УДК 681.3

Отказоустойчивый систолический процессор цифровой обработки сигналов, функционирующий в модулярном коде

И.А. Калмыков, М.И. Калмыков, Е.П. Степанова, А.В. Велигоша, В.В. Бороденко

ФГОУ ВПО Северо-Кавказский Федеральный Университет, kia762@yandex.ru, ytosss777@yandex.ru

Аннотация **— Рассмотрена систолическая модель, реализующая ортогональные преобразования сигналов в расширенных полях Галуа $GF(p^v)$ на основе полиномиальной системы классов вычетов. Доказана возможность использования модулярных кодов для повышения отказоустойчивости.**

Ключевые слова **— полиномиальная система классов вычетов, модулярные коды, отказоустойчивость, цифровая обработка сигналов.**

I. Введение

Телекоммуникационные технологии, бурное развитие которых наблюдается в последние годы, предоставляют пользователям все новые возможности. Повысить эффективность таких технологий можно за счет широкого применения методов цифровой обработки сигналов (ЦОС). Возрастание требований к технико-экономическим характеристикам современных систем ЦОС, расширение областей использования и усиливающаяся тенденция к параллельным методам их организации привели к необходимости применения моделей цифровой обработки сигналов, обладающих свойством параллельно-конвейерной организации вычислений.

Одно из направлений параллельно-конвейерной организации вычислений связано с использованием непозиционных модулярных кодов. Применение модулярной арифметики позволяет повысить эффективность выполнения ортогональных преобразований сигналов, обеспечивая их с высокой точностью и скоростью. При этом параллельный спецпроцессор (СП) цифровой обработки сигналов должен обладать свойством отказоустойчивости, которое позволяет ему сохранять работоспособное состояние в условиях возникновения отказов.

Поэтому разработка высокоскоростного отказоустойчивого спецпроцессора цифровой обработки сигналов, функционирующего в модулярном коде, является актуальной задачей.

II. Постановка и решение задач исследования

1) Анализ основных областей применения модулярных кодов

Наиболее характерной особенностью последних лет является расширение областей применения модулярной арифметики. Проведенный анализ позволяет выделить основные направления, в которых наиболее ярко проявляются достоинства непозиционных модулярных кодов.

Основу первого направления составляют классические методы и алгоритмы ЦОС, использующие ортогональные преобразования сигналов в поле комплексных чисел [1-3]. Параллельная обработка данных по вычислительным каналам, которые являются основаниями системы остаточных классов (СОК), малая разрядность остатков позволяет повысить скорость обработки сигналов.

Второе направление применения алгебраических систем, обладающих свойством кольца и поля, к которым относятся модулярные коды, связано с построением псевдослучайных функций (ПСФ). В работах [4-6] показана целесообразность реализации таких ПСФ в электронных коммерческих системах. А в работе [7] показан алгоритм определения статуса спутника системы спутниковой связи, применяемой для дистанционного управления экологически опасными технологиями, который использует ПСФ, реализованное на основе алгебраической системы, обладающей свойством кольца и поля.

В основу третьего направления можно положить методы и алгоритмы обеспечения отказоустойчивости специализированных вычислительных устройств. Введение дополнительных избыточных оснований позволяет осуществлять поиск и коррекцию ошибок, возникающих в процессе функционирования спецпроцессоров из-за сбоев и отказов. В работах [8, 9, 10] представлены алгоритмы и их схемные реализации, позволяющие исправлять ошибки с помощью непозиционных модулярных кодов.

2) Выполнение ортогональных преобразований сигналов в полиномиальной системе классов вычетов

Для решения задач, связанных с предоставлением таких услуг, как видео и речевая связь, системы видеоконференций, голосовая почта, как правило, используются ортогональные преобразования сигналов. В настоящее время СП ЦОС используют несколько математических моделей, которые можно разделить на следующие группы. Основу первой составляют математические модели, базирующиеся на

реализации ортогональных преобразований сигналов над полем комплексных чисел, в частности, дискретном преобразовании Фурье (ДПФ) и быстром преобразовании Фурье (БПФ). Так, в системах широкополосного беспроводного доступа (ШБД) для борьбы с помехами при многолучевом приеме применяется технология ортогонального частотного мультиплексирования OFDM. Технически метод OFDM реализуется путем выполнения обратного ДПФ в модуляторе передатчика и прямого ДПФ – в демодуляторе приемника приемопередающего устройства [11,12].

Однако БПФ характеризуется относительно низкой надежностью функционирования СП из-за наличия двух вычислительных трактов (для обработки действительных и мнимых частей). Кроме того, поворачивающие коэффициенты – иррациональные числа, что снижает точность вычислений.

Данных недостатков лишены модели ЦОС, обладающие свойством кольца и поля. Особое место среди них занимают модели ортогональных преобразований сигналов в полиномиальной системе классов вычетов (ПСКВ). Пусть заданы модулярные коды в кольце полиномов $A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z))$ и $B(z) = (\beta_1(z), \beta_2(z), ..., \beta_n(z))$. Применение ПСКВ позволяет свести операции в кольце полиномов к соответствующим операциям над остатками. Тогда:

$$\left|A(z) \otimes B(z)\right|^{+}_{p(z)} = \left|\alpha_i(z) \otimes \beta_i(z)\right|^{+}_{p_i(z)}, \qquad (1)$$

где $\alpha_i(z) \equiv A(z) \bmod p_i(z)$; $\beta_i(z) \equiv B(z) \bmod p_i(z)$; $\otimes$ – сложение, вычитание и умножение в GF(p); $l = 1,\ldots,n$.

За счет гомоморфизма, порожденного китайской теоремой об остатках (КТО), можно организовать многомерную обработку сигналов с использованием ПСКВ, что позволит повысить скорость выполнения ЦОС [8,9]. Это обусловлено тем, что вычисления организуются в кольце полинома $P(z) = P_1(z) + \ldots + P_n(z)$, представляющем собой сумму локальных колец полиномов $P_l(z)$, образованных неприводимым полиномом $p_l(z)$ над полем $GF(p)$, где $l=1,2,\ldots,n$, n – количество локальных колец. Тогда вычислениеN спектральных составляющих на основе обобщенного ДПФ в кольце полиномов определяется как

$$\begin{cases} X_1^k(z) = \sum_{m=0}^{N-1} x_1^m(z)\beta_1^{km}(z) \bmod p_1(z) \\ \vdots \\ X_n^k(z) = \sum_{m=0}^{N-1} x_n^m(z)\beta_n^{km}(z) \bmod p_n(z) \end{cases}, \qquad (2)$$

где $\left\{X_l^k(z), x_l^m(z), \beta_l^{km}(z)\right\} \in P_l(z)$; k = 0,1,…, N-1.

Повышение скорости реализации ЦОС возможно за счет систолических методов реализации.

3) Разработка систолического процессора, функционирующего в ПСКВ

Параллельно-конвейерные вычислительные структуры систолического типа представляют собой множество однотипных с точки зрения функциональных возможностей процессорных элементов, называемых вычислительными ячейками (ВЯ). Основным принципом систолической системы является то, что все данные, регулярно и ритмически проходящие через массив ВЯ, используются многократно. Для этого все процессорные элементы соединены между собой посредством локальных связей. При этом каждая ВЯ соединена только с ближайшими соседними вычислительными ячейками для передачи данных.

Систолический принцип вычисления наиболее удачно реализуется в кодах ПСКВ. Совмещение высокой производительности кодов ПСКВ и параллельно-конвейерной систолической организации вычислений позволяет осуществлять обработку сигналов в реальном масштабе времени, в частности, изображений. Известно, что цифровая обработка изображений требует выполнения двумерного ортогонального преобразования большого массива данных. Так, обработка и анализ двумерного изображения размером 500×500 точек при использовании окна с размерностью 30×30 пикселей требует порядка 200 000000 операций для проведения одного цикла расчетов.

Применение систолического принципа вычислений позволяет обеспечить соответствие структуры многомерных данных линейной структуре вычислительного устройства ЦОС. Представив исходные данные в виде матрицы X_N размером N×N,запишем двумерное ДПФ в кольце полиномов:

$$\begin{cases} C_N \bmod p_1(z) = \left(\left(X_N^1 E_N^1\right) E_N^1\right) \bmod p_1(z) \\ C_N \bmod p_2(z) = \left(\left(X_N^2 E_N^2\right) E_N^2\right) \bmod p_2(z) \\ \vdots \\ C_N \bmod p_n(z) = \left(\left(X_N^n E_N^n\right) E_N^n\right) \bmod p_n(z) \end{cases}, \qquad (3)$$

где $X_N^i = X_N \bmod p_i(z)$; $E_N^i = E_N \bmod p_i(z)$; E_N– матрица поворачивающих коэффициентов, образующих мультипликативную группу порядкаN.

Из (3) следует возможность использования систолической процедуры ДПФ в кольце полиномов:

$$\begin{cases} \left|C^{1}\right|^{+}_{p_i(z)} = \left|\sum_{l=1}^{N}\left|E_N X^{l}\right|^{+}_{p_i(z)}\right|^{+}_{p_i(z)} \\ \vdots \\ \left|C^{N}\right|^{+}_{p_i(z)} = \sum_{l=1}^{N}\left|\beta^{l-1}\ldots\left|\beta^{l-1}\left|E_N X^{l}\right|^{+}_{p_i(z)}\right|^{+}_{p_i(z)}\right|^{+}_{p_i(z)} \end{cases}, \quad (4)$$

где $\left|C^{l}\right|^{+}_{p_i(z)} = \left[\left|C_{l1}\right|^{+}_{p_i(z)},\ldots,\left|C_{lN}\right|^{+}_{p_i(z)}\right]^{+}_{p_i(z)}$ и

$\left|X^{l}\right|^{+}_{p_i(z)} = \left[\left|x_{l1}\right|^{+}_{p_i(z)},\ldots,\left|x_{lN}\right|^{+}_{p_i(z)}\right]^{+}_{p_i(z)}$ – транспонированное представление вектора конечных результатов ДПФ и построчного вектора входных данных по модулю$p_i(z)$.

Основным достоинством рассмотренной процедуры вычисления двумерного ДПФ в кольце полиномов является отсутствие в явной форме операции транспонирования матрицы промежуточных результатов, что позволяет в значительной степени повысить быстродействие процессора ЦОС.

Преобразования $\left|E_N X^{1}\right|^{+}_{p_i(z)}$, соответствующие выполнению одномерного ДПФ по строке матрицы исходных данных, осуществляется на первой систолической матрице. Данная матрица является чисто-систолической матрицей (ЧСМ) и содержит N-1 вычислительных ячеек, имеющих одинаковую структуру. Дополнительные вычисления, соответствующие выполнению преобразований Фурье по второй координате, выполняются с помощью второй систолической матрицы. Данная матрица относится к многоканальным систолическим матрицам (МСМ) с блоком сдвиговых регистров (БСР). Матрица МСМ содержит N вычислительных ячеек, имеющих однотипную структуру. Каждая ячейка МСМ содержит регистр *Рг* для хранения значений коэффициентов $W_3^{k-1} \bmod p_i(z) = \beta^{(k-1)j} \bmod p_i(z)$, взятых по модулю $p_i(z)$. Кроме того, в состав вычислительной ячейки входят модульный умножитель *(У$_j$)* и модульный сумматор (C_j), j=1,2,…,N. На рисунке 1 представлена структура систолического СП двумерного ДПФ по модулю $p(z)=z^2+z+1$.

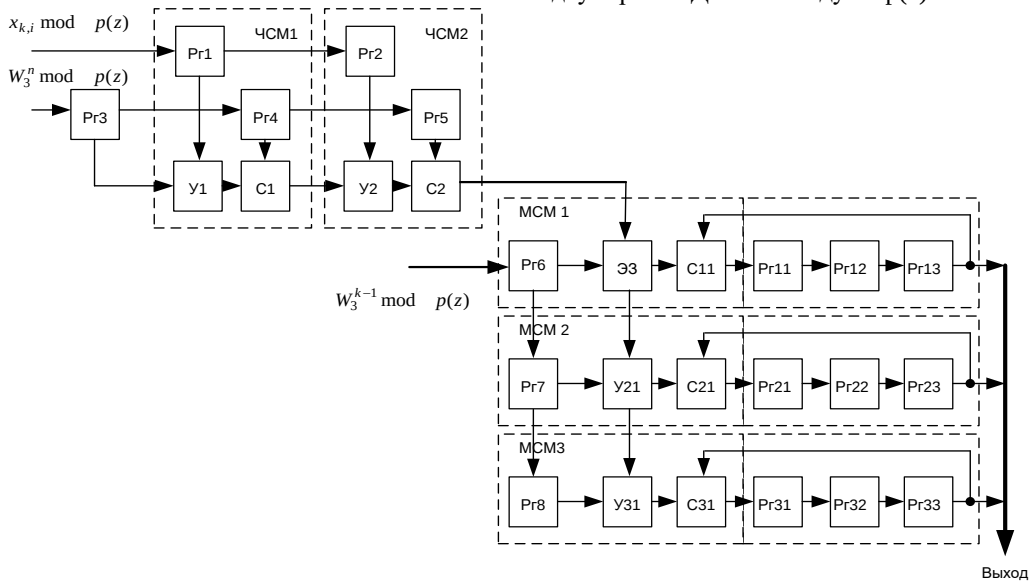

Рис. 1. Структура систолического СП для вычисления двумерного ДПФ по модулю $p(z)=z^2+z+1$

В ходе проводимых исследований было проведено моделирование СП двумерного ДПФ, функционирующего в ПСКВ, и позиционного СП БПФ. Так как разрядность обрабатываемых составляла 24 разряда, то для реализации непозиционного СП ПСКВ было выбрано четыре неприводимых полинома шестой степени. Для моделирования был использован центральный модуль NI PXIe-8115 фирмы National Instruments, в качестве программного обеспечения – LabVIEW 2013. Проведенные исследования показали, что совмещение достоинств модульного представления данных с систолической обработкой позволили повысить скорость вычисления двумерного ДПФ на 11,9% по сравнению с цифровой обработкой изображения на основе 24-разрядного СП БПФ.

4) Разработка отказоустойчивого непозиционного СП ПСКВ

Применение модулярного полиномиального кода позволяет не только повысить скорость обработки данных, но и обеспечить отказоустойчивость процессора, т.е. сохранять работоспособное состояние при возникновении последовательности отказов за счет снижения в допустимых пределах основных показателей качества функционирования [10]. Это реализуется за счет реконфигурации структуры СП

путем перераспределения вычислительной нагрузки между работоспособными вычислительными трактами.

Основным сдерживающим фактором широкого применения реконфигурации при построении отказоустойчивых СП, функционирующих в ПСКВ, является отсутствие эффективного алгоритма пересчета ортогональных базисов при постепенной деградации структуры вычислительного устройства, которые используются при обратном преобразовании из модулярного полиномиального кода в позиционный двоичный код. Решить данную проблему можно за счет применения теорем, которые можно положить в основу алгоритма вычисления новых значений ортогональных базисов при отказе модулей.

Теорема 1. В полиномиальной системе классов вычетов с набором оснований $p_1(z)$, $p_2(z),\ldots,p_{k+r}(z)$, которые могут динамически меняться, значение j-го ортогонального базиса будет определяться как

$$B_j(z) = \beta_j^{l_j} \bmod p_j(z) \prod_{\substack{i=1 \\ i\neq j}}^{k+r} p_i(z), \qquad (5)$$

где $l_j(z) = -\sum_{\substack{i=1 \\ i\neq j}}^{k+r} l_i \bmod(\deg p_j(z) - 1)$ – индекс веса j-го ортогонального базиса; $l_i(z) = \log_{p_j(z)} p_i(z)$ – индекс полинома $p_i(z)$; β_j – первообразный элемент по модулю $p_j(z)$.

Доказательство. Согласно китайской теореме об остатках, значение ортогонального базиса определяется как

$$B_j(z) \equiv 1 \bmod p_j(z), \qquad (6)$$

где j = 1,2,…,k+r.При этом ортогональный базис вычисляется как

$$B_j(z) = m_i(z) P(z) \big/ p_i(z) = m_j(z) M_j(z), \qquad (7)$$

где $m_j(z)$ – вес j-го ортогонального базиса; $P(z) = \prod_{l=1}^{k+r} p_l(z)$ – полный диапазон оснований ПСКВ.

Известно, что для определения веса ортогонального базиса используют

$$m_j(z)\sigma_j(z) \equiv 1 \bmod p_j(z). \qquad (8)$$

При этом значение

$$\sigma_j(z) = M_j(z) \bmod p_j(z). \qquad (9)$$

Тогда на основе (8) и (9) можно сделать вывод, что

$$m_j(z) \equiv (\sigma_j(z))^{-1} \bmod p_j(z). \qquad (10)$$

Используя первообразный элемент β_j мультипликативной группы, порожденной полиномом $p_j(z)$, представим последнее равенство в виде

$$\beta_j^{l_j} \equiv \beta_j^{-y_j} \bmod p_j(z), \qquad (11)$$

где $y_j(z) = \log_{p_j(z)} \sigma_j(z)$ – индекс элемента $\sigma_j(z)$.Но известно, что

$$\delta_j(z) = \left(\frac{P(z)}{p_i(z)}\right)\left(\prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z)\right) \bmod p_j(z). \qquad (12)$$

Тогда, используя свойство изоморфизма и выражение (12), получаем

$$l_j(z) = -\sum_{\substack{i=1 \\ i\neq j}}^{k+r} l_i \bmod(\deg p_j(z) - 1). \qquad (13)$$

Теорема доказана.

Теорема 2.В избыточной ПСКВ с основаниями p1(z), p2(z),…,pk+r(z) при деградации по j-му модулю значение ортогональных базисов новой системы оснований будет определяться как

$$B_i^j(z) = \left(\prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z)^{-1}\right) \bmod p_i(z) \prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z). \qquad (14)$$

Доказательство. Согласно китайской теореме об остатках, значение ортогонального базиса определяется из условия (6). Упростив выражения (7)-(9), получаем

$$\delta_i(z) = \left(\prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z)\right) \bmod p_i(z). \qquad (15)$$

Пусть в системе оснований ПСКВ произошла деградация по j-му основанию. Тогда новая система содержит следующие модули:$p_1(z)$, $p_2(z),\ldots$, $p_{j-1}(z)$, $p_{j+1}(z),\ldots$, $p_{k+r}(z)$. При этом полный диапазон новой деградируемой системы ПСКВ будет определяться как

$$P^j(z) = \left(\prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z)\right). \qquad (16)$$

Тогда новые значения ортогональных базисов при $i \neq j$определяются как

$$B_i^j(z) = m_i^j(z)\,P^j(z)\big/p_i(z). \qquad (17)$$

В этом случае значение веса ортогонального базиса в деградируемой системе оснований ПСКВ равно

$$m_i^j(z)\delta_i^j(z) \equiv 1 \bmod p_i(z). \qquad (18)$$

Тогда имеем:

$$\delta_i^j(z) = \left(\prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z) \right) \bmod p_i(z) \qquad (19)$$

Разделим обе части выражения (18) на равенство (19). Получаем

$$m_i^j(z) = \left(\prod_{\substack{l=1 \\ l\neq i,j}}^{k+r} p_l(z)^{-1} \right) \bmod p_i(z) \qquad (20)$$

Тогда значение ортогонального базиса в деградируемой ПСКВ определяется выражением (14). **Теорема доказана**.

Данные теоремы положены в основу разработанного алгоритма реконфигурации структуры СП ПСКВ. Для оценки эффективности разработанного алгоритма реконфигурации был проведен сравнительный анализ СП ПСКВ, реализующего этот алгоритм, с процессором, использующим корректирующие способности кодов ПСКВ, а также с позиционным СП, имеющим мажоритарную структуру. В качестве целевой функции был выбран коэффициент запаса работоспособности, определяемый как

$$\delta_a = H_a \big/ N_a, \qquad (21)$$

где H_a и N_a – число работоспособных состояний и общее число возможных состояний спецпроцессора при возникновении a=1, 2,… отказов.

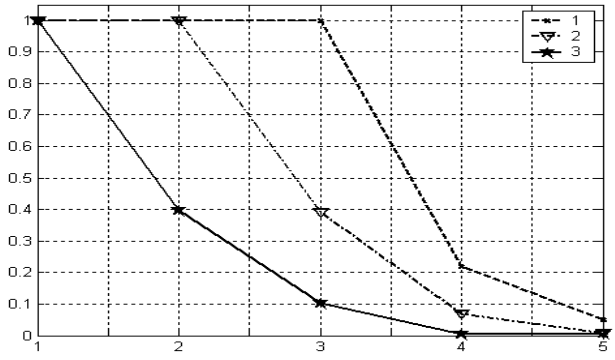

Рис. 2. Изменение коэффициента запаса работоспособности СП при накоплении отказов элементов a = 1, 2, …

Результаты исследования приведены на рис. 2. Обозначения: 1 – СП ПСКВ с реконфигурируемой структурой; 2 – СП ПСКВ с коррекцией ошибки; 3 – СП ПСС с мажоритаром «2 из 3».

Анализ графика показывает, что применение алгоритма реконфигурации позволяет сохранять работоспособное состояние СП ПСКВ с тремя контрольными основаниями даже при отказе трех вычислительных каналов. В то же самое время позиционный СП, имеющий схему «2 из 3», выходит из строя при втором отказе оборудования, а СП ПСКВ с коррекцией ошибки – при отказе третьего вычислительного канала.

III. Выводы

Применение систолических принципов организации вычислений в алгебраических системах, обладающих свойством кольца и поля, обеспечивает повышение скорости вычислений при выполнении цифровой обработки сигналов. Представленные в работе результаты показали, что применение модулярных кодов ПСКВ и систолических параллельно-конвейерных вычислений позволило повысить скорость выполнения двумерного преобразования сигналов на 11,9% по сравнению с цифровой обработкой изображений на основе позиционного 24-разрядного СП БПФ.

Кроме того, применение модулярных кодов позволяет повысить отказоустойчивость специализированных процессоров ЦОС. В работе представлены теоремы, применение которых позволяет осуществлять пересчет ортогональных базисов для реконфигурируемых СП ЦОС, функционирующих в кодах ПСКВ. Применение алгоритма реконфигурации позволяет сохранять работоспособное состояние непозиционного СП ЦОС при возникновении отказов за счет снижения в допустимых пределах основных показателей функционирования. Проведенные исследования показали, что применение алгоритма реконфигурации позволяет сохранять работоспособное состояние СП ПСКВ с тремя контрольными основаниями даже при отказе трех вычислительных каналов. В тоже самое время позиционный СП, имеющий схему «2 из 3», выходит из строя при втором отказе оборудования, а СП ПСКВ с коррекцией ошибки – при отказе третьего вычислительного канала.

Литература

[1] Bankas E. K. and Gbolagade K. A. A New Efficient FPGA Design of Residue-To-Binary Converter. International Journal of VLSI design & Communication Systems (VLSICS), Vol 4, No. 6, December, 2013.

[2] Gbolagade K. A. An Efficient MRC based RNS-to-Binary Converter for the {2 2n−1, 2 n, 2 2n+1 −1} Moduli Set. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013

[3] Omondi A. and Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK 2007.
[4] Qian Wang. Compact k-spendable E-cash with anonymity control based offline TTP. International Journal of Innovative Computing, Information and Control Volume 7, Number 1, January 2011 pp. 459 - 469
[5] Саркисов А.Б, Макарова А. В., Калмыков М. И. 2014. Расширение методов защиты систем электронной коммерции на основе модулярных алгебраических схем // Известия Южного федерального университета. Технические науки. 2014. № 2 (151). С. 218 - 225.
[6] Калмыков И.А., Дагаева О.И. Науменко Д.О., Вельц О.В. Системный подход к применению псевдослучайных функций в системах защиты информации// Известия ЮФУ. Технические науки, Таганрог: ТРТУ, 2013 г. №12, С. 228-234
[7] Пашинцев В.П., Калмыков И.А., Вельц О.В Методы защиты передаваемой информации для систем удаленного контроля и управления высокотехнологическими объектами // Вестник Северо-Кавказского федерального университета. 2014. № 4 (43). С. 38-43
[8] Kalmykov Igor Anatolyevich, Katkov Konstantin Aleksandrovich, Naumenko Daniil Olegovich, Artem Bronislavovich Sarkisov, Alena Vasilyevna Makarova, 2014. Parallel modular technologies in digital signal processing // Life Science Journal 2014; 11 (11s) p. 435 - 438. http://www.lifesciencesite.com
[9] Горденко Д.В., Резеньков Д. Н., Саркисов А. Б., 2014. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. Ставрополь, Издательство Фабула. 2014. – 180 с.
[10] Калмыков, И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов [Текст]/Под ред. Н.И. Червякова – М: Физматлит, 2005. - 276 с.
[11] YongSooCho, JaekwonKim, Won, Young, ChungG., 2010. Kang MIMO-OFDM Wireless Communications with MATLAB, - WILEY.2010
[12] T. Shahana, B. Jose, R. James, K. Jacob, and S. Sasi, 2008. RRNS-convolutional encoded concatenated code for ofdm based wireless communication. In Networks, 2008. 16th IEEE International Conference on, dec. 2008, pp. 1–6.

Fault-tolerant systolic processor for digital signal processing in modular code

I.A. Kalmykov, M.I. Kalmykov, E.P. Stepanova, A.V. Veligosha, V.V. Borodenko

Federal State Educational Institution of Higher Professional Education North-Caucasus Federal University, kia762@yandex.ru, ytosss777@yandex.ru

***Keywords*— polynomial residue number system, modular codes, fault tolerance, digital signal processing**

ABSTRACT

The goal of this work is to increase the fault tolerance of the position-independent special-purpose processor for digital signal processing (DSP) with a parallel-pipeline computing organization due to rearranging in the polynomial residue number system(PRNS).

Higher requirements to the technical and economic features of modern digital signal processing (DSP) systems, wider ranges of their application and a growing tendency to use parallel methods of their organization have made it necessary to apply models of digital signal processing with the parallel-pipeline computing organization. To further increase the speed of signal processing, the article suggests using modular parallel codes. It shows the implies of the two-dimensional signal transformation with use of a systolic processor that operates in the polynomial residue number system.

Independence of data handling on the bases of PRNS can become a basis for development of a method of reconfiguration of SP PRNS. In this case SP PRNS switches-off the refused channel and saves up state due to lowering in tolerable limits of the main figures of merit of functioning. However, the absence of algorithms for orthogonal basis recomputation makes it impossible to widely apply the reconfiguration in order to restore the SP PRNS working condition. That is why designing a method of orthogonal basis recomputation with the gradual degradation of the position-independent structure of SP PRNS is a relevant task.

REFERENCES

[1] Bankas E. K. and Gbolagade K. A. A New Efficient FPGA Design of Residue-To-Binary Converter. International Journal of VLSI design & Communication Systems (VLSICS), Vol 4, No. 6, December, 2013.
[2] Gbolagade K. A. An Efficient MRC based RNS-to-Binary Converter for the {2 2n−1, 2 n, 2 2n+1 −1} Moduli Set. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013
[3] Omondi A. and Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK 2007.
[4] Qian Wang. Compact k-spendable E-cash with anonymity control based offline TTP. International Journal of Innovative Computing, Information and Control Volume 7, Number 1, January 2011 pp. 459 - 469
[5] Sarkisov A.B, Makarova A. V., Kalmykov M. I. 2014. Extension of methods of protection of systems of electronic commerce on the basis of modular algebraic diagrams,

Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki. 2014. № 2 (151). pp. 218 - 225. (in Russian).

[6] Kalmykov I.A., Dagaeva O.I. Naumenko D.O., Vel'c O.V. The systems concept to application of pseudorandom functions in systems of information security, Izvestija JuFU. Tehnicheskie nauki, Taganrog: TRTU, 2013 g. №12, pp. 228-234

[7] Pashincev V.P., Kalmykov I.A., Vel'c O.V Methods of protection of the transmitted data for systems of remote monitoring and control of high-tech objects, Vestnik Severo-Kavkazskogo federal'nogo universiteta. 2014. № 4 (43). pp. 38-43

[8] Kalmykov Igor Anatolyevich, Katkov Konstantin Aleksandrovich, Naumenko Daniil Olegovich, Artem Bronislavovich Sarkisov, Alena Vasilyevna Makarova, 2014. Parallel modular technologies in digital signal processing // Life Science Journal 2014; 11 (11s) pp. 435 - 438. http://www.lifesciencesite.com

[9] Gordenko D.V., Rezen'kov D. N., Sarkisov A. B., 2014. Methods and algorithms of reconfiguration of not positional computing structures for support of fail safety of special processors. Stavropol', Izdatel'stvo Fabula. 2014. – 180 p.

[10] Kalmykov, I.A. Mathematical models of the neural network fault-tolerant computing means functioning in polynomial class system of residues. Pod red. N.I. Chervjakova – M: Fizmatlit, 2005. - 276 p.

[11] Yong Soo Cho, Jaekwon Kim, Won, Young, Chung G., 2010. Kang MIMO-OFDM Wireless Communications with MATLAB, - WILEY.2010

[12] T. Shahana, B. Jose, R. James, K. Jacob, and S. Sasi, 2008. RRNS-convolutional encoded concatenated code for ofdm based wireless communication. In Networks, 2008. 16th IEEE International Conference on, dec. 2008, pp. 1–6.