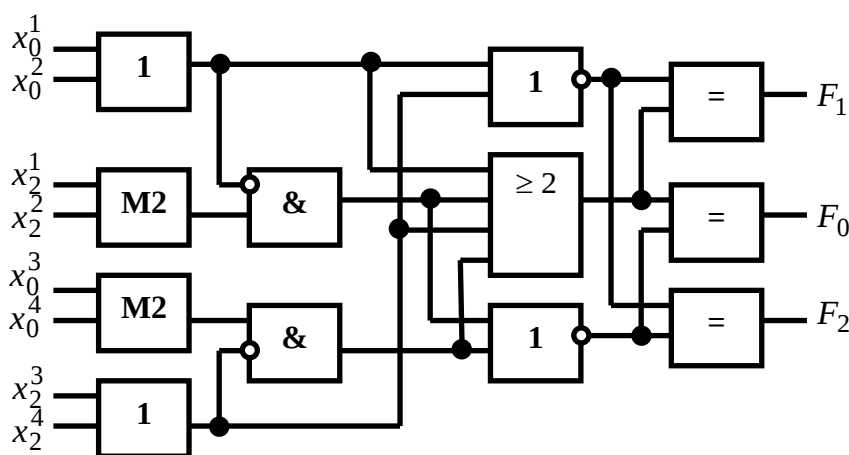


Рисунок 3.12 – Логическая схема устройства $H_2(\odot, 3)$

Число элементов схемы $H_1(\odot, 3)$ равно 14, ее сложность по Квайну и число уровней составляют $L(F(\odot, 3))=34$ и $T(F(\odot, 3))=3$ соответственно. Число элементов схемы $H_2(\odot, 3)$ равно 12, а ее сложность по Квайну и число уровней – $L(F(\odot, 3))=34$ и $T(F(\odot, 3))=4$. Схема $H_1(\odot, 3)$ обладает меньшей сложностью по сравнению с $H_2(\odot, 3)$, хотя сложность «блоков», реализующих элементарные операции, из которых состоит схема $H_1(\odot, 3)$ по отдельности превышает сложность «блоков», входящие в состав схемы $H_2(\odot, 3)$.

С помощью данного метода удалось синтезировать логические схемы, реализующие операции МА для различных значений модуля и числа операндов в позиционных и унитарных кодах, выполняющие, например, операции $\pm X_1 \pm X_2 \pm X_3 \pm X_4 = S \pmod{3}$, $(\pm X_1 \pm X_2) \cdot (\pm X_3 \pm X_4) = S \pmod{3}$, $(\pm X_1) \cdot (\pm X_2) + (\pm X_3) \cdot (\pm X_4) = S \pmod{3}$, $(\pm X_1)^{Y_1} \cdot (\pm X_2)^{Y_2} \cdot \dots \cdot (\pm X_N)^{Y_N} = S \pmod{3}$. Новизна и эффективность разработанных схем подтверждена Патентами на изобретение Республики Беларусь [20-А-24-А, 26-А, 27-А, 29-А, 30-А, 33-А, 36-А-39-А, 42-А, 43-А, 45-А, 47-А].

3.4 Устройства с управляющими входами

При разработке некоторых видов цифровой аппаратуры наряду с высокой скоростью обработки информации, регулярностью и однородностью его структуры, предъявляются требования универсальности и многофункциональности, возможность реализации отдельного класса функций на одном и том же оборудовании.

Одним из подходов решения этой задачи является разработка и применение многофункциональных логических модулей. Работы [10–12, 17, 22, 26, 47, 65, 78, 86, 87, 93, 117] посвящены вопросам использования настраиваемых модулей, методам проектирования устройств цифровой обработки информации на их основе, выбору их структуре и функциональных возможностей. Ряд работ посвящен методам реализации различных многофункциональных модулей на основе однородных элементов [11, 65].

Входы таких устройств классифицируются следующим образом [10]:

- 1) информационные – входы, на которые поступают значения булевых переменных входных операндов;
- 2) управляющие – входы, на которые поступают сигналы, определяющие тип операции, реализуемой на выходе устройства;
- 3) настроечные – входы, на которые поступают сигналы, определяющие функцию, реализуемую на выходе устройства.

Настройка может быть простой и сложной. В первом случае настроечные сигналы принимают значения из множества $\{0,1\}$, во втором – из множества $\{0,1, \overline{x_1}, \overline{x_2}, \dots, \overline{x_n}\}$.

Разработке и синтезу устройств, которые реализуют различные классы булевых функций и обладают различными типами настройки, посвящены, в частности, работы [3, 5, 12, 17, 26, 50, 52, 52–54, 65, 66, 77–82].

УЛМ называют устройство, предназначенное для реализации произвольной булевой функции $F = F(x_1, x_2, \dots, x_n)$. Как правило, на информационные входы УЛМ поступают значения n переменных $x_1, x_2, \dots, x_n$, а на 2^n настроечных входов $u_1, u_2, \dots, u_{2^n}$ – сигналы настройки, определяющие одну из 2^{2^n} функций, реализуемых на его выходе.

МЛМ называется такое устройство, которое реализует все функции $F = F(x_1, x_2, \dots, x_n)$ из некоторого класса булевых функций. Как правило, на информационные входы МЛМ поступают значения n переменных функции $x_1, x_2, \dots, x_n$, а на k настроечных входов $u_1, u_2, \dots, u_k$ – сигналы настройки, количество которых определяются размерностью этого класса. Например, МЛМ, реализующий симметрические булевы функции $F = F(x_1, x_2, \dots, x_n)$,

будет содержать n информационных входов и $n+1$ настроечных, так как существует именно 2^{n+1} симметрических булевых функций от n переменных.

Использование настраиваемых УЛМ и МЛМ позволяет укрупнить элементную базу без существенного увеличения номенклатуры элементов [11, 65], а применение сложной настройки позволяет уменьшить сложность схемы (число элементов или число входов элементов) за счет усложнения алгоритма настройки.

Управляющие сигналы, поступающие на входы различных арифметических устройств, элементами которых часто являются УЛМ и МЛМ, определяют тип операции, реализуемой этим устройством.

К устройствам, обладающим постоянной или управляемой настройкой, относятся устройства рассматриваемые выше. Эти устройства обладают только информационными входами, на которые поступают значения разрядов операндов, над которыми выполняются соответствующие операции. Далее рассмотрим устройства, обладающие двумя типами входных сигналов. Первая группа сигналов является информационной, а вторая – настроечной, определяющая тип выполняемой операции.

Рассмотрим устройства с управляющими входами, синтезированные с применением рассмотренных выше методов.

Заранее необходимо отметить, что при возведении в степень возникает неопределенность типа 0^0 . Так как $0 \equiv P \pmod{P}$, то $0^0 \equiv P^P \pmod{P}$. Поскольку $P^P \equiv 0 \pmod{P}$, то будем полагать, что $0^0 \equiv 0 \pmod{P}$.

Рассмотрим схему устройства $\star_{\mathbb{Z}_3}$, реализующего операцию $(X_1 + X_2)^n = F \pmod{3}$ в унитарных кодах [47-A] и представленную на рисунке 3.13. Обозначим ее $H(\star_{\mathbb{Z}_3})$. Схема состоит из трех элементов И, четырех мажоритарных элементов с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять и элемента РАВНОЗНАЧНОСТЬ.

На информационные входы устройства поступают разряды первого $X_1 = (x_0^1, x_1^1, x_2^1)$ и второго $X_2 = (x_0^2, x_1^2, x_2^2)$ операндов. На управляющий вход подается значение двоичной переменной u , где

$$u = \begin{cases} 0, & \text{если } n - \text{четное;} \\ 1 - & \text{в противном случае.} \end{cases}$$

В результате выполнения операции $(X_1 + X_2)^n = F \pmod{3}$ на выходах $H(\star_{\mathbb{Z}_3})$ формируются булевы функции F_0, F_1, F_2 , принимающие значения разрядов f_0, f_1, f_2 соответственно, где $F_1 = (f_0, f_1, f_2)$.

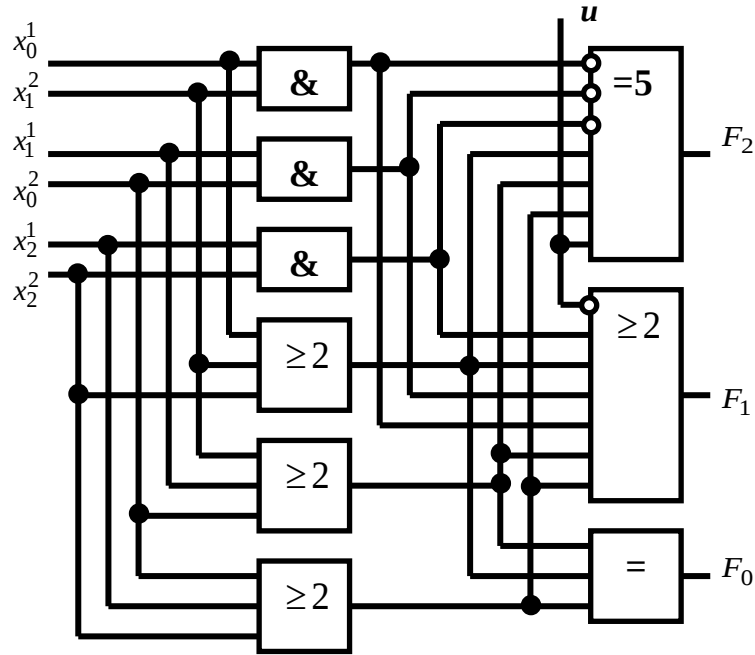


Рисунок 3.13 – Схема устройства $H(\odot_3)$

Аналитические представления функций F_0, F_1, F_2 имеют вид

$$F_0 = \begin{cases} 1, \text{ если } g_1 = g_2 = g_3; \\ 0 - \text{ в противном случае,} \end{cases}$$

$$F_1 = \begin{cases} 1, \text{ если } \bar{u} + h_1 + h_2 + h_3 + g_1 + g_2 + g_3 \geq 2; \\ 0 - \text{ в противном случае,} \end{cases}$$

$$F_2 = \begin{cases} 1, \text{ если } u + \bar{h}_1 + \bar{h}_2 + \bar{h}_3 + g_1 + g_2 + g_3 = 5; \\ 0 - \text{ в противном случае,} \end{cases}$$

где

$$h_1 = x_0^1 x_1^2, \quad h_2 = x_1^1 x_0^2, \quad h_3 = x_2^1 x_2^2,$$

$$g_1 = \begin{cases} 1, \text{ если } x_0^1 + x_1^2 + x_2^2 \geq 2; \\ 0 - \text{ в противном случае,} \end{cases} \quad g_2 = \begin{cases} 1, \text{ если } x_1^1 + x_0^2 + x_1^2 \geq 2; \\ 0 - \text{ в противном случае,} \end{cases}$$

$$g_3 = \begin{cases} 1, \text{ если } x_2^1 + x_0^2 + x_2^2 \geq 2; \\ 0 - \text{ в противном случае.} \end{cases}$$

Число элементов схемы $H(\odot_3)$ равно 9, сложность схемы по Квайну составляет $L(H(\odot_3)) = 32$, а число уровней и число внешних выводов равны $T(H(\odot_3)) = 2$ и $M(H(\odot_3)) = 10$.

Рассмотрим схему устройства $\odot_2$, реализующего операции $X_1^n + X_2^m = S \pmod{3}$ и $X_1^n - X_2^m = M \pmod{3}$ в унитарных кодах [42-A], которую обозначим $H(\odot_2, 3)$. Структура схемы будет состоять из «блоков» сложения, вычитания и возведения в степень, схемы которых обозначим $V_2(\odot_3)$, $M(\odot, 3)$ и $Q(\odot_3)$.

Схема $V_2(\odot, 3)$ представлена на рисунке 3.9 б), а схемы устройств $M(\odot, 3)$ и $Q(\odot, 3)$ – на рисунке 3.14 а) и б) соответственно.

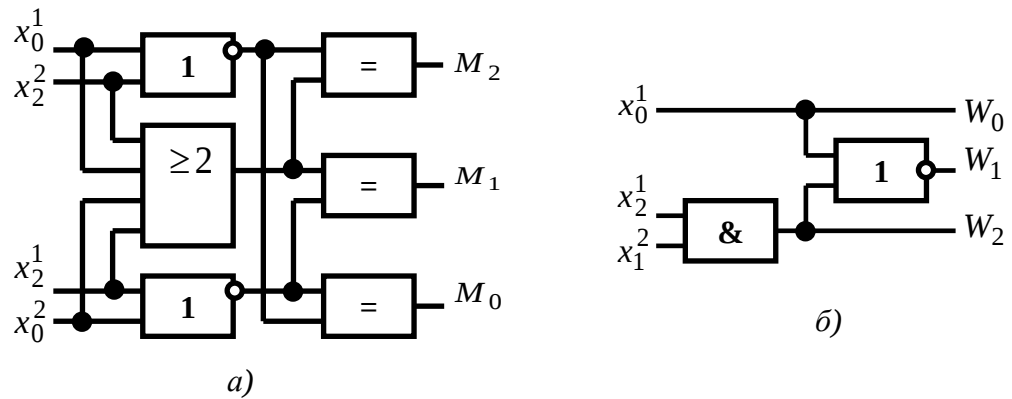


Рисунок 3.14 – Логические схемы
а) вычитателя $M(\odot, 3)$; б) устройства для возведения в степень $Q(\odot, 3)$

В результате составления «блоков» $Q(\odot, 3)$ с блоками $V_2(\odot, 3)$ и $M(\odot, 3)$ получим промежуточную логическую схему устройства $H^*(\odot, 3)$. Так как в схемах $V_2(\odot, 3)$ и $M(\odot, 3)$ отсутствуют входы, на которые подаются значения разрядов x_1^1 и x_1^2 , то из схемы $H^*(\odot, 3)$ можно удалить два элемента ИЛИ-НЕ, на выходах которых в схеме $Q(\odot, 3)$ реализуется функция W_1 . Полученная в результате таких преобразований схема $H(\odot, 3)$ представлена на рисунке 3.15.

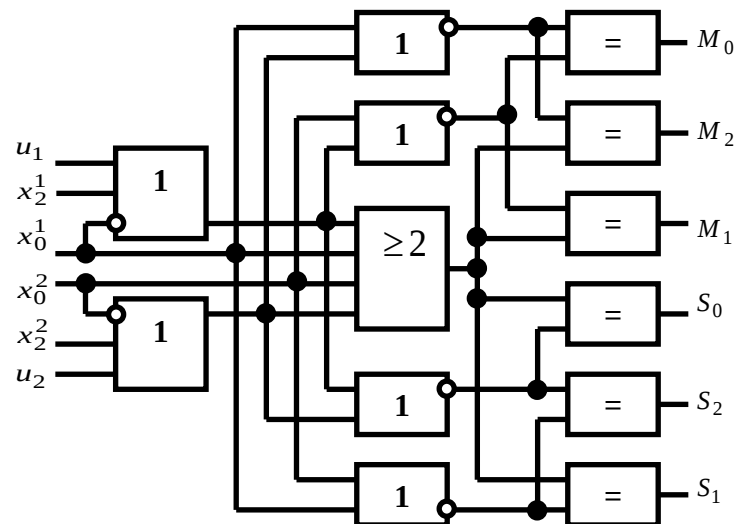


Рисунок 3.15 – Логическая схема $H(\odot, 3)$

Схема $H(\odot, 3)$ содержит два элемента ИЛИ, четыре элемента ИЛИ-НЕ, мажоритарный элемент с порогом два и шесть элементов РАВНОЗНАЧНОСТЬ.

На выходах $H(\odot, 3)$ формируются булевы функции $M_0, M_1, M_2, S_0, S_1, S_2$, принимающие значения разрядов $m_0, m_1, m_2, s_0, s_1, s_2$, где

$M = (m_0, m_1, m_2)$ и $S = (s_0, s_1, s_2)$. На выходе устройства $Q(\odot_{\mathbb{Z}_3}, 3)$ формируются булевы функции W_0, W_1, W_2 , принимающие значения разрядов w_0, w_1, w_2 , где $W = (w_0, w_1, w_2)$.

Устройство унитарных кодов по модулю три $H(\odot_{\mathbb{Z}_3}, 3)$ работает следующим образом. На его информационные входы поступают разряды «равно нулю» и «равно двум» первого $X_1 = (x_0^1, x_1^1, x_2^1)$ и второго $X_2 = (x_0^2, x_1^2, x_2^2)$ операндов. На управляющие входы подаются значения двоичных переменных u_1 и u_2 , где

$$u_1 = \begin{cases} 0, & \text{если } n - \text{четное;} \\ 1 - & \text{в противном случае} \end{cases} \quad \text{и} \quad u_2 = \begin{cases} 0, & \text{если } m - \text{четное;} \\ 1 - & \text{в противном случае} \end{cases}.$$

На выходах устройства формируется унитарный двоичный код результата выполнения операций $X_1^n - X_2^m = M \pmod{3}$ и $X_1^n + X_2^m = S \pmod{3}$, где $S = (s_0, s_1, s_2)$ и $M = (m_0, m_1, m_2)$.

Аналитические представления функций M_0, M_1, M_2 и S_0, S_1, S_2 , реализуемых на выходах вычислительного устройства $H(\odot_{\mathbb{Z}_3}, 3)$, имеют вид

$$\begin{aligned} M_0 &= \overline{g_1} \sim \overline{g_2}, & M_1 &= \overline{g_2} \sim K, & M_2 &= \overline{g_1} \sim K, \\ S_0 &= \overline{g_3} \sim K, & S_1 &= \overline{g_4} \sim K, & S_2 &= \overline{g_3} \sim \overline{g_4}, \end{aligned}$$

где " $\sim$ " – логическая операция «равнозначность» и

$$\begin{aligned} g_1 &= x_0^1 \vee h_2, & g_2 &= x_0^2 \vee h_1, & g_3 &= h_1 \vee h_2, & g_4 &= x_0^1 \vee x_0^2, \\ h_1 &= u_1 \overline{a_0} a_2, & h_2 &= u_2 \overline{b_0} b_2, \\ K &= \begin{cases} 1, & \text{если } x_0^1 + x_0^2 + h_1 + h_2 \geq 2; \\ 0 - & \text{в противном случае.} \end{cases} \end{aligned}$$

Число элементов схемы $H(\odot_{\mathbb{Z}_3}, 3)$ равно 13, сложность схемы по Квайну составляет $L(H(\odot_{\mathbb{Z}_3}, 3)) = 30$, а число уровней и число внешних выводов схемы равны $T(H(\odot_{\mathbb{Z}_3}, 3)) = 3$ и $M(H(\odot_{\mathbb{Z}_3}, 3)) = 12$.

Рассмотрим схемы устройств, реализующих операции $(X_1 \cdot X_2 \cdot \dots \cdot X_N)^m = F \pmod{3}$ и $X_1^{m_1} \cdot X_2^{m_2} \cdot \dots \cdot X_N^{m_N} = F \pmod{3}$ в унитарных кодах и обозначим их $H(\odot_3, 3)$ и $H(\odot_4, 3)$ соответственно. Структура обеих схем будет состоять из «блоков» умножения и возведения в степень, которые были приведены ранее $W_2(\odot_{\mathbb{Z}_3}, 3)$ и $Q(\odot_{\mathbb{Z}_3}, 3)$ (см. рисунки 3.10 б) и 3.14 б)).

На выходах $H(\odot_3, 3)$ и $H(\odot_4, 3)$ формируются булевы функции F_0, F_1, F_2 , принимающие значения разрядов f_0, f_1, f_2 , где $F = (f_0, f_1, f_2)$.

В результате объединения «блоков» $W_2(\odot_{\mathbb{Z}_3}, 3)$ и $Q(\odot_{\mathbb{Z}_3}, 3)$ получим промежуточную логическую схему устройства $H^*(\odot_3, 3)$. В результате объединения элементов И схем $W_2(\odot_{\mathbb{Z}_3}, 3)$ и $Q(\odot_{\mathbb{Z}_3}, 3)$ уменьшится число уровней

схемы $H^*(\odot_3, 3)$ за счет увеличения входов элемента И. Полученная в результате таких преобразований схема $H(\odot_3, 3)$ представлена на рисунке 3.16 [33-А].

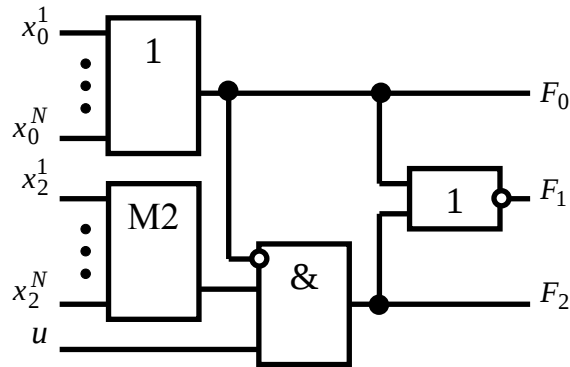


Рисунок 3.16 – Схема устройства $H(\odot_3, 3)$

Схема $H(\odot_3, 3)$ содержит элемент ИЛИ, элемент ИЛИ-НЕ, элемент СЛОЖЕНИЕ ПО МОДУЛЮ ДВА и элемент И. На входы устройства поступают значения разрядов $x_0^1, x_0^2, \dots, x_0^N$ и $x_2^1, x_2^2, \dots, x_2^N$ трехразрядных операндов $X_1 = (x_0^1, x_1^1, x_2^1)$, $X_2 = (x_0^2, x_1^2, x_2^2)$, ..., $X_N = (x_0^N, x_1^N, x_2^N)$ и управляющий вход u . На выходе устройства формируется результат выполнения операции $(X_1 \cdot X_2 \cdot \dots \cdot X_N)^m = F \pmod{3}$, где $F = (f_0, f_1, f_2)$.

Аналитические представления функций F_0, F_1, F_2 , реализуемых на выходах вычислительного устройства $H(\odot_3, 3)$, имеют вид

$$F_0 = x_0^1 \vee x_0^2 \vee \dots \vee x_0^N, \quad F_1 = \overline{F_0 \vee s_2}, \quad F_2 = \overline{F_0} g u,$$

где $g = x_2^1 \oplus x_2^2 \oplus \dots \oplus x_2^N$ и $u = \begin{cases} 0, & \text{если } m - \text{четное;} \\ 1 - & \text{в противном случае.} \end{cases}$

Число элементов схемы $H(\odot_3, 3)$ равно 4, сложность схемы по Квайну составляет $L(H(\odot_3, 3)) = 2N + 5$, а число уровней и число внешних выводов схемы равны $T(H(\odot_3, 3)) = 3$ и $M(H(\odot_3, 3)) = 2N + 4$.

В результате объединения «блоков» $Q(\odot_4, 3)$ и $W_2(\odot_3, 3)$ получим промежуточную логическую схему устройства $H^*(\odot_4, 3)$. Так как в схеме $W_2(\odot_3, 3)$ отсутствуют входы, на которые подаются значения разрядов $x_1^1, x_1^2, \dots, x_1^N$, то из схемы $H^*(\odot_4, 3)$ можно удалить N элементов ИЛИ-НЕ, на выходах которых в схеме $Q(\odot_4, 3)$ реализуется функция W_1 . Полученная в результате таких преобразований схема $H(\odot_4, 3)$ представлена на рисунке 3.17 [30-А].

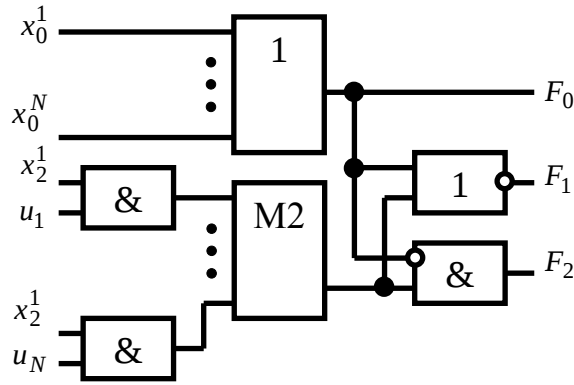


Рисунок 3.17 – Схема устройства $H(\odot_4, 3)$

Схема $H(\odot_4, 3)$ содержит $N + 1$ элементов И, элемент ИЛИ, элемент ИЛИ-НЕ и элемент СЛОЖЕНИЕ ПО МОДУЛЮ ДВА. На входы устройства поступают значения разрядов $x_0^1, x_0^2, \dots, x_0^N$ и $x_2^1, x_2^2, \dots, x_2^N$ трехразрядных операндов $X_1 = (x_0^1, x_1^1, x_2^1)$, $X_2 = (x_0^2, x_1^2, x_2^2)$, ..., $X_N = (x_0^N, x_1^N, x_2^N)$ и N управляющих входов $u_1, u_2, \dots, u_N$. На выходе устройства формируется результат выполнения операции $X_1^{m_1} \cdot X_2^{m_2} \cdot \dots \cdot X_N^{m_N} = F \pmod{3}$, где $F = (f_0, f_1, f_2)$.

Аналитические представления функций F_0, F_1, F_2 , реализуемых на выходах вычислительного устройства $H(\odot_4, 3)$, имеют вид

$$F_0 = x_0^1 \vee x_0^2 \vee \dots \vee x_0^N, \quad F_1 = \overline{F_0 \vee g}, \quad F_2 = \overline{F_0} g,$$

где $g = x_2^1 u_1 \oplus x_2^2 u_2 \oplus \dots \oplus x_2^N u_N$ и $u = \begin{cases} 0, & \text{если } N - \text{четное;} \\ 1 - & \text{в противном случае.} \end{cases}$

Число элементов схемы $H(\odot_4, 3)$ равно $N + 4$, сложность схемы по Квайну составляет $L(H(\odot_4, 3)) = 4N + 2$, а число уровней и число внешних выводов схемы равны $T(H(\odot_4, 3)) = 3$ и $M(F_4(\odot)) = 3N + 3$.

Рассмотрим схемы устройств, реализующих операции $X_1^n + X_2^m = F \pmod{3}$ и $(X_1 + X_2)^n = F \pmod{3}$ в позиционных кодах и обозначим их $H(\odot_5, 3)$ и $H(\odot_6, 3)$ соответственно. Структура обеих схем будет состоять из «блоков» возведения в степень $Q(\odot_{\blacksquare}, \odot_{\blacksquare})$ и сложения $V(\odot_{\blacksquare}, 3)$.

На выходах $H(\odot_5, 3)$ и $H(\odot_6, 3)$ формируются булевы функции F_1, F_2 , принимающие значения разрядов f_1, f_2 , где $F = (f_1, f_2)$.

Схема $H(\odot_5, 3)$ содержит два элемента И, мажоритарный элемент с порогом два, два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один и два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два. На входы устройства поступают значения разрядов x_1^1, x_2^1 и x_1^2, x_2^2 двухразрядных операндов $X_1 = (x_1^1, x_2^1)$, $X_2 = (x_1^2, x_2^2)$ и два управляющих входа u_1 и u_2 . На выходе устройства формируется двухразрядный результат выполнения операции

$X_1^n + X_2^m = F \pmod{3}$, где $F = (f_1, f_2)$. Схема $H(\odot_5, 3)$ приведена на рисунке 3.18.

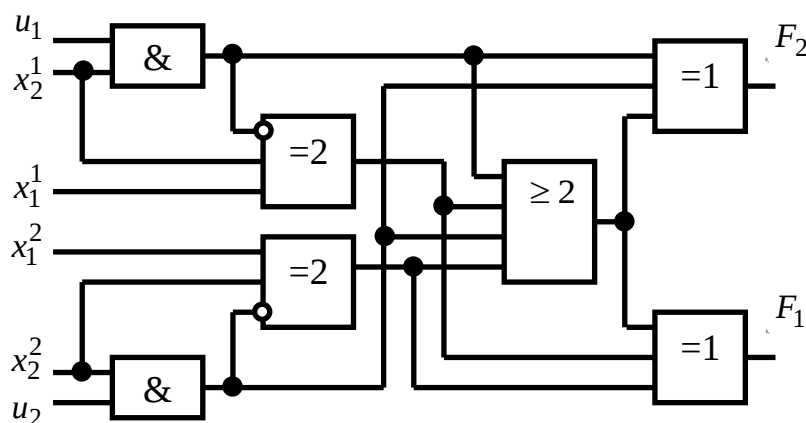


Рисунок 3.18 – Схема устройства $H(\odot_5, 3)$

Аналитические представления функций F_1, F_2 , реализуемых на выходах схемы устройства $H(\odot_5, 3)$ имеют вид

$$F_1 = \begin{cases} 1, & \text{если } g_1 + g_2 + h = 1; \\ 0 & - \text{в противном случае,} \end{cases} \quad F_2 = \begin{cases} 1, & \text{если } p_1 + p_2 + h = 1; \\ 0 & - \text{в противном случае,} \end{cases}$$

где

$$p_1 = x_2^1 \cdot u_1, \quad p_2 = x_2^2 \cdot u_2,$$

$$g_1 = \begin{cases} 1, & \text{если } x_1^1 + x_2^1 + \overline{p_1} = 2; \\ 0 & - \text{в противном случае,} \end{cases} \quad g_2 = \begin{cases} 1, & \text{если } x_1^2 + x_2^2 + \overline{p_2} = 2; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$h = \begin{cases} 1, & \text{если } p_1 + p_2 + g_1 + g_2 \geq 2; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$u_1 = \begin{cases} 0, & \text{если } n - \text{четное;} \\ 1 & - \text{в противном случае} \end{cases} \quad \text{и} \quad u_2 = \begin{cases} 0, & \text{если } m - \text{четное;} \\ 1 & - \text{в противном случае.} \end{cases}$$

Число элементов схемы $H(\odot_5, 3)$ равно 7, сложность схемы по Квайну составляет $L(H(\odot_5, 3)) = 20$, а число уровней и число внешних выводов равны $T(H(\odot_5, 3)) = 4$ и $M(H(\odot_5, 3)) = 8$.

Схема $H(\odot_6, 3)$ содержит два мажоритарных элемента с порогом два, два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ и элемент И. На входы устройства поступают значения разрядов x_1^1, x_2^1 и x_1^2, x_2^2 двухразрядных операндов $X_1 = (x_1^1, x_2^1)$, $X_2 = (x_1^2, x_2^2)$ и управляющий вход u . На выходе устройства формируется двухразрядный результат выполнения операции $(X_1 + X_2)^n = F \pmod{3}$, где $F = (f_1, f_2)$. Схема $H(\odot_6, 3)$ приведена на рисунке 3.19 [43-А].

Аналитические представления функций F_1, F_2 , реализуемых на выходах схемы устройства $H(\star_6, 3)$, имеют вид

$$F_1 = g u \quad \text{и} \quad F_2 = \begin{cases} 1, & \text{если } p + g + \overline{s_1} \geq 2; \\ 0 & - \text{в противном случае,} \end{cases}$$

где

$$p = \begin{cases} 1, & \text{если } x_1^1 + x_1^2 + h = 1; \\ 0 & - \text{в противном случае,} \end{cases} \quad g = \begin{cases} 1, & \text{если } x_2^1 + x_2^2 + h = 1; \\ 0 & - \text{в противном случае,} \end{cases}$$

$$h = \begin{cases} 1, & \text{если } x_{21}^1 + x_2^1 + x_1^2 + x_2^2 \geq 2; \\ 0 & - \text{в противном случае,} \end{cases} \quad \text{и} \quad u = \begin{cases} 0, & \text{если } n - \text{четное;} \\ 1 & - \text{в противном случае.} \end{cases}$$

Число элементов схемы $H(\star_6, 3)$ равно 5, сложность схемы по Квайну составляет $L(H(\star_6, 3)) = 15$, а число уровней и число внешних выводов равны $T(H(\star_6, 3)) = 4$ и $M(H(\star_6, 3)) = 7$.

Рассмотрим схему устройства $\star_7$, реализующего операции $X_1 \cdot X_2 = R \pmod{3}$ или $X_1 + X_2 = S \pmod{3}$ в позиционных кодах, которую обозначим $H(\star_7, 3)$.

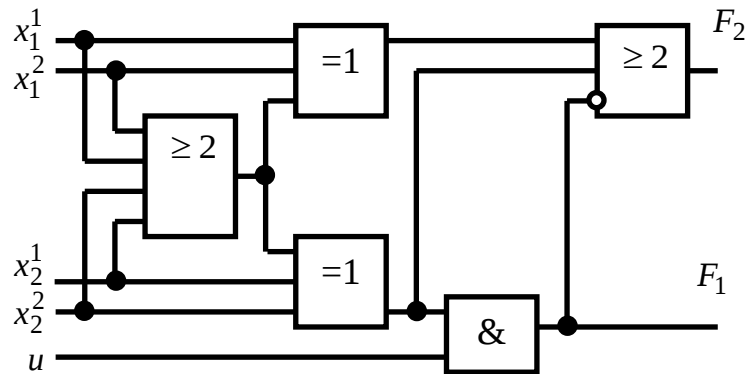


Рисунок 3.19 – Логическая схема устройства $H(\star_6, 3)$

На выходах $H(\star_7, 3)$ формируются булевы функции S_1, S_2 или R_1, R_2 , принимающие значения разрядов s_1, s_2 или r_1, r_2 , где $S = (s_1, s_2)$ или $R = (r_1, r_2)$.

Схема $H(\star_7, 3)$ содержит два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два и элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом три. На входы устройства поступают значения разрядов x_1^1, x_1^2 и x_2^1, x_2^2 двухразрядных операндов $X_1 = (x_1^1, x_1^2)$, $X_2 = (x_2^1, x_2^2)$ и управляющий вход u , определяющий тип выполняемой операции. На выходе устройства формируется двухразрядный результат выполнения операции $X_1 \cdot X_2 = R \pmod{3}$ или $X_1 + X_2 = S \pmod{3}$, где $S = (s_1, s_2)$ и $R = (r_1, r_2)$. Схема $H(\star_7, 3)$ приведена на рисунке 3.20.

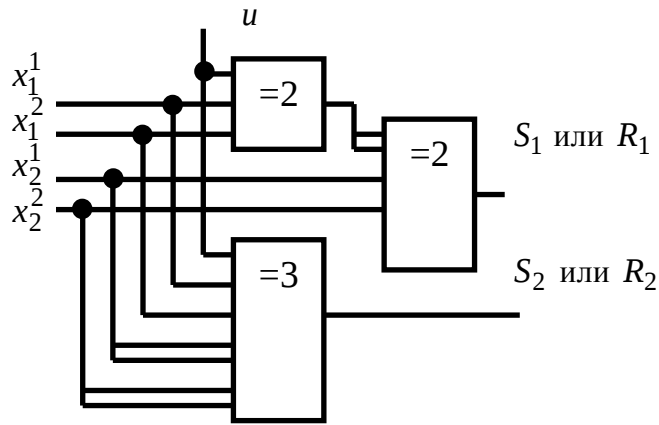


Рисунок 3.20 – Логическая схема устройства $H(\odot_7, 3)$

Аналитические представления функций, реализуемых на выходах схемы устройства $H(\odot_7, 3)$ в зависимости от значения управляющего сигнала u , имеют вид

$$p_1 = \begin{cases} 1, & \text{если } x_2^1 + x_2^2 + 2g = 2; \\ 0 & - \text{в противном случае,} \end{cases} \quad p_2 = \begin{cases} 1, & \text{если } u + x_1^1 + 2x_2^1 + x_1^2 + 2x_2^2 = 3; \\ 0 & - \text{в противном случае,} \end{cases}$$

где

$$g = \begin{cases} 1, & \text{если } u + x_1^1 + x_1^2 = 2; \\ 0 & - \text{в противном случае,} \end{cases} \quad p_1 = \begin{cases} R_1, & \text{если } u = 0; \\ S_1 & - \text{в противном случае,} \end{cases}$$

$$p_2 = \begin{cases} R_2, & \text{если } u = 0; \\ S_2 & - \text{в противном случае.} \end{cases}$$

Число элементов схемы $H(\odot_7, 3)$ равно 3, сложность схемы по Квайну составляет $L(H(\odot_7, 3)) = 15$, а число уровней и число внешних выводов схемы равны $T(H(\odot_7, 3)) = 2$ и $M(H(\odot_7, 3)) = 4$.

3.5 Выводы

1. Метод синтеза логических схем модулярных сумматоров (в позиционных и унитарных кодах) и модулярных умножителей (в унитарных кодах), основан на применении математического аппарата СБФ, является эффективным с точки зрения синтеза быстродействующих логических схем и ориентирован на схемную реализацию вычислительных устройств МА посредством современных САПР. Предложенный метод позволяет синтезировать логические схемы, превосходящие свои аналоги, синтезированные на основе известных методов.

2. Применение метода блочно-структурного синтеза устройств МА, в основе которого положено использование существующих (ранее

синтезированных) логических схем устройств, реализующих основные операции МА (таких, как сложение, умножение и возведение в степень) является эффективным средством синтеза логических схем устройств МА, имеющих небольшую конструктивную сложность (по Квайну) и высокое быстродействие.

3. Логические схемы а) модулярных сумматоров в позиционных кодах; б) модулярных сумматоров и умножителей в унитарных кодах; в) вычислительных устройств, реализующих суперпозицию основных модулярных операций; г) вычислительных устройств с управляющими входами, синтезированные на основе применения рассмотренных в этой главе методов, являются эффективными по сложности, по глубине и по числу внешних выводов, а их мировая новизна подтверждена 30 Патентами Республики Беларусь на изобретение в области автоматики и вычислительной техники [20-А-49-А].