УДК 681.3

УВЕЛИЧЕНИЕ КОРРЕКТИРУЮЩИХ СПОСОБНОСТЕЙ МОДУЛЯРНОГО ПОЛИНОМИАЛЬНОГО КОДА

Стрижков Н.С., Калмыков М.И.

ФГАОУ ВПО «Северо-кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Параллельные вычисления нашли широкое применение в областях цифровой обработки сигналов (ЦОС). Однако при этом снижается вероятность безотказной работы вычислительного устройства. Чтобы повысить надежность работы спецпроцессора ЦОС предлагается использовать избыточные модулярные полиномиальные коды. В работе предлагается алгоритм, позволяющий повысить корректирующие способности этих кодовых конструкций полиномиальной системы классов вычетов (ПСКВ). Благодаря этому алгоритму модулярный полиномиальный код, имеющий два контрольных основания, способен исправлять все двукратные ошибки. Данное свойство достигается за счет преодоления коллизий, возникающих при обнаружении и коррекции ошибок.

Ключевые слова: остатки, полиномиальная система классов вычетов, корректирующие способности кода, обнаружение и коррекция ошибок

INCREASE CORRECTING CAPABILITY MODULAR POLYNOMIAL CODE

Strizhkov N.S., Kalmykov M.I.

North-caucasian federal university, Stavropol, e-mail: kia762@yandex.ru

Parallel computing have been widely applied in the fields of digital signal processing (DSP) . However, it reduces the probability of failure of a computing device. To improve the reliability of special processor DSP is proposed to use the redundant modular polynomial codes. In this paper, we propose an algorithm that allows to increase the ability of these corrective code designs polynomial system of residue classes (PSKV). Thanks to this modular polynomial algorithm code having two control base, capable of correcting all errors twofold. This property is achieved by addressing collisions that occur when the detection and correction of errors

Keywords: residues, polynomial system of residue classes, the coefficients of the generalized polyadic notations, detection and correction of errors

Применение методов цифровой обработки, которые характеризуются обработкой значительных объемов информации в реальном масштабе времени, делает целесообразным разработку специализированных процессоров (СП) для их решения. Для обеспечения высокой скорости обработки данных в работах [1, 2] предлагается использовать модулярные арифметические системы. Применение данных систем позволяет повысить скорость выполнения операций сложения, вычисления и умножения по модулю за счет распараллеливания на уровне операций. Очевидно, что усложнение структуры СП ЦОС приводит к увеличению числа отказов, возникающих во время работы вычислительных устройств. Для решения данной проблемы необходимо разработать алгоритм поиска и коррекции ошибок, который позволил бы обнаруживать и корректировать ошибки, которые возникают в процессе функционирования непозиционного СП ЦОС. При этом данный алгоритм должен обеспечивать максимальную корректирующую способность.

Постановка задачи исследований

В настоящее время модулярные арифметические модулярные системы нашли широкое применение в различных сферах, связанных с информационными технологиями. В работах [1-4] доказана целесообразность использования модулярных кодов при реализации методов цифровой обработки сигналов. Широкое применение модулярные алгебраические системы нашли в сфере обеспечения защиты информации от несанкционированного доступа (НСД). Так в работах [5, 6] показана возможность применения модулярной арифметики в криптографических системах, использующих полиномиальную систему классов вычетов. В работе [7] рассмотрены вопросы использования модулярной псевдослучайной функции повышенной эффективности в электронных коммерческих системах. Использование модулярных алгебраических структур позволяет обеспечить требуемый уровень защиты информации от НСД.

Кроме отмеченных выше сфер применения, модулярные алгебраические системы целесообразно использовать для реализации операций поиска и коррекции ошибок, возникающих в процессе функционирования непозиционных спецпроцессоров. Так в работах [8-10] приведены алгоритмы, которые позволяют провести обнаружение

и коррекцию ошибок в полиномиальной системе классов вычетов. Основным недостатком данных систем, является то, что при наличии двух контрольных оснований ПСКВ система способна исправлять только однократные ошибки. В работе предлагается алгоритм, позволяющий повысить корректирующие способности полиномиальных кодов.

В полиномиальной системе классов вычетов в качестве оснований системы используются неприводимые полиномы $p_i(z)$, где $i = 1, 2, ..., n$. В этом случае любой полином $A(z)$, удовлетворяющий условию

$$\deg A(z) < \deg P(z), \qquad (1)$$

где $P(z) = \prod_{i=1}^{n} p_i(z)$ – рабочий диапазон системы, $\deg P(z)$ – степень полинома, можно однозначно представить в виде набора остатков

$$A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)), \qquad (2)$$

где $\alpha_i(z) \equiv \mathrm{A(z)} \bmod \mathrm{p_i}(z); i = 1, 2, ..., n.$

Для реализации процесса обнаружения и исправления ошибок в модулярном коде полинома $A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z))$ вводят избыточность. С этой целью выбирается одно контрольное основание $p_{n+1}(z)$, удовлетворяющее условию

$$\deg p_{n+1}(z) \geq \deg p_n(z). \qquad (3)$$

В прототипе доказано, что используя данное контрольное основание для вычисления двух проверочных остатков

$$\alpha_{n+1}(z) = \sum_{i+1}^{n} \alpha_i(z), \qquad (4)$$

$$\alpha_{n+2}(z) = \sum_{i+1}^{n} (i(z) \cdot \alpha_i(z)) \bmod p_{n+1}(z), \qquad (5)$$

где $i(z)$ – полиномиальная форма i-го порядкового номера, $\sum$ – суммирование по модулю два, можно однозначно исправить однократную ошибку.

Под однократной ошибкой понимается искажение одного разряда в кодовой комбинации, представленной равенством (2).

При работе данное устройство обрабатывает n информационных остатка $\alpha_1(z) \div \alpha_n(z)$ и два контрольных остатка $\alpha_{n+1}(z)$ и $\alpha_{n+2}(z)$.

Для обнаружения ошибки в переданной кодовой комбинации вычисляются значения

$$\alpha^*_{n+1}(z) = \sum_{i+1}^{n} \alpha_i(z), \qquad (6)$$

$$\alpha^*_{n+2}(z) = \sum_{i+1}^{n} (i(z) \cdot \alpha_i(z)) \bmod p_{n+1}(z). \qquad (7)$$

Полученные значения $\alpha^*_{n+1}(z)$ и $\alpha^*_{n+2}(z)$ используются для вычисления синдрома ошибки согласно

$$\delta_1(z) = \alpha_{n+1}(z) \oplus \alpha^*_{n+1}(z), \qquad (8)$$

$$\delta_2(z) = \alpha_{n+2}(z) \oplus \alpha^*_{n+2}(z), \qquad (9)$$

где $\oplus$ – суммирование по модулю два.

Если синдром ошибки $\delta_1(z) = 0$ и $\delta_2(z) = 0$, то данная комбинация не содержит ошибки. В противном случае, когда $\delta_1(z) \neq 0$ и $\delta_2(z) \neq 0$, принятая комбинация является запрещенной, т.е. ошибочной. По величине $\delta_1(z)$ и $\delta_2(z)$ можно провести коррекцию однократной ошибки.

В табл. 1 приведены значения синдромов $\delta_1(z)$ и $\delta_2(z)$, а также соответствующие им константы ошибки для рабочих оснований $p_1(z) = z + 1$, $p_2(z) = z^2 + z + 1$, $p_3(z) = z^4 + z^3 + z^2 + z + 1$ и контрольного основания $p_4(z) = z^4 + z + 1$.

Таблица 1

Синдромы ошибки в коде ПСКВ

$\delta_1(z)$	$\delta_2(z)$	константа ошибки Δконст
0	0	(0, 0, 0, 0, 0)
1	1	(1, 0, 0, 0, 0)
1	z	(0, 1, 0, 0, 0)
z	z^2	(0, z, 0, 0, 0)
1	z+1	(0, 0, 1, 0, 0)
z	$z^2 + z$	(0, 0, z, 0, 0)
z^2	$z^3 + z^2$	(0, 0, z^2, 0, 0)
z^3	$z^3 + z + 1$	(0, 0, z^3, 0, 0)

Однако, используя два контрольных остатка $\alpha_{n+1}(z)$ и $\alpha_{n+2}(z)$, можно исправить и двукратные ошибки, т.е. ошибки, произошедшие в двух разрядах комбинации $A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_{n+1}(z),\alpha_{n+2}(z))$ одновременно.

В табл. 2 приведены значения синдромов ошибки $\delta_1(z)$ и $\delta_2(z)$ при всех возможных двукратных ошибках по рабочим основаниям $p_1(z)=z+1$, $p_2(z)=z^2+z+1$, $p_3(z)=z^4+z^3+z^2+z+1$, в которых произошла коллизия, т.е. совпадение.

Таблица 2

Коллизии при двукратных ошибках в коде ПСКВ

№ п/п	Отказавший разряд 1-го основания	Отказавший разряд 2-го основания	δ_1	δ_2	Δ кор
1	$\alpha_1^0(z)=1$	$\alpha_2^1(z)=z$	$z+1$	z^2+1	коллизия
2	$\alpha_1^0(z)=1$	$\alpha_3^0(z)=1$	0	z	коллизия
3	$\alpha_1^0(z)=1$	$\alpha_3^1(z)=z$	$z+1$	z^2+z+1	коллизия
4	$\alpha_2^1(z)=z$	$\alpha_3^0(z)=1$	$z+1$	z^2+z+1	коллизия
5	$\alpha_2^1(z)=z$	$\alpha_3^1(z)=z$	0	z	коллизия
6	$\alpha_3^0(z)=1$	$\alpha_3^1(z)=z$	$z+1$	z^2+1	коллизия

Проведенный анализ табл. 2 показывает, что совпадение пар значений $\delta_1(z)$ и $\delta_2(z)$ не произошло, за исключением совпадения строк 1 и 4, 2 и 5, 3 и 6. Это означает, что устройство способно корректировать двукратные ошибки за исключением отмеченных совпадающих строк.

Чтобы обеспечить процедуру коррекции результата в условиях коллизии (совпадение синдрома $\delta_1(z)$ и $\delta_2(z)$) в устройство введены блок управления, второй блок памяти, блок устранения коллизии.

Функциональная схема устройства представлена на рис. 1. Она включает: регистр 1, вход 2, блок устранения коллизии 3, модуль вычисления синдрома ошибки 4, содержащий первый блок вычисления ошибки 5, второй блок вычисления синдрома ошибки 6, блок управления 7, первый блок памяти 8, второй блок памяти 9, сумматор 10, выход устройства 11.

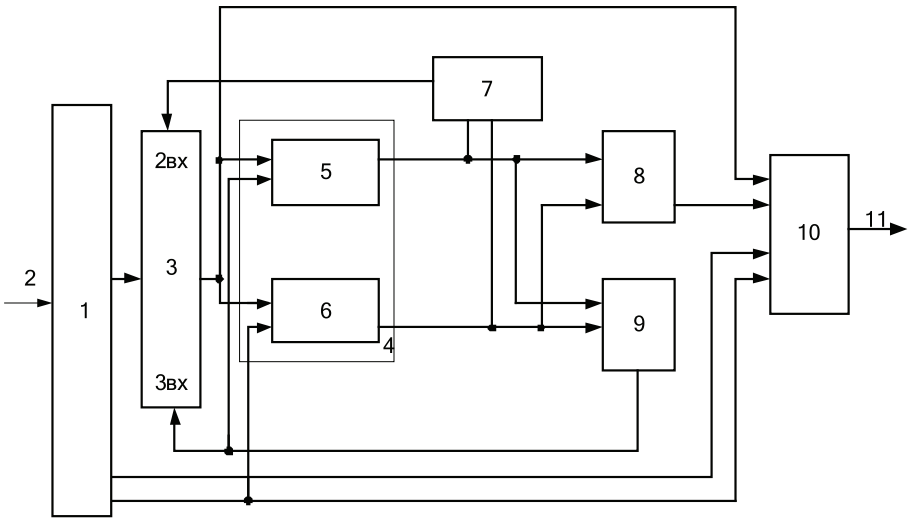

Рис. 1. Функциональная схема устройства, позволяющего увеличить корректирующие способности кодов ПСКВ

Устройство работает следующим образом: на вход 2 устройства поступает модулярный код полинома $A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_{n+1}(z),\alpha_{n+2}(z))$. Контролируемая комбинация записывается в регистр 1. На первый вход блока 3 устранения коллизии с первого выхода регистра 1 поступает значение $(\alpha_1(z),\alpha_2(z),...,\alpha_n(z))$. Если коллизия не обнаружена блоком управления 7, то на второй вход блока 3 поступает управляющая комбинация y=0. Одновременно с выхода второго блока 9 памяти на третий вход блока 3 устранения коллизии поступает четырехразрядная комбинация $x=0000$. Благодаря этому входная комбинация не изменяется и с выхода блока 3 устранения коллизии подается на первый вход первого блока 5 и второго блока 6 вычисления синдрома ошибки, входящих в состав модуля 4 вычисления синдрома ошибки, а также на первый вход сумматора 10.

На второй вход первого блока 5 вычисления синдрома ошибки подается с второго выхода регистра 1 значение первого контрольного остатка $\alpha_{n+1}(z))$. Блок 5 реализует выражение (8).

На второй вход второго блока 6 вычисления синдрома ошибки подается с третьего выхода регистра 1 значение второго контрольного остатка $\alpha_{n+2}(z))$. Данный блок 6 реализует выражение (9).

Величины $\delta_1(z)$ и $\delta_2(z)$ в двоичном коде поступают на соответствующие входы первого 8 и второго 9 блоков памяти и блок управления 7.

Если коллизия отсутствует, а это соответствует условию, когда контролируемая комбинация

$$A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_{n+1}(z),\alpha_{n+2}(z))$$

не содержит ошибки или имеет однократную ошибку или двухкратную, за исключением когда ошибка одновременно произошла в комбинациях $\alpha_1^0(z)$ и $\alpha_2^1(z)$; $\alpha_1^0(z)$ и $\alpha_3^0(z)$; $\alpha_1^0(z)$ и $\alpha_3^1(z)$; $\alpha_2^1(z)$ и $\alpha_3^0(z)$; $\alpha_2^1(z)$ и $\alpha_3^1(z)$; $\alpha_3^0(z)$ и $\alpha_3^1(z)$, где $\alpha_i^j(z)$ – j-й разряд i-го канала, то с выхода блока управления 7 поступает управляющий сигнал $y=0$ на второй вход блока 3 устранения коллизии.

Если однократная ошибка произошла в нулевом разряде первого основания, в $\alpha_1^0(z)$ т. е. когда значение синдрома ошибки $\delta_1(z)=1$ и $\delta_2(z)=1$, то с выхода второго блока 9 памяти снимается комбинация x=1000 которая подается на третий вход блока 3 устранения коллизии.

Если однократная ошибка произошла в первом разряде второго основания $\alpha_2^1(z)$, т. е. когда значение синдрома ошибки $\delta_1(z)=z$ и $\delta_2(z)=z^2$, то с выхода второго блока 9 памяти подается на третий вход блока 3 устранения коллизии комбинация x=0100.

Если однократная ошибка произошла в нулевом разряде третьего основания $\alpha_3^0(z)$, то есть когда значение синдрома ошибки $\delta_1(z)=1$ и $\delta_2(z)=z+1$, то с выхода второго блока 9 памяти подается на третий вход блока 3 устранения коллизии комбинация $x=0010$.

Если однократная ошибка произошла в первом разряде третьего основания $\alpha_3^1(z)$, т. е. когда значение синдрома ошибки $\delta_1(z)=z$ и $\delta_2(z)=z^2+z$, то с выхода второго блока 9 памяти подается на третий вход блока 3 устранения коллизии комбинация $x=0001$.

В зависимости от величины $\delta_1(z)$ и $\delta_2(z)$ с выхода первого блока 8 памяти выдается соответствующая константа ошибки Δконс. Это значение поступает в сумматор 10, где суммируется со значением комбинации $A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_{n+1}(z),\alpha_{n+2}(z))$, которая подается в параллельном коде на первый, третий и четвертый входы сумматора 10. Исправленное значение $A(z)$ с выхода сумматора 10 подается на выход 11 устройства.

При возникновении коллизии, это соответствует ситуации, когда с выходов блоков 5 и 6 вычисления синдрома ошибки подаются значения $\delta_1(z)=z+1$ и $\delta_2(z)=z^2+1$, $\delta_1(z)=0$ и $\delta_2(z)=z$, $\delta_1(z)=z+1$ и $\delta_2(z)=z^2+z+1$, то с выхода блока управления 7 на второй вход блока 3 поступает управляющий сигнал $y=1$.

В результате контролируемая комбинация модулярного кода $A(z)=(\alpha_1(z),\alpha_2(z),...,\alpha_{n+1}(z),\alpha_{n+2}(z))$ будет содержать только однократную ошибку. Эта ошибка будет обнаружена в модуле 4 вычисления синдрома по значениям $\delta_1(z)$ и $\delta_2(z)$. Эти значения подаются на входы первого блока 8 памяти, с выхода которого выдается Δкор, что позволяет ис-

править вторую ошибку в контролируемой комбинации.

Проведенные исследования показали, что предлагаемый алгоритм работы устройства позволяет повысить корректирующие способности кода ПСКВ с двумя контрольными основаниями.

Вывод. Использование модулярного полиномиального кода позволяет не только повысить скорость выполняемых вычислений, но и проводить процедуры поиска и коррекции ошибок, которые возникают в процессе работы спецпроцессоров. В ходе проведенных исследований был разработан алгоритм, позволяющий повысить корректирующие способности непозиционных кодов ПСКВ. Благодаря данному алгоритму избыточный код ПСКВ с двумя контрольными основаниями может исправлять все двукратные ошибки.

СПИСОК ЛИТЕРАТУРЫ

1. Калмыков И.А., Резеньков Д.Н., Тимошенко Л.И. Непозиционное кодирование информации в конечных полях для отказоустойчивых спецпроцессоров цифровой обработки сигналов // Инфокоммуникационные технологии. – 2007. – Т.5. – №3. – С.36-39.

2. Калмыков И.А., Емарлукова Я.В., Зиновьев А.В. Высокоскоростные систолические отказоустойчивые процессоры цифровой обработки сигналов для инфотелекоммуникационных систем// Инфокоммуникационные технологии. Самара. – 2009. – №2. – С. 31-37.

3. Калмыков И.А., Воронкин Р.А, Резеньков Д.Н., Емарлукова Я.В. Генетические алгоритмы в системах цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. – 2011. – Вып. 5. – С. 20-27.

4. Чипига А.Ф., Калмыков И.А. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности// Наука. Инновации. Технологии. – 2004. – Т.38. С. 46.

5. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О. А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. – 2010. – Т.8. № 2. – С. 14-22.

6. Калмыков И.А., Чипига А.Ф., Барильская А.В., Кихтенко О. А. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем // Известия Южного федерального университета. Технические науки. – 2009. – Т.100. № 11. – С.210-220.

7. Калмыков И.А.,. Дагаева О.И., Разработка псевдослучайной функции повышенной эффективности // Известия Южного федерального университета. Технические науки. – 2011. – Т.125. № 12. – С.160-169.

8. Калмыков И.А., Лободин М.В., Чипига А.А., Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов // Патент России № 2301441. 01.08.2005.

9. Калмыков И.А., Петлеванный С.В., Сагдеев А.К., Емарлукова Я.В. Устройство для преобразования числа из полиномиальной системы классов вычетов в позиционный код с коррекцией ошибки // Патент России № 2309535. 31.03.2006.

10. Калмыков И.А., Гахов В.Р., Емарлукова Я.В. Устройство обнаружения и коррекции ошибок в кодах полиномиальной системы классов вычетов на основе нулевизации // Патент России № 2300801. 30.06.2005.