Лебедев Борис Константинович – Южный федеральный университет; e-mail: lebedev.b.k@gmail.com; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89282897933; кафедра систем автоматизированного проектирования; профессор.

Лебедев Владимир Борисович – Таганрогский политехнический институт Донского государственного технического университета; e-mail: lebvlad@rambler.ru; 347920, г. Таганрог, ул. Петровская, 109 а; тел.: 88634623538; декан высшего профессионального образования; доцент.

Lebedev Boris Konstantinovich – Southern Federal University; e-mail: lebedev.b.k@gmail.com; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: 89282897933; the department of computer aided design; professor.

Lebedev Vladimir Borisovich – Taganrog Polytechnic Institute Don State Technical University; e-mail: lebvlad@rambler.ru; 109 a, Petrovskaya street, Taganrog, 347920, Russia; phone: +78634623538; dean of Higher Professional Education; associate professor.

УДК 004.272.2

Е.С. Балака, А.Н. Щелоков

СОВЕРШЕНСТВОВАНИЕ СТРУКТУРЫ ВЫЧИСЛИТЕЛЬНЫХ КАНАЛОВ МОДУЛЯРНОГО УСТРОЙСТВА ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ ВЫЧИСЛЕНИЙ

Возможность повышения надежности цифровых устройств путем применения кодов, способных обнаруживать и исправлять возникающие в процессе вычислений ошибки, является альтернативой мажоритарным методам резервирования, обладающим характерной для них высокой избыточностью. Наилучшим базисом для построения таких кодов может служить модулярная арифметика. Корректирующие возможности модулярных кодов известны давно. Однако на практике, широкого применения они не получили. В первую очередь, это связано с аппаратными расходами на реализацию алгоритмов кодирования и декодирования (немодульные операции), которые носят последовательно-параллельный характер. Встает актуальная задача сокращения аппаратных затрат на реализацию немодульных операций. В данной работе предлагается принципиально новый подход к построению вычислительных каналов модулярного устройства, основанный на бимодульной арифметике, обладающей внутренней избыточностью в представлении операндов. Предложенный авторами способ однотипного кодирования компонент представления вычетов позволил свести вычисления от модуля p к модулю (p–1). Тем самым стало возможным реализовать параллельную структуру модульного канала и организовать контроль вычислений по каждому модулю p модулярного устройства. Результаты экспериментов показали, что разработанный комплекс методов по повышению защиты модулярного устройства от сбоев позволяет сократить аппаратные затраты по сравнению с резервированием – затраты на контрольное оборудование составили 40 % относительно незащищенной схемы, при потере производительности на 7 %.

Корректирующие коды модулярной арифметики; бимодульная арифметика; архитектурная сбоеустойчивость.

E.S. Balaka, A.N. Schelokov

IMPROVING THE STRUCTURE OF COMPUTATION CHANNELS RNS-BASED DEVICE FOR ENHANCING THE RELIABILITY OF THE CALCULATION

Opportunity to improve the reliability of digital devices through the use of codes that can detect and correct calculations involved in making mistakes is an alternative to the majority of redundancy having their characteristic high redundancy. Best basis for constructing such codes

can serve as modular arithmetic. Corrective opportunities modular codes are known. However, in practice, they have a wide application not received. Primarily, this is due to the hardware costs of implementing the encoding and decoding algorithms (non-modular), which are series-parallel in nature. Thus, the actual problem arises of reducing the hardware costs of the non-modular operations. In this paper, we propose a fundamentally new approach to the construction of computing channels modular device based on the bimodular arithmetic with internal redundancy in the representation of the operands. The proposed method have the same type of encoding components of the representation deductions allowed to reduce the computation of the module p to module (p-1). Thus, it was possible to realize the parallel structure of the modular channel and organize the control calculations for each mod p modular device. The experimental results showed that the developed set of methods to improve the protection of the modular unit from failure reduces hardware costs compared to redundant - the cost of monitoring equipment amounted to 40 % compared to an unprotected circuit, the loss of productivity by 7 %.

Redundant RNS codes; bimodular arithmetic; architectural failure protection.

Введение. Надежность изделий вычислительной техники является одним из важнейших компонентов их качества. В особенности это относится к специализированным вычислительным системам с высокой степенью распараллеливания вычислений, предназначенных для решения сложных и ответственных задач, отказы которых связаны с возможностью аварий и крупных материальных потерь. В связи с этим задачи сбое- и отказоустойчивого проектирования специализированных вычислительных систем играют все большую роль, являясь неотъемлемой частью общего процесса проектирования вычислительной системы на всех его этапах.

С ростом степени распараллеливания вычислительного процесса, растет и объем используемой контрольной аппаратуры, необходимой для требуемого уровня сбоеустойчивости; усложняется устройство управления вычислительной системой, требуются дополнительные аппаратные и временные затраты на обеспечение его бесперебойной работы; вычислительная система разрастается, при этом частота сбоев в схемах увеличивается; резко возрастает потребляемая мощность. Возникает *противоречие*: с одной стороны, постоянный рост требований к производительности вычислительных устройств приводит к необходимости организации параллельных вычислений, с другой – при глубоком уровне распараллеливания увеличивается частота сбоев и отказов, что приводит к увеличению времени простоя спецустройства, вызванное трудностью поиска и устранения неисправности, что негативно влияет на общий объем используемой контрольной аппаратуры и соответственно на потребляемую мощность системы в целом.

Одним из перспективных направлений разрешения данного противоречия является придание устройствам свойств устойчивости к сбоям в процессе вычислений, с возможностью минимизации используемой аппаратуры за счет совершенствования архитектуры устройства [1].

Способы обнаружения и исправления одиночных сбоев в работе исполнительных устройств рассматриваются с позиций построения архитектуры вычислительного устройства (архитектурная сбоеустойчивость) [2]. Подходы к архитектурной сбоеустойчивости известны и определяются применением следующих основных методов: структурная, временная, программная, информационная избыточности [3].

Для обнаружения и исправления одиночных сбоев в работе исполнительных устройств используются корректирующие коды, сохраняющие свои свойства при выполнении арифметических операций [4]. Наиболее широкими возможностями обладают модулярные коды, при использовании которых не только контрольная часть, но и информационная часть представляются остатками по модулям принятой модулярной системы счисления [5, 6].

Практически любая вычислительная система на основе модулярной арифметики может быть представлена согласно общей структуре устройства (рис. 1) [7].

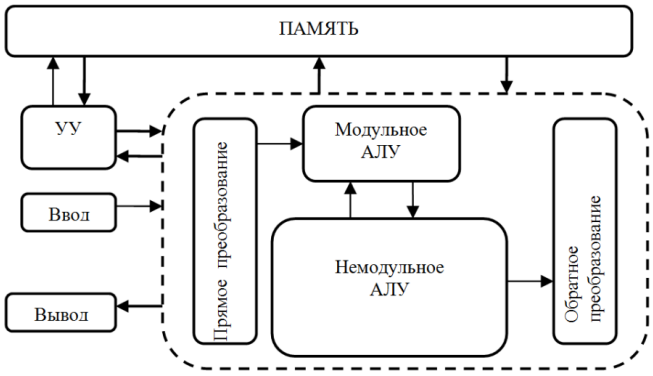


Рис. 1. Блок-схема вычислительной системы на основе модулярной арифметики

Арифметическое устройство модулярной вычислительной системы разбивается на отдельные компоненты «модульное АЛУ» и «немодульное АЛУ». Блок модульного АЛУ отвечает за выполнение всего набора кольцевых операций модулярной арифметики, т.е. за выполнение параллельных операций. Тогда как блок немодульного АЛУ отвечает за выполнение последовательно-параллельных процедур модулярной арифметики. К классу немодульных процедур относят: кодирование/декодирование, сравнение чисел по величине, определение знака числа, округление, определение признака переполнения за диапазон, а также процедуры самокоррекции. Перечисленные операции являются важнейшими для машинной арифметики. Однако устройства, реализующие этот ряд немодульных процедур, являются медленными и громоздкими по аппаратным затратам.

Для обнаружения и исправления одиночных сбоев в работе модульного АЛУ используются корректирующие коды модулярной арифметики (избыточные коды). Для того чтобы выяснить, является ли некоторое слово, полученное в результате вычислений, верным, необходимо определить величину соответствующего числа, т.е. осуществить немодульную процедуру – непосредственный перевод числа, представленного остатками, в позиционную систему счисления.

Таким образом, надежность модульного АЛУ напрямую зависит от надежности громоздкого по аппаратным затратам немодульного АЛУ. Громоздкость немодульного АЛУ в сравнении с модульным АЛУ оценивается в единицах аппаратных затрат на модульное АЛУ величиной большей, чем $\frac{n(n-1)}{2}$ единиц затрат на одно модульное АЛУ [8]. Кроме того, немодульное АЛУ дополнительно утяжеляется за счет реализации процедур самокоррекции. Использование аппаратных методов защиты от сбоев самого немодульного блока приведет к еще большему росту занимаемой площади, увеличению потребляемой мощности, уменьшению быстродействия схемы, и увеличению частоты сбоев в схеме, что может свести на нет саму целесообразность использования модулярной арифметики.

Бимодульная арифметика конечного поля GF(p). Решение задач оптимизации вычислительного процесса модулярной арифметики привело к развитию нескольких способов представления элементов конечного поля GF(p): традиционно-индексный [9]; логарифмический [10]; бимодульный [11]; рекурсивный [12]. Каждый из представленных способов обладает индивидуальными особенностями и своей областью применения. Как показали результаты исследований [13], бимодульная арифметика открывает новые возможности в области построения сбое- и отказоустойчивых модулярных вычислительных систем.

Бимодульная арифметика впервые была рассмотрена профессором Д.А. Поспеловым в работе [14]. Им было предложено кодировать элементы конечного поля парами $\left\langle |x|_p, ind_w|x|_p \right\rangle$, где $|x|_p$ есть вычет x по mod p, $i = ind_w|x|_p$ – соответствующий вычету $|x|_p$ индекс, при этом условно считается, что вычету 0 соответствует специальный символ λ, который обладает свойством $\lambda + i = i + \lambda = \lambda$ для любого индекса $0 \le i \le p-2$.

Таким образом, операции сложения и умножения сводятся к операциям сложения по модулю p и модулю $p-1$ соответственно и одной табличной операции выбора второй компаненты пары результата (рис. 2).

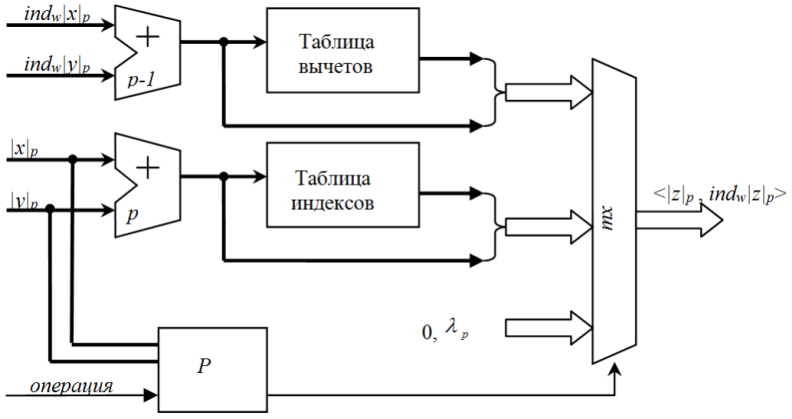


Рис. 2. Структура вычислительного канала бимодульной арифметики

Однако, несмотря на достоинство однотипного выполнения кольцевых операций, с позиций повышения надежности данный способ кодирования обладает существенным недостатком – использованием модульных сумматоров двух типов по модулям p и $(p-1)$.

Преодоление данного недостатка достигается введением требования однотипности кодового представления обеих компонент пар каждого операнда. В связи с этим вводится понятие модифицированного вычета по модулю p:

$$|\tilde{x}|_p = \lambda_p \delta\left((p-1) - |x|_p\right) + \left||x|_p\right|_{p-1} \hat{\delta}\left((p-1) - |x|_p\right),$$

где $\delta(u) = \begin{cases} 1, & u = 0, \\ 0, & \text{иначе}, \end{cases}$ – функция Кронекера, $\hat{\delta}(u) = 1 - \delta(u)$ – кофункция Кронекера.

То есть, в случае, когда x принимает значения от 0 до $p-2$ включительно (регулярный случай), то его вычет $|x|_p$ кодируется вычетами по модулю $p-1$; в случае, если $x=p-1$, то вычету $|x|_p$ ставится в соответствие технически легко распознаваемый символ сингулярности λ_p, числовое представление которого отлично от регулярных случаев.

Для представления второй компоненты пары операнда, вместо индекса, используется дискретно-логарифметическое представление. Отличие состоит в том, что индексная арифметика определена на множестве отличных от нуля точек поля GF(p). Исскуственно доопределяя значение дискретного логарифма в точке 0, переходим к вычислениям в логарифметике поля GF(p) [15].

Мультипликативные операции в этом случае выполняются согласно выражению: если $<|\tilde{x}|_p, \log_w|\tilde{x}|_p>$, $<|\tilde{y}|_p, \log_w|\tilde{y}|_p>$, то

$$(x\cdot y) \bmod p \longrightarrow <\log^{-1}\left(\left|\log_w|\tilde{x}|_p + \log_w|\tilde{y}|_p\right|_{p-1}\right), \left|\log_w|\tilde{x}|_p + \log_w|\tilde{y}|_p\right|_{p-1}>,$$

т.е.

$$(x\cdot y) \bmod p = \begin{cases} \lambda_p, \textit{если } \delta\left(\log_w|\tilde{x}|_p - \lambda_p\right) \vee \delta\left(\log_w|\tilde{y}|_p - \lambda_p\right) = 1, \\ \left|\left|\log_w|\tilde{x}|_p + \log_w|\tilde{y}|_p\right|_{p-1}\right|_{p-1}. \end{cases}$$

Логика выполнения аддитивных операций усложнится за счет введения дополнительных логических функций, связанных с переходом к однородному представлению: если $<|\tilde{x}|_p, \log_w|\tilde{x}|_p>$, $<|\tilde{y}|_p, \log_w|\tilde{y}|_p>$, то

$$(x+y) \bmod p \longrightarrow <|\tilde{x}+\tilde{y}|_{p-1}, \log_w(|\tilde{x}+\tilde{y}|_{p-1})),$$

т.е.

$$(x+y) \bmod p = \begin{cases} p-2, \ \textit{если} \ \ \tilde{x}=\tilde{y}=p-1, \\ \lambda_p, \ \textit{если} \ \ \tilde{x}+\tilde{y}=p-1, \\ \tilde{x}-1, \textit{если} \ \ \tilde{x}\neq 0 \ \textit{и} \ \tilde{y}=\lambda_p, \\ \tilde{y}-1, \textit{если} \ \ \tilde{y}\neq 0 \ \textit{и} \ \tilde{x}=\lambda_p \\ \tilde{x}+\tilde{y}, \ \textit{если} \ \ \tilde{x}+\tilde{y}<p-1, \\ |\tilde{x}+\tilde{y}|_{p-1}-1, \ \textit{если} \ \ \tilde{x}+\tilde{y}>p-1. \end{cases}$$

Как было показано в работе [13], бимодульный вычислительный канал является более экономичным с точки зрения апаратных затрат относительно аналогов, использующих другие способы представления элементов конечного поля GF(p). В работе [17] был произведен анализ структурных методов для повышения надежности вычислительных каналов. Однако, переход к вычислениям по модулю (*p–1*) позволяет распараллелить структуру внутри каждого вычислительного канала за счет разбиения на субмодули [18], а также использовать избыточные модулярные коды для обнаружения и исправления сбоев, не обращаясь к немодульному блоку АЛУ.

Способ построения защищенного вычислительного канала на основе бимодульной арифметики. Избыточная система модулей имеет n – рабочих и k – контрольных оснований [15]. Под одиночной ошибкой понимается любое искажение символа, относящегося к какому-либо одному модулю.

Рассмотрим набор субмодулей бимодульного вычислительного канала $q_1, q_2, \ldots, q_s, q_{s+1}$, $Q = \prod_{i=1}^{s+1} q_i$ – рабочий диапазон. Известно, что для обнаружения и коррекции одиночной ошибки достаточно использовать два избыточных оснований q_{s+2}, q_{s+3} [7]. Для обнаружения и исправления одиночной ошибки в данной работе используется метод вычисления невязок по контрольным основаниям системы [19].

Суть метода заключается в следующем. Пусть в результате вычислений получено число $A' = \left(|A'|_{q_1}, |A'|_{q_2}, \ldots, |A'|_{q_s}, |A'|_{q_{s+1}}, |A'|_{q_{s+2}}, |A'|_{q_{s+3}}\right)$. Для определения правильности числа A' необходимо по известным остаткам $|A'|_{q_1}, |A'|_{q_2}, \ldots, |A'|_{q_s}, |A'|_{q_{s+1}}$

определить значения его остатков по контрольным основаниям $\left|A''\right|_{q_{s+2}}, \left|A''\right|_{q_{s+3}}$. Затем необходимо сравнить значения $\left|A'\right|_{q_{s+2}}, \left|A'\right|_{q_{s+3}}$ с $\left|A''\right|_{q_{s+2}}, \left|A''\right|_{q_{s+3}}$. Сравнение остатков по контрольным основаниям можно осуществить их вычитанием:

$$\gamma_{s+2} = \left|\left|A''\right|_{q_{s+2}} - \left|A'\right|_{q_{s+2}}\right|_{q_{s+2}}, \ \gamma_{s+3} = \left|\left|A''\right|_{q_{s+3}} - \left|A'\right|_{q_{s+3}}\right|_{q_{s+3}}.$$

Числа γ_{s+2}, γ_{s+3} называются невязками. Согласно КТО:

$$A' = \sum_{\substack{k=1 \\ k\neq i}}^{n} \alpha_k B_k + \tilde{\alpha}_i B_i - r_{A'} \cdot Q, \ A = \sum_{\substack{k=1 \\ k\neq i}}^{n} \alpha_k B_k + \alpha_i B_i - r_A \cdot Q,$$

где $r_{A'}, r_A$ – ранги чисел A и A' соответственно, B_k $\left(k = \overline{1,n}\right)$ – ортогональные базисы, которые определяются по формуле $B_k = \frac{m_k Q}{q_k} = m_k Q_k$, где $Q_k = \frac{Q}{q_k}$, m_k – целые положительные числа, которые называются весами базиса, их определяют из сравнений $Q_k m_k \equiv 1 \left(\mathrm{mod}\ q_k\right)$.

Тогда $A' - A = \left(\tilde{\alpha}_i - \alpha_i\right) B_i - r_{A'-A} \cdot Q = \Delta_i B_i - r_{A'-A} \cdot Q$. При этом

$$\Delta_i B_i = \Delta_i Q_i m_i = \left(\Delta_i m_i\right) \cdot Q_i = \left(\left|\Delta_i m_i\right|_{q_i} + \left\lfloor \frac{\Delta_i m_i}{q_i} \right\rfloor \cdot q_i\right) \cdot Q_i = \left|\Delta_i m_i\right|_{q_i} \cdot Q_i + \left\lfloor \frac{\Delta_i m_i}{q_i} \right\rfloor \cdot Q.$$

Отсюда, ранг искаженного числа равен: $rang\ \Delta_i B_i = \left\lfloor \frac{\Delta_i m_i}{q_i} \right\rfloor \cdot Q$. Таким образом,

$$\gamma_{s+2} = \left|\left|\Delta_i m_i\right|_{q_i} \cdot Q_i\right|_{q_{s+2}}, \quad \left|\Delta_i m_i\right|_{q_i} = \left|\gamma_{s+2} \cdot Q_i^{-1}\right|_{q_{s+2}},$$

$$\gamma_{s+3} = \left|\left|\Delta_i m_i\right|_{q_i} \cdot Q_i\right|_{q_{s+3}}, \quad \left|\Delta_i m_i\right|_{q_i} = \left|\gamma_{s+3} \cdot Q_i^{-1}\right|_{q_{s+3}}.$$

То есть ошибка обнаружена, если

$$\left|\gamma_{s+2} \cdot Q_i^{-1}\right|_{q_{s+2}} = \left|\gamma_{s+3} \cdot Q_i^{-1}\right|_{q_{s+3}} = \delta_i. \qquad (1)$$

Величина ошибки определяется согласно выражению $\Delta_i = \left|\delta_i \cdot Q_i\right|_{q_i}$.

В предположении, что в полученном числе A' оказался искаженным не более чем один остаток, можно сформулировать следующие свойства невязок:

1. Если значение всех невязок равны нулю: $\gamma_{s+2} = \gamma_{s+3} = 0$, то ошибки не возникло, число A' является правильным.
2. Если одина из невязок равна нулю, а другая не равна, то ошибка произошла по контрольному основанию, где невязка отлична от нуля, при этом число A' является правильным.
3. Если значения невязок $\gamma_{s+2} \neq \gamma_{s+3} \neq 0$, то ошибка произошла по рабочему основанию.

Для демонстрации данного механизма обнаружения и исправления ошибок, рассмотрим пример для p=7 в случае возникновения одиночной ошибки по рабочему субмодульному основанию.

Имеем набор субмодулей: $q_1=2$, $q_2=3$, $q_3=5$, для которого рабочий диапазон есть P=2×3×5=30. Введем контрольные основания $q_4=7$, $q_5=11$. Пусть в результате вычислений получено число A = 5 = (1, 2, 0) $\in$(0,P), вычет по контрольным субмодулям равены (5, 5). Внесем ошибку в один рабочий канал, в результате принято число A' = (1, 2, 1, 5, 5).

Запишем набор констант, необходимых для перевода в полиадический код:

$$\left|q_1^{-1}\right|_{q_2}=\left|2^{-1}\right|_3=2,$$

$$\left|q_1^{-1}\right|_{q_3}=\left|2^{-1}\right|_5=3, \qquad \left|q_2^{-1}\right|_{q_3}=\left|3^{-1}\right|_5=2,$$

$$\left|q_1^{-1}\right|_{q_4}=\left|2^{-1}\right|_7=4, \qquad \left|q_2^{-1}\right|_{q_4}=\left|3^{-1}\right|_7=5, \qquad \left|q_3^{-1}\right|_{q_4}=\left|5^{-1}\right|_7=3,$$

$$\left|q_1^{-1}\right|_{q_5}=\left|2^{-1}\right|_{11}=6, \qquad \left|q_2^{-1}\right|_{q_5}=\left|3^{-1}\right|_{11}=4, \qquad \left|q_3^{-1}\right|_{q_5}=\left|5^{-1}\right|_{11}=9.$$

Расширяясь на контрольные субмодули, получим: $\left|A''\right|_{q_4}=4, \left|A''\right|_{q_5}=0.$ Вычислим невязки:

$$\gamma_{s+2}=\left|\left|A''\right|_{q_{s+2}}-\left|A'\right|_{q_{s+2}}\right|_{q_{s+2}}=\left|4-5\right|_7=6,$$

$$\gamma_{s+3}=\left|\left|A''\right|_{q_{s+3}}-\left|A'\right|_{q_{s+3}}\right|_{q_{s+3}}=\left|0-5\right|_{11}=6.$$

Определим при каком i выполняется (1):

$$P_1=\frac{P}{q_1}=\frac{30}{2}=15$$

$i=1$ $\quad \left|\Delta_1\mu_n\right|_{q_1}=\left|\gamma_{s+2}\cdot P_1^{-1}\right|_{q_{s+2}}=\left|6\cdot 15^{-1}\right|_7=6, \qquad 6\neq 7$

$$\left|\Delta_1\mu_n\right|_{q_1}=\left|\gamma_{s+3}\cdot P_1^{-1}\right|_{q_{s+3}}=\left|6\cdot 15^{-1}\right|_{11}=7,$$

$$P_2=\frac{P}{q_2}=\frac{30}{3}=10$$

$i=2$ $\quad \left|\Delta_2\mu_n\right|_{q_2}=\left|\gamma_{s+2}\cdot P_1^{-1}\right|_{q_{s+2}}=\left|6\cdot 10^{-1}\right|_7=2, \qquad 2\neq 5$

$$\left|\Delta_2\mu_n\right|_{q_2}=\left|\gamma_{s+3}\cdot P_1^{-1}\right|_{q_{s+3}}=\left|6\cdot 10^{-1}\right|_{11}=5,$$

$$P_3=\frac{P}{q_3}=\frac{30}{5}=6$$

$i=3$ $\quad \left|\Delta_3\mu_n\right|_{p_1}=\left|\gamma_{s+2}\cdot P_1^{-1}\right|_{q_{s+2}}=\left|6\cdot 6^{-1}\right|_7=1, \qquad \mathbf{1=1}$

$$\left|\Delta_3\mu_n\right|_{p_1}=\left|\gamma_{s+3}\cdot P_1^{-1}\right|_{q_{s+3}}=\left|6\cdot 6^{-1}\right|_{11}=1,$$

Следовательно, ошибка произошла по субмодульному каналу q_3, при этом величина ошибки равна: $\Delta_3=\left|r_3\cdot P_3\right|_{q_3}=\left|1\cdot 6\right|_5=1.$

Для уменьшения сложности реализации алгоритма обнаружения и исправления ошибки, а также для уменьшения временных затрат, целесообразно при проектировании использовать табличный подход: входами в таблицу являются вычисленные значения невязок, а выходами – номер неисправного субмодульного канала и вели-

чина ошибки. Поскольку таблица перекодировок строится внутри вычислительного канала, то такой метод построения блока коррекции вполне приемлем как с точки зрения быстродействия, так и аппаратных затрат. В этом случае количество возможных вхождений в таблицу будет определяться согласно тождеству [20]:

$$TableSize = 2\sum_{i=1}^{p}(p_i - 1) + (p_{s+2} - 1) + (p_{s+3} - 1) + 1.$$

На рис. 3 представлена структурная схема блока локализации и исправления единичного сбоя в вычислительном канале.

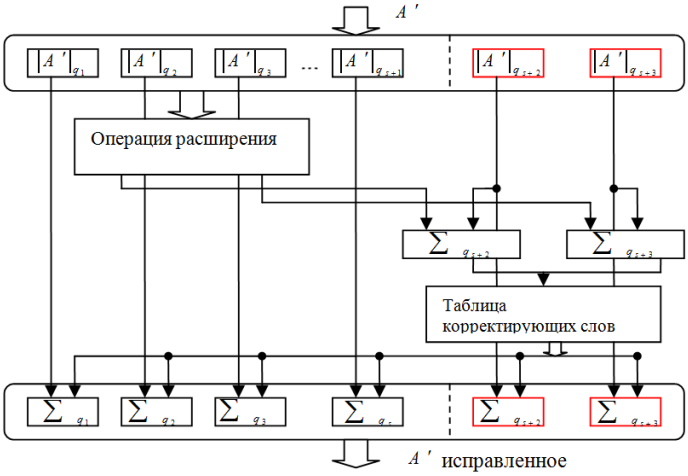
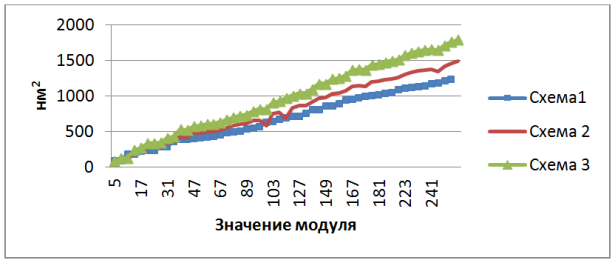


Рис. 3. Структура блока локализации и исправления одиночной ошибки в вычислительном канале

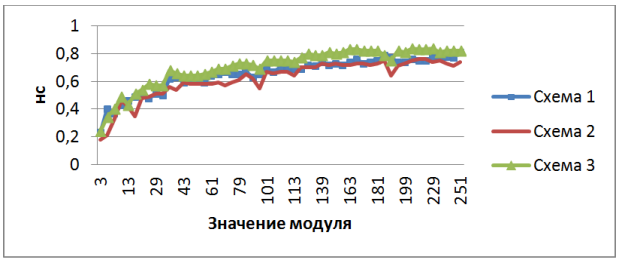
Результаты моделирования. Сравнительная характеристика методов коррекции ошибок основывается на надежности обнаружения сбоев, возможности исправления ошибок после сбоев, площади, занимаемой дополнительной аппаратурой, влиянии конрольной аппаратуры на быстродействие устройства. Таким образом, эффективность предложенного способа построения вычислительных каналов модулярного устройства была рассмотрена с этих позиций.

Для проведения экспериментов выбран маршрут проектирования цифровых ИС на основе библиотек стандартных ячеек. В маршруте используется: поведенческое описание устройств на языке Verilog HDL; средства логического синтеза Synopsys Design Compiler; библиотека стандартных ячеек Nangate Open Cell Library с проектными нормами 45 нм; среда для симуляции и отладки проектов ModelSim. Модель эксперимента построена для обнаружения и исправления одиночного сбоя в схеме. Эксперименты проводились для диапазаона простых модулей битностью до 8 бит, что является достаточным для большинства задач из области применения модулярной арифметики. Для сравнительного анализа реализованы модели вычислительных каналов с возможностью обнаружения и исправления одиночной ошибки и без, а также модель из работы [16].

На рис. 4 представлены результаты моделирования вычислительных каналов с использованием стандартных методов проектирования модульных сумматоров (Схема 1), с использованием субмодульного разложения модуля (p–1) (Схема 2), с использованием субмодульного разложения модуля (p–1) и схемой обнаружения и исправления одиночной ошибки (Схема 3). На графиках представлены аппаратные и временные затратам для всех простых модулей *p* из диапазона до 8 бит.



а



б

Рис. 4. Сравнение моделей вычислительных каналов по площади (а) и быстродействию (б)

Как можно заметить из графиков, для некоторых значений модулей для схем 2 и 3 с увеличением их значения происходит уменьшение показателей (например, модули 41, 97, 113, 193). Такой эффект объясняется тем, что в наборе используемых субмодулей максимальное из значений является величиной типа 2^n. Известно [21], что модулярные сумматоры такого типа являются наиболее быстродействующими и экономичными по занимаемой площади, тогда как в случае стандартного проектирования, сумматор для маскимального из субмодулей вносит значительный вклад в занимаемую площадь и, в целом, определяет максимальную задержку.

Результаты моделирования показали следующие данные о влиянии контрольной аппаратуры на характеристики схемы бимодульного вычислительного канала: потеря производительности в среднем составила 7 %, рост дополнительного контрольного оборудования составил 40 %. Стоит отметить, что при проведении экспериментов не учитывалась специфика используемого модуля, а также не проводился анализ его субмодульного разложения, влияющего на проектирование последовательно-параллельных участков используемых алгоритмов, с точки зрения минимизации аппаратных и временных затрат.

Заключение. В работе поднимается вопрос об альтернативном способе построения вычислительных каналов модулярного устройства, выгодно отличающейся от традиционной. В основе нового принципа построения лежит бимодульный способ представления вычетов конечного поля GF(p), на основе которого разработан метод построения вычислительных каналов с возможностью обнаружения и исправления одиночной ошибки. Результаты исследований по разработанному методу показали, что потеря в производительности относительно схемы вычислительного канал без защиты составила порядка 7 %, а затраты на дополнительное контрольное оборудование составили в среднем 40 %.

Разработанные технические решения позволили на архитектурном уровне сократить аппаратные и временные затраты на локализацию и исправление сбоя в процессе вычислений. В случае использования бимодульного кодирования вычис-

лительные каналы модулярного устройства способны выполнять самопроверку на наличие сбоя, не привлекая при этом специализированной аппаратуры немодульной операции арифметического устройства. Таким образом, кодовая защищенность модулярной вычислительной системы слагается из двух типов защищенности: внутренней (надежный вычислительный канал) и внешней (избыточная модулярная система).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Каляев И.А., Левин И.И., Семерников Е.А., Шмойлов В.И.* Реконфигурируемые мультиконвейерные вычислительные структуры. – Ростов-на-Дону: Изд-во: ЮНЦ РАН, 2008. – 320 с.
2. *Осипенко П.* Одиночные сбои – вызов для современных микропроцессоров // Электронные компоненты. – 2009. – № 7. – С. 12-15.
3. *Иыуду К.А.* Надежность, контроль и диагностика вычислительных машин и систем. – М.: Высшая школа, 1989. – 216 с.
4. *Дадаев Ю.Г.* Теория арифметических кодов. – М.: Радио и связь, 1981. – 272 с.
5. *Торгашев В.А.* Система остаточных классов и надежность ЦВМ. – М.: Сов. радио, 1973. – 118 с.
6. *Амербаев В.М., Балака Е.С., Соловьев Р.А., Тельпухов Д.В*. Построение обратных преобразователей модулярной арифметики с коррекцией ошибок на базе полиадического кода // Нейрокомпьютеры: разработка и применение. – 2014. – № 9. – С. 30-36.
7. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
8. *Стемпковский А.Л., Амербаев В.М.* Принцип факторизации в проблеме проектирования модулярных процессоров // VI Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2014»: Сб. трудов / Под общ. ред. Ак. РАН Стемпковского А.Л. – М.: ИППМ РАН, 2014. – Ч. IV. – С. 183-186.
9. *Амербаев В.М., Малашевич Д.Б.* Анализ эффективности реализации модульных операций индексной модулярной арифметики // Известия вузов. Электроника. – 2009. – № 80. – С. 54-57.
10. *Стемпковский А.Л., Амербаев В.М., Корнилов А.И.* Модулярная логарифметика – новые возможности для проектирования модулярных вычислителей и преобразователей // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2010»: Сб. научн. тр. / Под общ. ред. А.Л. Стемпковского. – М.: ИППМ РАН, 2010.
11. *Амербаев В.М., Балака Е.С.* Бимодульные вычисления над полем Галуа GF(p) // Вестник Московской государственной академии делового администрирования. Серия: Экономика. – 2013. – № 1 (20). – С. 36-42.
12. *Стемпковский А.Л., Амербаев В.М., Соловьев Р.А.* Принципы рекурсивных модулярных вычислений // Информационные технологии. – 2013. – № 2. – С. 22-27.
13. *Амербаев В.М., Балака Е.С., Соловьев Р.А., Тельпухов Д.В.* Анализ и синтез арифметического узла проф. Поспелова Д.А. поля Галуа // VI Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2014»: Сб. трудов / Под общ. ред. ак. РАН Стемпковского А.Л. – М.: ИППМ РАН, 2014. – Ч. IV. – С. 179-182.
14. *Поспелов Д.А.* Арифметические основы вычислительных машин дискретного действия. – М.: Высшая школа, 1970. – 308 с.
15. *Стемпковский А.Л., Амербаев В.М., Корнилов А.И.* Модулярная логарифметика – новые возможности для проектирования модулярных вычислителей и преобразователей (краткий обзор) // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2010»: Сб. научн. тр. / Под общ. ред. А.Л. Стемпковского”. – М.: ИППМ РАН, 2010.

16. *Амербаев В.М., Балака Е.С., Константинов А.В., Тельпухов Д.В.* Методы ускорения вычислений скалярных произведений векторов в базисе модулярной логарифметики // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2010»: Сб. трудов / Под общ. ред. ак. РАН А.Л. Стемпковского. – М.: ИППМ РАН, 2010. – С. 378-381.
17. *Амербаев В.М., Балака Е.С., Щелоков А.Н.* Применение структурной избыточности для повышения надежности арифметического узла вычислительного элемента бимодульной арифметики // Известия ЮФУ. Технические науки. – 2014. – № 7. – С. 248-254.
18. *Корнилов А.И., Исаева Т.Ю., Семенов М.Ю.* Методы логического синтеза сумматоров с ускоренным переносом по модулю (2n-1) на основе BDD-технологии // Известия вузов. Электроника. – 2004. – № 3. – С. 54-60.
19. *Амербаев В.М.* Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976. – 324 с.
20. *Калашников В.С.* Исследование и разработка методов проектирования быстродействующих вычислительных узлов для реализации отказоустойчивых систем на основе модулярной арифметики: Дис. … канд. тех. наук: 05.13.05. – М., 2007.
21. *Jaberipur and S. Nejati.* Balanced minimal latency RNS addition for moduli set $\{2^n-1,2^n,2^{n+1}\}$ // in Proc. 18th Int. Conf. Systems, Signals and Image Processing (IWSSIP). – 2011. – P. 1-7.

REFERENCES

1. *Kalyaev I.A., Levin I.I., Semernikov E.A., Shmoylov V.I.* Rekonfiguriruemye mul'tikonveyernye vychislitel'nye struktury [Multiconference reconfigurable computing structures]. Rostov-on-Don: Izd-vo: YuNTs RAN, 2008, 320 p.
2. *Osipenko P.* Odinochnye sboi – vyzov dlya sovremennykh mikroprotsessorov [Single failures – a challenge for modern microprocessors], *Elektronnye komponenty* [Electronic Components], 2009, No. 7, pp 12-15.
3. *Iyudu K.A.* Nadezhnost', kontrol' i diagnostika vychislitel'nykh mashin i system [Reliability, control and diagnostics of computers and computer systems]. Moscow: Vysshaya shkola, 1989, 216 p.
4. *Dadaev Yu.G.* Teoriya arifmeticheskikh kodov [The theory of arithmetic codes]. Moscow: Radio i svyaz', 1981, 272 p.
5. *Torgashev V.A.* Sistema ostatochnykh klassov i nadezhnost' TsVM [The system of residual classes and the reliability of the CVM]. Moscow: Sov. Radio, 1973, 118 p.
6. *Amerbaev V.M., Balaka E.S., Solov'ev R.A., Tel'pukhov D.V.* Postroenie obratnykh preobrazovateley modulyarnoy arifmetiki s korrektsiey oshibok na baze poliadicheskogo koda [The construction of inverter modular arithmetic with the error correction code on the basis politicheskogo], *Neyrokomp'yutery: razrabotka i primenenie* [Neurocomputers: development and application], 2014, No. 9, pp. 30-36.
7. *Akushskiy I.Ya., Yuditskiy D.I.* Mashinnaya arifmetika v ostatochnykh klassakh [Machine arithmetic in residual classes]. Moscow: Sovetskoe radio, 1968, 440 p.
8. *Stempkovskiy A.L., Amerbaev V.M.* Printsip faktorizatsii v probleme proektirovaniya modulyarnykh protsessorov [The principle of factorization in the problem of designing modular processors], *VI Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Problemy razrabotki perspektivnykh mikro- i nanoelektronnykh sistem – 2014»: Sb. trudov* [VI all-Russian scientific-technical conference "Problems of development of perspective micro- and nanoelectronic systems – 2014": the collected works], Under the General ed. ak. RAS Stempkovskogo A.L. Moscow: IPPM RAN, 2014. Part IV, pp. 183-186.
9. *Amerbaev V.M., Malashevich D.B.* Analiz effektivnosti realizatsii modul'nykh operatsiy indeksnoy modulyarnoy arifmetiki [Analysis of the effectiveness of the implementation of modular operations, modular arithmetic index], *Izvestiya vuzov. Elektronika* [Izvestiya vuzov. Electronics], 2009, No. 80, pp. 54-57.
10. *Stempkovskiy A.L., Amerbaev V.M., Kornilov A.I.* Modulyarnaya logarifmetika – novye vozmozhnosti dlya proektirovaniya modulyarnykh vychisliteley i preobrazovateley [Modular logaritmica – new opportunities for the design of modular calculators and converters], *IV Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Problemy razrabotki perspektivnykh mikro- i nanoelektronnykh sistem – 2010»: Sb. nauchn. tr.* [IV all-Russian scientific-technical conference "Problems of development of perspective micro- and nanoelectronic systems – 2010": Collection of scientific papers], Under the General ed. ak. RAS Stempkovskogo A.L. Moscow: IPPM RAN, 2010.

11. *Amerbaev V.M., Balaka E.S.* Bimodul'nye vychisleniya nad polem Galua GF(p) [Bimodule computation over Galois field GF(p)], *Vestnik Moskovskoy gosudarstvennoy akademii delovogo administrirovaniya. Seriya: Ekonomika* [Bulletin of the Moscow state Academy of business administration. Series: Economics], 2013, No. 1 (20), pp. 36-42.
12. *Stempkovskiy A.L., Amerbaev V.M., Solov'ev R.A.* Printsipy rekursivnykh modulyarnykh vychisleniy [The recursive principles of modular computing], *Informatsionnye tekhnologii* [Information Technologies], 2013, No. 2, pp. 22-27.
13. *Amerbaev V.M., Balaka E.S., Solov'ev R.A., Tel'pukhov D.V.* Analiz i sintez arifmetiche-skogo uzla prof. Pospelova D.A. polya Galua [Analysis and synthesis of arithmetic node Prof. Pospelov D. A. Galois field], *VI Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Problemy razrabotki perspektivnykh mikro- i nanoelektronnykh sistem – 2014»: Sb. Trudov* [VI all-Russian scientific-technical conference "Problems of development of perspective micro- and nanoelectronic systems – 2014": the collected works], Under the General ed. ak. RAS Stempkovskogo A.L. Moscow: IPPM RAN, 2014, Part IV, pp. 179-182.
14. *Pospelov D.A.* Arifmeticheskie osnovy vychislitel'nykh mashin diskretnogo deystviya [Arithmetic basics of computers discrete action]. Moscow: Vysshaya shkola, 1970, 308 p.
15. *Stempkovskiy A.L., Amerbaev V.M., Kornilov A.I.* Modulyarnaya logarifmetika – novye vozmozhnosti dlya proektirovaniya modulyarnykh vychisliteley i preobrazovateley (kratkiy obzor) [Modular logaritmica – new opportunities for the design of modular calculators and converters (a brief overview)], *IV Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Problemy razrabotki perspektivnykh mikro- i nanoelektronnykh sistem – 2010»: Sb. nauchn. tr.* [IV all-Russian scientific-technical conference "Problems of development of perspective micro- and nanoelectronic systems – 2010": Collection of scientific papers], Under the General ed. ak. RAS Stempkovskogo A.L. Moscow: IPPM RAN, 2010.
16. *Amerbaev V.M., Balaka E.S., Konstantinov A.V., Tel'pukhov D.V.* Metody uskoreniya vychisleniy skalyarnykh proizvedeniy vektorov v bazise modulyarnoy logarifmetiki [Methods to accelerate the computation of scalar products of vectors in the basis of modular logarithmitic], *IV Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Problemy razrabotki perspektivnykh mikro- i nanoelektronnykh sistem – 2010»: Sb. trudov* [IV all-Russian scientific-technical conference "problems of development of perspective micro - and nanoelectronic systems – 2010": proceedings of the], Under the General ed. ak. RAS Stempkovskogo A.L. Moscow: IPPM RAN, 2010, pp. 378-381.
17. *Amerbaev V.M., Balaka E.S., Shchelokov A.N.* Primenenie strukturnoy izbytochnosti dlya povysheniya nadezhnosti arifmeticheskogo uzla vychislitel'nogo elementa bimodul'noy arifmetiki [Use of structural redundancy for increase of reliability of arithmetic unit of the computing element of bimodular arithmetic], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 7, pp. 248-254.
18. *Kornilov A.I., Isaeva T.Yu., Semenov M.Yu.* Metody logicheskogo sinteza summatorov s uskorennym perenosom po modulyu (2n-1) na osnove BDD-tekhnologii [Methods of logic synthesis of adders with accelerated migration modulo (2n-1) based on BDD technologies], *Izvestiya vuzov. Elektronika* [News of higher educational institutions. Electronics], 2004, No. 3, pp. 54-60.
19. *Amerbaev V.M.* Teoreticheskie osnovy mashinnoy arifmetiki [Theoretical foundations of computer arithmetic]. Alma-Ata: Nauka, 1976, 324 p.
20. *Kalashnikov V.S.* Issledovanie i razrabotka metodov proektirovaniya bystrodeystvuyushchikh vychislitel'nykh uzlov dlya realizatsii otkazoustoychivykh sistem na osnove modulyarnoy arifmetiki: Dis. … kand. tekh. nauk: 05.13.05 [Research and development of design techniques for high-performance computing nodes to implement failover systems based on modular arithmetic. Cand. eng. sc. diss.]. Moscow, 2007.
21. *Jaberipur and S. Nejati.* Balanced minimal latency RNS addition for moduli set $\{2^n-1,2^n,2^{n+1}\}$, *in Proc. 18th Int. Conf. Systems, Signals and Image Processing (IWSSIP)*, 2011, pp. 1-7.

Статью рекомендовал к опубликованию д.т.н., профессор А.Л. Глебов.

Щелоков Альберт Николаевич – Институт проблем проектирования в микроэлектронике РАН; e-mail: schan@ippm.ru; 124681, Зеленоград, ул. Советская, 3; тел.: +74997299890; зам. директора; к.ф.-м.н.

Балака Екатерина Станиславовна – e-mail: balakaes@yandex.ru; тел.: +79067389568; м.н.с.

Schelokov Albert Nikolaevich – The Institute for Design Problems in Microelectronics (IPPM RAS); e-mail: schan@ippm.ru; 3, Sovetskaya street, Zelenograd, 124681, Russia; phone: +74997299890; deputy director; cand. of phis.-math. sc.

Balaka Ekaterina Stanislavovna – e-mail: balakaes@yandex.ru; phone: +79067389568; researcher.

УДК 621.3.049.771.14

С.В. Гаврилов, Г.А. Иванова, А.Н. Соловьев, А.Л. Стемпковский

ОПТИМИЗАЦИЯ СХЕМ КОДИРОВАНИЯ НА ОСНОВЕ ВЫБОРА ВАРИАНТА КОММУТАЦИЙ С УЧЕТОМ ЛОГИЧЕСКИХ КОРРЕЛЯЦИЙ МЕЖДУ ВЫХОДАМИ КОМБИНАЦИОННОЙ СХЕМЫ*

Данная статья посвящена исследованию и разработке методов повышения помехозащищенности микроэлектронных схем. По мере роста степени интеграции и уменьшения технологических размеров возрастает роль повышения надежности и помехоустойчивости проектируемых устройств под воздействием различных источников помех и сбоев: технологических, радиационных, перекрестных помех, деградации во времени, скачков напряжения питания и др. В настоящее время складывается ситуация, когда фактор помехоустойчивости в микроэлектронике становится определяющим условием работоспособности и надежности разрабатываемой электронной аппаратуры. При этом одни из ключевых компонентов – комбинационные схемы. Поэтому актуальным является исследование и разработка методов повышения отказоустойчивости микроэлектронных комбинационных схем. Для обеспечения необходимого уровня помехозащищенности (обнаружение ошибок с заданной степенью кратности) для синтеза схемы кодирования предлагается использовать операцию деления на образующий многочлен в двоичном поле Галуа. Предлагается оптимизация схем кодирования за счет выбора варианта коммутирования выходов дубликата основной схемы на основе результатов анализа логических корреляций.

Помехоустойчивость; упорядоченные диаграммы двоичных решений; поля Галуа.

S.V. Gavrilov, G.A. Ivanova, A.N. Soloviev, A.L. Stempkovskiy

OPTIMIZATION OF CODER CIRCUIT BASED ON THE VARIANT COMMUTATIONS SELECTION WITH ACCOUNT FOR LOGIC CORRELATION BETWEEN THE OUTPUTS OF THE COMBINATIONAL CIRCUIT

This article is dedicated to research and develop methods for increasing the microelectronic circuits' noise immunity. The role of improving the reliability and noise immunity of designed devices under the influence of various sources of interference and disruption is increases. At present time, the noise immunity factor in microelectronics is becoming critical condition of reliability and working capacity of the developed electronic equipment. Thus one of the key components are combinational circuits. Therefore, research and development of methods for noise immunity improving of microelectronic combinational circuits is actual problem. The operation of division by the polynomial generator in binary Galois field is proposed to use to ensure the necessary level of noise immunity (error detection with a predetermined degree of multiplicity) for the synthesis of the coder circuit. Optimization of coder circuit is proposed by choosing variant of outputs commutation basic circuit duplicate based on the results of logical correlations analysis.

Noise tolerance; binary decision diagram (BDD); Galois field.

* Работа выполнена при поддержке РФФИ (проект № 15-07-02065).