УДК 681.04

В.А. КРАСНОБАЕВ, А.А. КУЗНЕЦОВ, С.А. КОШМАН, Е.А. КУЗНЕЦОВА

МЕТОД РЕАЛИЗАЦИИ ОПЕРАЦИИ СЛОЖЕНИЯ ДВУХ ОСТАТКОВ ЧИСЕЛ ПО МОДУЛЮ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Аннотация. Рассмотрен метод реализации арифметической операции сложения двух остатков чисел по модулю m_i в системе остаточных классов (СОК). Метод основан на использовании сумматоров по модулю $M = 2^n - 1$, состоящих из совокупности последовательных двоичных одноразрядных сумматоров, путем использования дополнительных связей. Сформулированы правила введения дополнительных связей, что дает возможность реализовать операцию сложения по произвольному модулю СОК. Рассмотрены примеры синтеза двоичных сумматоров и реализации операции сложения двух остатков чисел по модулю СОК.

Ключевые слова: компьютерная система, система остаточных классов, малоразрядный двоичный сумматор, позиционная система счисления, модульная операция сложения.

ВВЕДЕНИЕ

Реализация арифметической операции сложения двух чисел $A = (a_1 \,||\, a_2 || \ldots \ldots || \, a_i || \ldots || \, a_k)$ и $B = (b_1 \,||\, b_2 || \ldots || \, b_i || \ldots || \, b_k)$ в системе остаточных классов (СОК) осуществляется сложением соответствующих остатков a_i и b_i по основаниям (модулям) m_i $(i = \overline{1, k})$ независимо и параллельно во времени по каждому из k оснований СОК [1–3]. Малоразрядность остатков a_i и b_i в представлении слагаемых чисел в СОК дает возможность осуществить модульную операцию сложения $(a_i + b_i) \bmod m_i$ на основе использования малоразрядных двоичных сумматоров по модулю. Для упорядоченной $(m_i < m_{i+1})$ СОК выполнение операции сложения чисел определяется временем, необходимым для получения результата операции $(a_k + b_k) \bmod m_k$ по наибольшему m_k основанию СОК. Один из методов реализации модульной операции сложения $(a_i + b_i) \bmod m_i$ основывается на использовании двоичных сумматоров [4–6]. Данный подход предоставляет широкий выбор вариантов возможной реализации внутренней структуры такого сумматора. Это позволяет в полной мере использовать имеющийся практический опыт проектирования двоичных сумматоров [7–9].

СУММАТОРЫ ДВУХ ЧИСЕЛ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Одним из основных компонентов компьютерной системы (КС) является сумматор двух чисел. В частности, компонентами КС могут быть сумматоры двух чисел по модулю m_i. Данный тип сумматоров широко используется как в позиционных системах счисления (ПСС), так и в непозиционных системах счисления [10–12]. Такая задача является особенно важной для КС, функционирующей в СОК. Сумматор чисел $A = (a_1 \,||\, a_2 || \ldots || \, a_i || \ldots || \, a_k)$ и $B = (b_1 \,||\, b_2 || \ldots \ldots || \, b_i || \ldots || \, b_k)$ в СОК состоит из совокупности k n-разрядных сумматоров, $n = [\log_2 (m_i - 1) + 1]$, по модулю m_i. В этом аспекте актуальной научно-прикладной задачей является задача построения сумматоров, работающих по произвольному модулю m_i, выполненных на логических элементах с двумя устойчивыми состояниями. Если остатки a_i и b_i чисел $A = (a_1 \,||\, a_2 || \ldots \ldots || \, a_i || \ldots || \, a_k)$ и $B = (b_1 \,||\, b_2 || \ldots || \, b_i || \ldots || \, b_k)$ в СОК представлены в двоичной

ПСС, то сумматор двух остатков a_i и b_i по модулю m_i представляет последовательную совокупность из $n = [\log_2 (m_i - 1) + 1]$ двоичных одноразрядных сумматоров (ДОС), объединенных между собой связями подобно связям между позиционными двоичными сумматорами.

Известно, что двоичные сумматоры имеют фиксированную величину модуля, равную значению $M = 2^n - 1$. Данное обстоятельство исключает возможность их непосредственного использования для произвольного модуля m_i СОК. Если значение модуля M сумматора отличается от значения модуля m_i СОК на небольшую величину, то существует два варианта практической реализации операции сложения $((a_i + b_i) \bmod m_i)$ двух остатков a_i и b_i по модулю СОК [1]. При этом возможны следующие соотношения модулей:

1) имеет место соотношение модулей $M = m_i + 1$;

2) имеет место соотношение модулей $M = m_i - 1$.

Очевидно, что при рассмотренных вариантах соотношений между модулями m_i и M реализация операции сложения остатков $(a_i + b_i) \bmod m_i$ осуществляется довольно легко. Однако при существенном отличии значений модулей m_i и M операция модульного сложения $(a_i + b_i) \bmod m_i$ двух остатков является довольно сложной задачей. Это приводит к необходимости постановки и решению отдельной задачи синтеза сумматоров по произвольному модулю m_i СОК.

МЕТОД СИНТЕЗА СУММАТОРОВ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ СОК

Рассмотрим один из методов синтеза сумматоров по произвольному модулю m_i СОК, основанный на использовании структуры сумматора по модулю $M = 2^n - 1$, путем организации дополнительных связей $X_{\downarrow i \uparrow j}$ между *j*-м и *i*-м двоичными разрядами сумматора по модулю M. Сформулируем задачу синтеза сумматора двух остатков чисел по модулю m_i следующим образом.

Пусть задана произвольная исходная структура *n*-разрядного двоичного сумматора по модулю $M = 2^n - 1$ (рис. 1). Необходимо создать структуру сумматора для реализации операции сложения двух остатков чисел по произвольному модулю m_i СОК. Иными словами, необходимо посредством сумматора по модулю M обеспечить выполнение операции сложения по модулю m_i. Это достигается организацией и использованием дополнительных связей вида $X_{\downarrow i \uparrow j}$ в сумматоре по модулю $M = 2^n - 1$, где $X_{\downarrow i \uparrow j}$ обозначает связь между выходом *j*-го ДОС и входом *i*-го ДОС.

Для синтеза сумматора по модулю m_i СОК в структуре сумматора по модулю M необходимо между определенной парой ДОС исходного сумматора по модулю M сформировать дополнительные связи вида $X_{\downarrow i \uparrow j}$ таким образом, чтобы посредством сумматора по модулю M осуществлялась операция сложения двух остатков чисел по модулю m_i. Схема введения дополнительной связи $X_{\downarrow i \uparrow j}$ между выходом *j*-го ДОС и входом *i*-го ДОС представлена на рис. 2 ($j > i$).

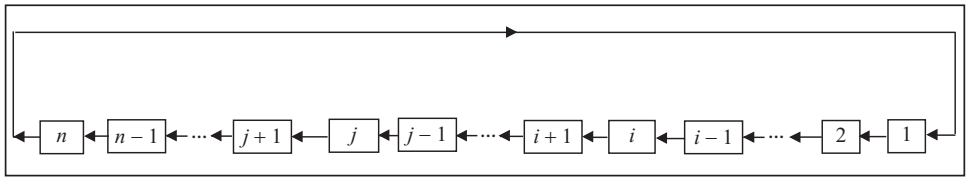

Рис. 1. Схема расположения и нумерация двоичных одноразрядных сумматоров в сумматоре по модулю $M = 2^n - 1$

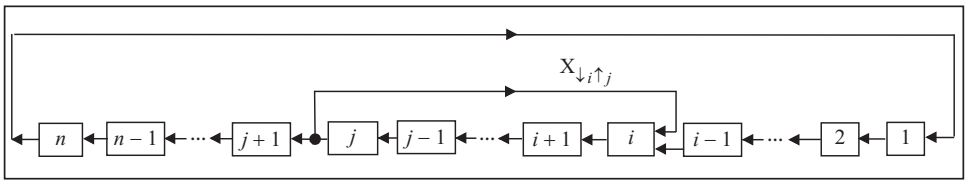

Рис. 2. Схема двоичного сумматора с дополнительной связью $X_{\downarrow i\uparrow j}$

Рассмотрим влияние дополнительной связи $X_{\downarrow i\uparrow j}$ на величину содержимого сумматора по модулю M.

АНАЛИЗ ВЛИЯНИЯ ДОПОЛНИТЕЛЬНЫХ СВЯЗЕЙ СУММАТОРА ПО МОДУЛЮ *M* НА ВЕЛИЧИНУ СОДЕРЖИМОГО СУММАТОРА

Рассмотрим влияние одной дополнительной связи $X_{\downarrow i\uparrow j}$, установленной между выходом *j*-го ДОС и входом *i*-го ДОС в сумматоре по модулю $M = 2^n - 1$ (см. рис. 2) на величину G_L исходного содержимого сумматора. Покажем, что число $L = \{l_i\}$, $i = \overline{1, n}$, являющееся содержимым величины G_L сумматора, при введении одной дополнительной связи $X_{\downarrow i\uparrow j}$ уменьшается на величину $\Delta G_L = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} 2^m \cdot l_m$ [1]. Отметим, что введение дополнительной связи $X_{\downarrow i\uparrow j}$ переводит исчисление чисел из двоичной системы счисления (СС), в которой работает сумматор по модулю M, в полиадическую СС с основаниями $\tau_1, \tau_2, \ldots, \tau_k$ с модулем $M = \tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_k - 1$. В этом случае содержимое числа $L = \{l_i\}$, $i = \overline{1, k}$, определяется следующим образом:

$$G_L = \sum_{m=1}^{k} l_m \cdot \prod_{i=1}^{m-1} \tau_i = l_1 \cdot \tau_2 \cdot \tau_3 \cdot \ldots \cdot \tau_k + l_2 \cdot \tau_3 \cdot \tau_4 \cdot \ldots \cdot \tau_k + \ldots$$

$$\ldots + l_{k-2} \cdot \tau_{k-1} \cdot \tau_k + l_{k-1} \cdot \tau_k + l_k . \qquad (1)$$

Соотношение (1) можно представить в виде

$$G_L = l_1 \cdot \prod_{i=2}^{k} \tau_i + l_2 \cdot \prod_{i=3}^{k} \tau_i + \ldots + l_{k-2} \cdot \prod_{i=k-1}^{k} \tau_i + l_{k-1} \cdot \prod_{i=k}^{k} \tau_i + l_k . \qquad (2)$$

В двоичной СС ($\tau_1 = \tau_2 = \ldots = \tau_k = 2$) выражение (2) примет следующий вид:

$$G_L = \sum_{m=1}^{k} l_m \cdot 2^{k-m} = l_1 \cdot 2^{k-1} + l_2 \cdot 2^{k-2} + \ldots + l_{k-1} \cdot 2 + l_k .$$

В случае отсутствия в сумматоре дополнительных связей $X_{\downarrow i\uparrow j}$ величина G_L содержимого сумматора определяется как

$$G_L = \sum_{m=1}^{n} l_m \cdot q_m ,$$

где величина l_m в *m*-м разряде содержимого сумматора может принимать одно из двух значений: $l_m = 0$ или $l_m = 1$, а значение q_m является весом *m*-го разряда содержимого сумматора, который определяется местоположением двоичного разряда сумматора (см. рис 1).

При дополнительной связи $X_{\downarrow i\uparrow j}$, объединяющей ДОС с номерами от *i* до *j* в единый (обобщенный) разряд сумматора по модулю

$$\tau_{ij} = 2^{j-(i-1)} - 1 = 2^{j-i+1} - 1, \qquad (3)$$

вес q_m каждого разряда сумматора с номерами от $(i-1)$-го до первого (младшего разряда сумматора) определяется как $q_m = 2^{m-1}$ $(m = \overline{1, i-1})$ (рис. 3).

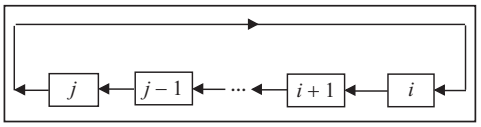

Рис. 3. Схема обобщенного $(j-i+1)$-го разряда сумматора по модулю τ_{ij}

Исходя из структуры сумматора по модулю с дополнительной связью (рис. 4) вес разрядов сумматора с номерами от $(j+1)$-го до n-го (старшего разряда сумматора) определяется выражением

$$q_m = 2^{i-1} \cdot \tau_{ij} \cdot 2^{m-j-1}. \tag{4}$$

С учетом соотношения (3) выражение (4) можно представить в виде

$$q_m = 2^{m+i-j-2} \cdot \tau_{ij} = 2^{m+i-j-2} \cdot (2^{j-i+1} - 1) = 2^{m-1} - 2^{m+i-j-2}. \tag{5}$$

Выражение (5) для любого разряда сумматора можно представить следующим образом:

$$q_m = 2^{m-1} - 2^{m+i-j-2} \cdot \Delta_{mj}, \tag{6}$$

где число Δ_{mj} может принимать два значения:

$$\Delta_{mj} = \begin{cases} 1, & \text{если } m > j, \\ 0, & \text{если } m \le j. \end{cases}$$

Согласно (6) величина G_L равна следующей разности:

$$G_L = \sum_{m=1}^{n} l_m \cdot 2^{m-1} - \sum_{m=j+1}^{n} l_m \cdot 2^{m+i-j-2}. \tag{7}$$

Из соотношения (7) очевидно, что введение в сумматор одной дополнительной связи вида $X_{\downarrow i \uparrow j}$ уменьшает его содержимое G_L на величину, равную значению

$$\Delta G_L = \sum_{m=j+1}^{n} l_m \cdot 2^{m+i-j-2} = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} l_m \cdot 2^m.$$

Таким образом, при введении одной дополнительной связи $X_{\downarrow i \uparrow j}$ исходное содержимое сумматора по модулю M уменьшается на величину ΔG_L:

$$\Delta G_L = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} l_m \cdot 2^m.$$

Следует особо отметить, что при введенной дополнительной связи вида $X_{\downarrow i \uparrow j}$ значение величины модуля $M = 2^n - 1$ исходного сумматора уменьшается на величину

$$\Delta M = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} S_m \cdot 2^m,$$

где S_m — значение m-го разряда числа, содержащегося в сумматоре [1]. При этом, естественно, диапазон представимых чисел по модулю M уменьшается

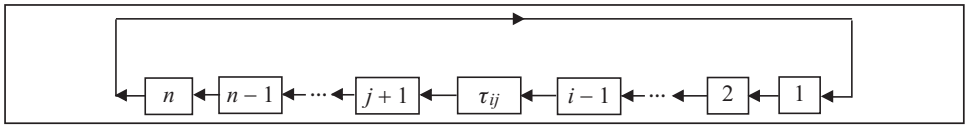

Рис. 4. Эквивалентная схема сумматора по модулю с дополнительной связью $X_{\downarrow i \uparrow j}$

на величину ΔM. В результате появляется возможность за счет введения в сумматор по модулю M определенных дополнительных связей (или одной дополнительной связи) уменьшить величину M модуля до необходимого значения модуля m_i СОК. В этом случае выполняется следующее условие:

$$M = m_i. \tag{8}$$

МЕТОД СИНТЕЗА СУММАТОРОВ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ m_i СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

В общем виде в представлении модуля m_i содержимое двоичных разрядов имеет вид

$$m_i = S_n \cdot 2^{n-1} + S_{n-1} \cdot 2^{n-2} + \ldots + S_2 \cdot 2 + S_1.$$

Исходное содержимое сумматора по модулю $M = 2^n - 1$ имеет вид

$$G_L = l_n \cdot 2^{n-1} + l_{n-1} \cdot 2^{n-2} + \ldots + l_2 \cdot 2 + l_1.$$

Для выполнения условия (8) в сумматор по модулю $M = 2^n - 1$ вводят дополнительные связи $\mathrm{X}_{\downarrow i \uparrow j}$. В этом случае *i*-й ДОС примет значение $l_i + c_{i-1} + x_{ij}$, где l_i — содержимое *i*-го ДОС исходного состояния сумматора по модулю M; c_{i-1} — значение сигнала переноса содержимого $(i-1)$-го ДОС в *i*-й ДОС; x_{ij} — значение l_j содержимого *j*-го ДОС сумматора; S_i — значение содержимого *i*-го двоичного разряда модуля m_i СОК. При этом выполняется следующее тождество:

$$l_i + c_{i-1} + x_{ij} + S_i = l_i. \tag{9}$$

С учетом одного из свойств модуля сумматора (модуль сумматора является его вторым нулем) выражение (9) принимает вид

$$c_{i-1} + x_{ij} + S_i = 0, \tag{10}$$

что для двоичного представления чисел равнозначно следующему соотношению:

$$S_i = c_{i-1} + x_{ij}. \tag{11}$$

Исходя из результата анализа выражений (10) и (11), можно сделать следующие выводы относительно влияния дополнительных связей $\mathrm{X}_{\downarrow i \uparrow j}$ на сумматор по модулю $M = 2^n - 1$, а также сформировать правила организации дополнительных связей.

1. Влияние дополнительных связей $\mathrm{X}_{\downarrow i \uparrow j}$ на уменьшение величины модуля $M = 2^n - 1$ сумматора для значения ΔM не зависит от исходного содержимого G_L сумматора.

2. В *n*-разрядном сумматоре, работающем по модулю $M = 2^n - 1$, дополнительная связь $\mathrm{X}_{\downarrow i \uparrow j}$ может иметь место лишь в *i*-х двоичных разрядах S_i $(i = \overline{2, n})$, соответствующих нулевым значениям двоичной кодовой комбинации модуля m_i. Это обусловлено тем, что наличие сигнала $x_{ij} = 1$ обеспечивает условие выполнения равенства (11).

3. В двоичных разрядах S_i сумматора, соответствующих единичным значениям, дополнительные связи $\mathrm{X}_{\downarrow i \uparrow j}$ должны отсутствовать, т.е. необходимо, чтобы $x_{ij} = 0$ (см. (11)).

Суть метода синтеза сумматоров по модулю m_i СОК состоит в следующем. В исходном сумматоре по модулю $M = 2^n - 1$ на основании определенных, приведенных выше правил формируются дополнительные связи сумматора. Использование дополнительных связей позволит реализовать исходный сумматор для выполнения операции сложения вычетов чисел по модулю m_i СОК, так как вве-

дение дополнительных связей $X_{\downarrow i \uparrow j}$ изменяет веса отдельных разрядов сумматора и уменьшает величину модуля от M до m_i.

Метод синтеза сумматора по модулю m_i СОК состоит из совокупности следующих операций.

1. Представление структуры сумматора по модулю $M = 2^n - 1$, где $n = [\log_2 (m_i - 1)] + 1$, и определение разрядности n (количество ДОС) сумматора по модулю m_i.

2. Определение двоичных разрядов S_i сумматора, для которых выполняется условие $S_i = 0$. Процесс определения условия $S_i = 0$ проводится, исходя из представления модуля числа m_i в двоичном коде.

3. Введение дополнительной связи сумматора, которое начинается с выхода n-го (старшего) ДОС ($j = n$). Это обеспечивает минимальное значение величины $\Delta G_L = 0$ коррекции.

4. Введение дополнительной связи, поступающей на вход ДОС, для которого $S_i = 0$ (см. п. 2 метода синтеза).

Фактически почти для каждого основания m_i СОК может быть синтезировано одновременно несколько видов сумматоров. В этом случае возникает необходимость выбора «наилучшего» сумматора по модулю m_i из возможных вариантов. Выбор сумматора часто проводится по следующим двум критериям:

— с учетом несложной организации дополнительных связей $X_{\downarrow i \uparrow j}$ сумматора;

— исходя из минимального значения величины ΔG_L коррекции модуля $M = 2^n - 1$.

ПРИМЕРЫ СИНТЕЗА СУММАТОРОВ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ m_i

В соответствии с описанным методом синтеза рассмотрим примеры синтеза сумматоров по модулю m_i СОК.

Пример 1. Пусть $m_i = 53$.

1. Определим количество n ДОС в сумматоре по модулю $M = 2^n - 1$. Для модуля $m_i = 53$ имеем $n = [\log_2 (m_i - 1)] + 1 = [\log_2 (53 - 1)] + 1 = 6$. Структура сумматора по модулю $M = 2^n - 1 = 63$ приведена на рис. 5.

Исходная структура сумматора по модулю $m_i = 53$ без дополнительных связей $X_{\downarrow i \uparrow j}$ будет иметь тот же вид.

2. Модуль $m_i = 53$ в двоичном коде $S_6 S_5 S_4 S_3 S_2 S_1$ представляется в виде 110101, т.е. $S_6 = 1$, $S_5 = 1$, $S_4 = 0$, $S_3 = 1$, $S_2 = 0$ и $S_1 = 1$. Для представленного в двоичном коде модуля $m_i = 53$ имеем $S_2 = S_4 = 0$.

3. На основании полученных результатов структура сумматора по модулю $m_i = 53$ приведена на рис. 6.

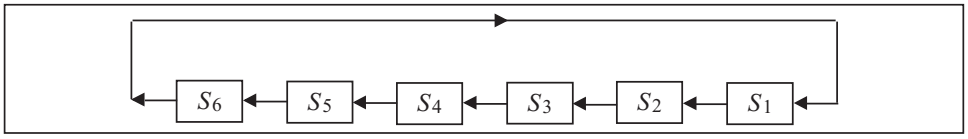

Рис. 5. Исходная структура сумматора по модулю $M = 2^6 - 1$

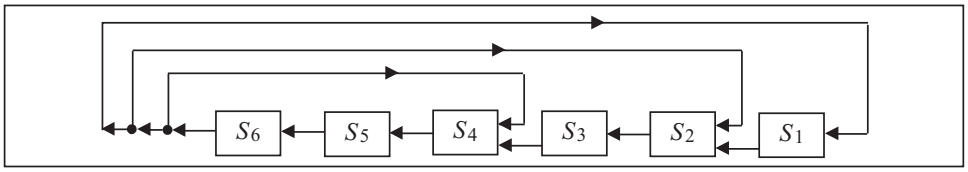

Рис. 6. Структура сумматора по модулю $m_i = 53$

В соответствии с методом синтеза в сумматор по модулю $M = 2^6 - 1$ введены две дополнительные связи: $X_{\downarrow 4 \uparrow 6}$ и $X_{\downarrow 2 \uparrow 6}$. В целях проверки правильности синтеза сумматора по модулю $m_i = 53$ определим для данной структуры сумматора значение модуля $M = m_i$ СОК. На основании рис. 6 составим ряд структур отдельных частей сумматора по модулю $m_i = 53$.

Для первой части структуры сумматора модуль M_1 определится следующим образом: $M_1 = \tau_6 \cdot \tau_5 \cdot \tau_4 - 1$.

Для этой части структуры модуль M_2 определится выражением $M_2 = M_1 \cdot \tau_3 \cdot \tau_2 - 1 = (\tau_6 \cdot \tau_5 \cdot \tau_4 - 1) \cdot \tau_3 \cdot \tau_2 - 1$.

Для сумматора по модулю значение модуля $M = m_i$ СОК определится следующим образом (см. рис. 6):

$$m_i = M_2 \cdot \tau_1 - 1 = [(\tau_6 \cdot \tau_5 \cdot \tau_4 - 1) \cdot \tau_3 \cdot \tau_2 - 1] \cdot \tau_1 - 1 = [(2^3 - 1) \cdot 2^2 - 1] \cdot 2 - 1 = 53.$$

На основании проведенных расчетов можно сделать вывод, что синтез сумматора по модулю $m_i = 53$ (см. рис. 6) выполнен правильно.

Пример 2. Пусть $m_i = 37$. Покажем следующие этапы синтеза сумматора по модулю СОК.

1. В соответствии с величиной $m_i = 37$ модуля определим количество n двоичных разрядов (количество ДОС) сумматора по модулю. Для модуля $m_i = 37$ имеем $n = [\log_2 (37 - 1)] + 1 = 6$. При этом структура сумматора по модулю $M = 2^n - 1 = 63$ имеет такой же вид, как на рис. 5.

2. Для реализации процесса синтеза структуры сумматора по модулю $M = 63$ (см. рис. 5) введем дополнительные связи $X_{\downarrow i \uparrow j}$. Предварительно определим двоичные разряды S_i сумматора, в записи модуля m_i которых в двоичном коде содержатся нули, т.е. $S_i = 0$. Так как модуль $m_i = 37$ в двоичном коде имеет вид 100101, то нулевыми двоичными разрядами сумматора будут $S_2 = 0$, $S_4 = 0$ и $S_5 = 0$.

3. На основании полученных в п. 2 результатов описания метода синтеза сумматора по модулю m_i введем в сумматор по модулю $M = 2^n - 1$ (см. рис. 5) три дополнительные связи: $X_{\downarrow 5 \uparrow 6}$, $X_{\downarrow 4 \uparrow 6}$ и $X_{\downarrow 2 \uparrow 6}$. Структура сумматора по модулю $m_i = 37$ приведена на рис. 7. Для данной структуры определим значение модуля $M = m_i$ СОК. Для этого предварительно составим ряд структур отдельных частей сумматора, представленного на рис. 7.

Для первой части структуры сумматора $M_1 = \tau_6 \cdot \tau_5 - 1$.

Для второй части структуры сумматора $M_2 = M_1 \cdot \tau_4 - 1 = (\tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1$.

Для третьей части структуры сумматора $M_3 = M_2 \cdot \tau_3 \cdot \tau_2 - 1 = [(\tau_6 \cdot \tau_5 - 1) \times \times \tau_4 - 1] \cdot \tau_3 \cdot \tau_2 - 1$.

Значение модуля $M = m_i$ СОК определится следующим образом:

$$m_i = M_3 \cdot \tau_1 - 1 = \{[(\tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1] \cdot \tau_3 \cdot \tau_2 - 1\} \cdot \tau_1 - 1 =$$
$$= \{[(2 \cdot 2 - 1) \cdot 2 - 1] \cdot 2 \cdot 2 - 1\} \cdot 2 - 1 = 37.$$

Следовательно, синтез сумматора по модулю $m_i = 37$ выполнен правильно.

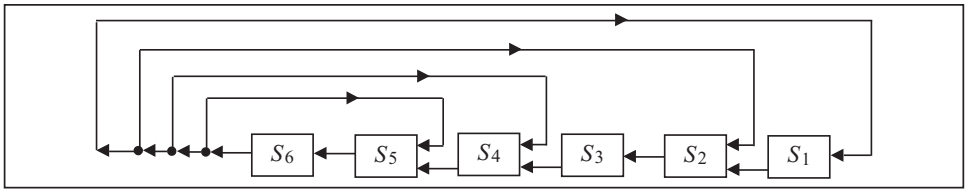

Рис. 7. Структура сумматора по модулю $m_i = 37$

Пример 3. Пусть $m_i = 11$. Покажем следующие этапы синтеза сумматора по модулю $m_i = 11$ СОК.

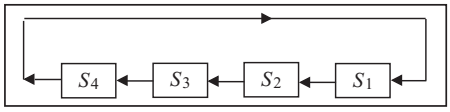

Рис. 8. Исходная структура сумматора по модулю $M = 2^n - 1$

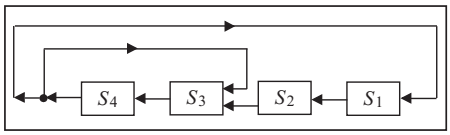

Рис. 9. Структура сумматора по модулю $m_i = 11$

1. Определим количество n ДОС. Для модуля $m_i = 11$ имеем $n = [\log_2 (11-1)] + 1 = 4$. Структура сумматора по модулю $M = 2^n - 1 = 15$ приведена на рис. 8.

2. Для синтеза сумматора по модулю $m_i = 11$ СОК предварительно определим значения двоичных разрядов S_i сумматора, в записи модуля $m_i = 11$ которых содержатся нули, т.е. для случая $S_i = 0$. Таким разрядом будет третий, т.е. $S_3 = 0$, так как в двоичном коде модуль $m_i = 11$ имеет вид 1011.

3. Исходя из того, что $S_3 = 0$, дополнительная связь в сумматоре имеет вид $X_{\downarrow 3 \uparrow 4}$. При этом $\Delta G_L = 0$. Структура сумматора по модулю $m_i = 11$ представлена на рис. 9.

Для структуры сумматора, представленной на рис. 9, определим значения модуля $M = m_i$ СОК. Предварительно рассмотрим часть структуры такого сумматора. Для этой части модуль $M_1 = \tau_4 \cdot \tau_3 - 1$. Значение модуля $M = m_i$ СОК сумматора (см. рис. 9) определится следующим образом: $m_i = M_1 \cdot \tau_2 \cdot \tau_1 - 1 = (\tau_4 \cdot \tau_3 - 1) \cdot \tau_2 \cdot \tau_1 - 1 = (2 \cdot 2 - 1) \cdot 2 \cdot 2 - 1 = 11$.

Следовательно, синтез сумматора по модулю $m_i = 11$ выполнен правильно.

Примеры синтеза сумматоров по модулю m_i СОК подтверждают возможность практического использования предложенного метода синтеза сумматора по модулю СОК.

ПРИМЕРЫ РЕАЛИЗАЦИИ ОПЕРАЦИИ СЛОЖЕНИЯ ДВУХ ОСТАТКОВ ЧИСЕЛ ПО МОДУЛЮ m_i СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

На основании изложенного метод реализации операции сложения $(a_i + b_i) \bmod m_i$ двух остатков a_i и b_i чисел в СОК включает использование совокупности следующих операций.

1. Синтез сумматора по модулю m_i СОК.

2. Получение в двоичном коде результата $S_n S_{n-1} \ldots S_2 S_1$ суммирования двух остатков a_i и b_i чисел по модулю два.

3. Занесение содержимого двоичных разрядов полученной модульной суммы $S_n S_{n-1} \ldots S_2 S_1$ в соответствующие ДОС структуры сумматора по модулю m_i СОК.

4. На основании синтезированной структуры сумматора по модулю СОК реализуется алгоритм сложения двух остатков a_i и b_i чисел в СОК.

Рассмотренный метод имеет ограничение на применение его для сложения двух остатков чисел по модулю m_i СОК в случае их равенства, т.е. когда $a_i = b_i$.

Представим примеры реализации операции сложения двух остатков чисел по модулю m_i СОК.

Пример 4. Рассмотрим возможность реализации модульной операции $(a_i + b_i) \bmod 37$ для значения остатков $a_i = 35 = 100011$ и $b_i = 24 = 011000$. Используем структуру сумматора по модулю $m_i = 37$ (см. рис. 7) и алгоритм модульного сложения, представленный в [1]. Поразрядная сумма остатков $a_i = 100011$ и $b_i = 011000$ будет иметь вид $a_i \oplus b_i = 100011 \oplus 011000 = 111011$. Полученное значение $S_6 S_5 S_4 S_3 S_2 S_1 = 111011$ суммы заносим в соответствующие ДОС сумматора по модулю $m_i = 37$. В соответствии со схемой сложения по

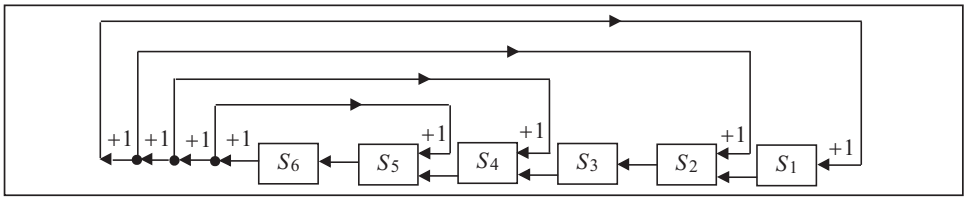

Рис. 10. Схема сложения остатков чисел по модулю $m_i = 37$

Таблица 1. Алгоритм реализации операции модульного сложения остатков $a_i = 100011$ и $b_i = 011000$

Номер ДОС S_i	Исходное состояние ДОС S_i	Значение сигналов входов ДОС S_i	Результат операции ДОС S_i
S_1	1	+1	0
S_2	1	+1+1	1
S_3	0	+1	1
S_4	1	+1	0
S_5	1	+1+1	1
S_6	1	+1	0

модулю $m_i = 37$ (рис. 10) представим алгоритм сложения двух остатков $a_i = 100011$ и $b_i = 011000$ (табл. 1). В результате проведения этой операции получим $S_6S_5S_4S_3S_2S_1 = 010110$.

Проверка: $(35+24) = 22 \bmod 37$.

Пример 5. Рассмотрим процедуру реализации операции модульного сложения двух остатков a_i и b_i чисел $(a_i + b_i) \bmod m_i$ для примера 3 (см. рис. 9) синтеза сумматора по модулю $m_i = 11$.

Пусть $a_i = 1010$ и $b_i = 0101$. Тогда поразрядная сумма остатков a_i и b_i по модулю два равна значению $a_i \oplus b_i = 1010 \oplus 0101 = 1111$. В соответствии со структурой сумматора по модулю 11 (см. рис. 9) его содержимое равно 1111. Схема сложения приведена на рис. 11. Здесь $S_1 = 1$, $S_2 = 1$, $S_3 = 1$ и $S_4 = 1$. На основании введенной дополнительной связи $X_{\downarrow 3 \uparrow 4}$ и содержимого 1111 сумматора в табл. 2 приведен алгоритм сложения двух остатков $a_i = 1010$ и $b_i = 0101$ чисел по модулю 11.

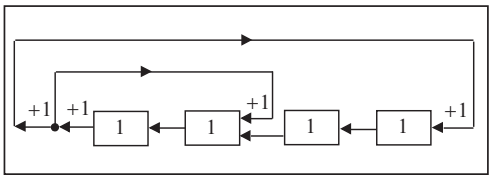

Рис. 11. Схема сложения двух остатков по модулю $m_i = 11$

В итоге проведения операции модульного сложения получим результат в виде $S_4S_3S_2S_1 = 0100$.

Проверка: $(10+5) = 4 \bmod 11$.

Таблица 2. Алгоритм реализации операции модульного сложения остатков $a_i = 1010$ и $b_i = 0101$

Номер ДОС S_i	Исходное состояние ДОС S_i	Значение сигналов входов ДОС S_i	Результат операции ДОС S_i
S_1	1	+1	0
S_2	1	+1	0
S_3	1	+1+1	1
S_4	1	+1	0

ЗАКЛЮЧЕНИЕ

В настоящей статье рассмотрен метод реализации операции сложения двух остатков a_i и b_i чисел $A=(a_1,a_2,...,a_i,...,a_k)$ и $B=(b_1,b_2,...,b_i,...,b_k)$, представленных в СОК. Метод основан на использовании сумматоров по модулю $M=2^n-1$, состоящих из совокупности последовательных двоичных одноразрядных сумматоров, путем введения и использования дополнительных связей. Сформулированы правила введения дополнительных связей, что позволяет из сумматора по модулю $M=2^n-1$ создать сумматор, реализующий операцию сложения двух остатков a_i и b_i по модулю m_i. Сформулирована и решена задача синтеза двоичных сумматоров по произвольному модулю m_i СОК. Рассмотрены примеры синтеза двоичных сумматоров и реализации операции сложения двух остатков чисел по модулю m_i.

СПИСОК ЛИТЕРАТУРЫ

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. Москва: Сов. радио, 1968. 440 с.
2. Спеціалізовані комп'ютерні технології в інформатиці. Під заг. ред. Я.М. Николайчука. Тернопіль: ТзОВ «Терно-граф», 2017. 913 с.
3. Корнилов А.И., Семенов М.Ю., Калашников В.С. Методы аппаратной оптимизации сумматоров для двух операндов в системе остаточных классов. *Изв. вузов. Электроника.* 2004. № 1. С. 75–82.
4. Bayoumi M.A., Jullien G.A., Miller W.C. A VLSI implementation of residue. *Adders IEEE Trans. on Circuits and Systems*. 1987. Vol. 34, N 3. P. 284–288.
5. Корнилов А.И., Исаева Т.Ю., Семенов М.Ю. Методы логического синтеза сумматоров с ускоренным переносом по модулю (2*n* – 1) на основе BDD-технологии. *Изв. вузов. Электроника*. 2004. № 3. С. 54-60.
6. Долгов А.И. Диагностика устройств, функционирующих в системе остаточных классов. Москва: Радио и связь, 1982. 64 с.
7. Safari A., Nugent J., Kong Y. Novel implementation of full adder based scaling in residue number systems. *2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*. 4–7 Aug. 2013. Columbus, OH, 2013. P. 657–660. doi: 10.1109/MWSCAS.2013.6674734.
8. Shugang Wei. Fast signed-digit arithmetic circuits for residue number systems. *IEEE International Conference on Electronics, Circuits, and Systems (ICECS*). 6–9 Dec. 2015. P. 344–347.
9. Ananda Mohan P.V. Residue number systems: Theory and applications. Birkhäuser; Basel: Springer International Publishing, Switzerland, 2016. 351 p.
10. Балака Е.С., Тельпухов Д.В., Осинин И.П., Городецкий Д.А. Сравнительное исследование и анализ методов аппаратной реализации сумматоров по модулю. *Universum: технические науки.* 2016. № 1 (23). URL: https://cyberleninka.ru/article/n/sravnitelnoe-issledovanie-i-analiz-metodov-apparatnoy-realizatsii-summatorov-po-modulyu.
11. Gorbenko I., Hanzia R. Examination and implementation of the fast method for computing the order of elliptic curve. *European Journal of Enterprise Technologies*. 2017. Vol. 2, N 9 (86). P. 11–21.
12. Krasnobayev V.A., Koshman S.A. Method for implementing the arithmetic operation of addition in residue number system based on the use of the principle of circular shift. *Cybernetics and Systems Analysis*. 2019. Vol. 55, N 4. P. 692–698. https://doi.org/10.1007/s10559-019-00179-8.

Надійшла до редакції 10.09.2019

В.А. Краснобаєв, О.О. Кузнецов, С.О. Кошман, К.О. Кузнецова

МЕТОД РЕАЛІЗАЦІЇ ОПЕРАЦІЇ ДОДАВАННЯ ДВОХ ЗАЛИШКІВ ЧИСЕЛ ЗА МОДУЛЕМ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Анотація. Розглянуто метод реалізації арифметичної операції додавання двох залишків чисел за модулем m_i у системі залишкових класів (СЗК). Метод базується на використанні суматорів за модулем $M = 2^n - 1$, що складаються з сукупності послідовних двійкових однорозрядних суматорів, шляхом використання додаткових зв'язків. Сформульовано правила введення додаткових зв'язків, що дає можливість реалізувати операцію додавання за довільним модулем СЗК. Розглянуто приклади синтезу двійкових суматорів та реалізації операції додавання двох залишків чисел за модулем СЗК.

Ключові слова: комп'ютерна система, система залишкових класів, малорозрядний двійковий суматор, позиційна система числення, модульна операція додавання.

V.A. Krasnobayev, A.A. Kuznetsov, S.A. Koshman, K.O. Kuznetsova

A METHOD FOR IMPLEMENTING THE OPERATION OF MODULO ADDITION OF TWO NUMBERS RESIDUES OF THE RESIDUAL NUMBER SYSTEM

Abstract. The paper describes a method for implementing the arithmetic operation of modulo m_i addition of the residues of two numbers in the residual number system (RNS). The method is based on the use of modulo $M = 2^n - 1$ adders, which consist of a set of sequential binary single-digit adders, by introducing and using additional feedbacks. The authors formulate the rules for introducing additional feedbacks, which makes it possible to implement the addition operation for an arbitrary modulo of RNS. Examples of the synthesis of binary adders and examples of the operation of RNS modulo addition of two numbers residues are given.

Keywords: computer system, residual number system, small-bit binary adder, positional number system, modular addition operation.

Краснобаев Виктор Анатольевич,
доктор техн. наук, профессор, профессор кафедры Харьковского национального университета им В.Н. Каразина, e-mail: v.a.krasnobaev@gmail.com.

Кузнецов Александр Александрович,
доктор техн. наук, профессор, профессор кафедры Харьковского национального университета им. В.Н. Каразина, e-mail: kuznetsov@karazin.ua.

Кошман Сергей Александрович,
кандидат техн. наук, доцент, доцент кафедры Харьковского национального университета им. В.Н. Каразина, e-mail: s_koshman@ukr.net.

Кузнецова Екатерина Александровна,
студентка Харьковского национального университета им. В.Н. Каразина, e-mail: kate7smith12@gmail.com.