УДК 681.3

АЛГОРИТМЫ ОБНАРУЖЕНИЯ И КОРРЕКЦИИ ОШИБОК В МОДУЛЯРНЫХ ПОЛИНОМИАЛЬНЫХ КОДАХ

Барсагаев А.А., Калмыков М.И.

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

В работе рассмотрены вопросы, связанные с анализом корректирующих способностей модулярных полиномиальных кодов (МПК). Данные коды позволяют осуществлять обработку данных в реальном масштабе времени за счет использования малоразрядных данных. При этом обработка информации осуществляется параллельно по вычислительным трактам и независимо друг от друга. Такое свойство МПК позволяет осуществлять процедуры поиска и коррекции ошибок. Для повышения корректирующих способностей кодов в МПК вводят дополнительные контрольные основания. С целью определения местоположения и глубины ошибки используются позиционные характеристики. В статье представлен алгоритм поиска и коррекции ошибок с использованием псевдоортогональных базисов модулярных полиномиальных кодов.

Ключевые слова: модулярные полиномиальные коды, параллельные вычисления, остатки, псевдоортогональные базисы, коррекция ошибок.

ALGORITHMS OF DETECTION AND CORRECTION OF ERRORS IN MODULAR POLYNOMIAL CODES

Barsagaev A.A., Kalmykov M.I.

Federal state Autonomous educational institution higher professional education «North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

The article considers the issues associated with the analysis of corrective abilities modular- polynomial codes (MPC). These codes allow to process data in real-nom-time through the use of data. The processing of information on the parallel computing highway and independently. Such properties in the MPC allows the procedure of search and correction of errors. To increase the influence-stimulating abilities codes in the MPC introduce additional control grounds. With the purpose of definition of the location and depth of the error using positional characteristics. In the article presented flax search algorithm and error correction using псевдоортогональных bases of modular polynomial codes.

Keywords: modular polynomial codes, parallel computing, the remains of the псевоортогональные bases, error correction.

Введение

В последние годы цифровая обработка сигналов (ЦОС) занимает доминирующее положение в системах и средствах передачи и обработки информации в связи с неоспоримыми достоинствами – точность, гибкость и высокая скорость обработки. Кроме того, с развитием средств вычислительной техники системы ЦОС становятся все дешевле и компактнее. Эффективность ЦОС полностью определяется объемом вычислений, которые получаются при реализации математической модели процесса цифровой обработки сигнала с помощью специализированного процессора (СП). Снижение объема вычислений приводит к уменьшению аппаратурных затрат при реализации систем ЦОС или к повышению производительности вычислительного устройства. Таким образом, выбор алгебраической системы оптимальной с точки зрения минимума объема вычислений при реализации методов ЦОС является актуальной и важной.

Постановка задачи исследований

Как правило, в подавляющем большинстве приложений задачи ЦОС сводится к нахождению значений ортогонального преобразования конечной реализации сигнала для большого числа точек, что предопределяет повышенные требования к скорости обработки и разрядности вычислительного устройства. Решить данную проблему можно за счет перехода от одномерных вычислений к многомерным. В основу данного преобразования положена китайская теорема об остатках (КТО) [1-5].

Особое место среди таких систем занимает модулярная полиномиальная система класса вычетов, с помощью которых возможна организация ортогональных преобразований сигналов в расширенных полях Галуа $GF(p^v)$. Если исходное число A представить в полиномиальной форме, а в качестве оснований выбрать минимальные многочлены поля Галуа, то справедливо

$$A(z) = (\alpha_1(z), \alpha_2(z).., \alpha_n(z)), \quad (1)$$

где $\alpha_i(z) \equiv A(z \bmod p_i(z)$; $p_i(z)$ – минимальный многочлен.

Применение модулярных полиномиальных кодов позволяет свести операции в кольце полиномов к соответствующим операциям над остатками [1-6]. В этом случае

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

где

$$A(z)=\left(\alpha_1(z)\ \alpha_2(z),...,\alpha_n(z)\right),$$

$$B(z)=\left(\beta_1(z)\ \beta_2(z),...,\beta_n(z)\right)-$$

модулярный код в кольце полиномов;

$\alpha_l(z)\equiv A(z)\,mod\ p_l(z)$;

$\beta_l(z)\equiv \hat{A}(z)\,mod\ p_l(z)$;

$\otimes$ – операции сложения, вычитания и умножения в *GF(p); l = 1, ...,n*.

Таким образом, основным достоинством непозиционных кодов является, то, что данные представляются в виде малоразрядных остатков, которые обрабатываются по параллельным вычислительным трактам. Это позволяет повысить скорость вычислений, что и предопределяет интерес к полиномиальным непозиционным кодам в различных областях применения [1-6].

В работах [1-5] предлагается для эффективной реализации ортогональных преобразований с высокой точностью и скоростью вычислений реализация дискретного преобразования Фурье (ДПФ) в кольце полиномов. В этом случае, если имеется кольцо полиномов *P(z)*, с коэффициентами в виде элементов поля *GF(p),* то данное кольцо разлагается в сумму

$$P(z)=P_1(z)+P_2(z)+...+P_n(z), \quad (2)$$

где $P_l(z)$ – локальное кольцо полиномов, образованное неприводимым полиномом $p_l(z)$ над полем *GF(p); l=1, ..., n*.

При этом в кольце полиномов можно организовать ортогональное преобразование, представляющее собой полиномиальное ДПФ, вида

$$X_l^k(z)=\sum_{n=0}^{d-1}x_l^n(z)\beta_l^{kn}(z), \quad (3)$$

где $\{\ X_l^k(z), x_l^n(z), \beta_l^{kn}(z)\ \}\in P_l(z)$, *l = 1,2,...,m; k = 0,1,...,d-1*.

При этом должны выполняться следующие условия:

1. $\beta_l(z)$ – первообразный элемент порядка *d* для локального кольца $P_l(z)$.

2. *d* имеет мультипликативный обратный элемент d^*.

Если отмеченные условия выполняются, то получается циклическая группа, которая имеет порядок *d*. В этом случае ортогональное преобразование является полиномиальным ДПФ для кольца вычетов *P(z)* если существуют преобразования над конечным кольцом $P_l(z)$.

Поэтому ДПФ над $P_l(z)$ можно обобщить над кольцом *P(z),* если конечное кольцо $P_l(z)$ содержит корень *d*-ой степени из единицы и *d* имеет мультипликативный обратный элемент d^*, такой что справедливо

$$d^*d=p^{\nu}-1. \quad (4)$$

Основным достоинством системы класса вычетов является сравнительная простота выполнения модульных операций (сложения, вычитания, умножения). Формальные правила выполнения таких операций в МПК позволяют существенно повысить скорость вычислительных устройств ЦОС [5].

Кроме модульных операций, позволяющих повысить скорость обработки информации, модулярные коды позволяют обнаруживать и исправлять ошибки, возникающие в процессе функционирования СП. Если в качестве рабочих оснований выбрать *k* минимальных многочленов МПК *(k<n)*, то данные основания определяют рабочий диапазон

$$P_{раб}(z)=\prod_{i=1}^{k}p_i(z). \quad (5)$$

Если $A(z)\in P_{раб}(z)$, то такой полином считается разрешенным и не содержит ошибок. В противном случае, полином, представленный в модулярном полиномиальном коде, содержит ошибки [6-10].

Для определения местоположения и глубины ошибки в полиномиальной системе классов вычетов используются позиционные характеристики. В работе [9] представлен алгоритм вычисления такой характеристики как интервальный номер. Синдром ошибки для полиномиального кода вычисляется в работе [8]. В работе [7] показана математическая модель поиска ошибочного основания с использованием алгоритма нулевизации. Структура устройства спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов приведена в работе [10].

Одной из характеристик, использующемой при выполнении процедур поиска и коррекции ошибок в модулярных кодах, является след полинома. Для получения данной характеристики используются псевдоортогональные полиномы. Они представляют собой ортогональные полиномы, у которых нарушена ортогональность по нескольким основаниям. Известно, что если в псевдоортогональных полиномах нарушена ортогональность по контрольным основаниям, то данные полиномы являются ортого-

нальными полиномами безизбыточной системы оснований полиномиальной системы классов вычетов.

Для получения псевдоортогональных полиномов проведем расширение системы оснований $p_1(z), ..., p_k(z)$ на r контрольных оснований $p_{k+1}(z), ..., p_{k+r}(z)$ и представим ортогональные полиномы в виде:

Следовательно, справедливо

$$\begin{cases} \alpha_{k+1}(z) = \sum_{j=1}^{k} \gamma_{k+1}^{j}(z) \bmod p_{k+1}(z): \\ \vdots \\ \alpha_{k+r}(z) = \sum_{j=1}^{k} \gamma_{k+r}^{j}(z) \bmod p_{k+r}(z). \end{cases} \quad (9)$$

$$\begin{cases} \alpha_1(z)B_1^*(z) \bmod P_{раб}(z) \equiv (\alpha_1(z),0,...,0,\gamma_{k+1}^1(z),...,\gamma_{k+r}^1(z)); \\ \alpha_2(z)B_2^*(z) \bmod P_{раб}(z) \equiv (0,\alpha_2(z),...,0,\gamma_{k+1}^2(z),...,\gamma_{k+r}^2(z)); \\ \vdots \\ \alpha_k(z)B_k^*(z) \bmod P_{раб}(z) \equiv (0,0,...,\alpha_k(z),\gamma_{k+1}^k(z),...,\gamma_{k+r}^k(z)). \end{cases} \quad (6)$$

Выражение (6) определяет значения псевдоортогональных полиномов, у которых нарушена ортогональность по контрольным основаниям.

Согласно китайской теореме об остатках

$$A(z) = \sum_{i=1}^{k+r} a_i(z)B_i(z) \bmod P(z), \quad (7)$$

полином можно представить в виде:

$$A(z) = (\alpha_1(z),0,...,0) + (0,\alpha_2(z),...,0) + ... + (0,0,...,\alpha_k(z)) . \quad (8)$$

Таким образом, на основании (9) и воспользовавшись значениями псевдоортогональных полиномов, определяемых равенством (6), можно вычислить значения остатков по контрольным основаниям $\alpha_{k+1}^*(z),...,\alpha_{k+r}^*(z)$ согласно

$$\begin{cases} \alpha_{k+1}^*(z) = \sum_{j=1}^{k} \gamma_{k+1}^{j}(z) \bmod p_{k+1}(z): \\ \vdots \\ \alpha_{k+r}^*(z) = \sum_{j=1}^{k} \gamma_{k+r}^{j}(z) \bmod p_{k+r}(z). \end{cases} . \quad (10)$$

Затем на основании полученных значений и значений, поступающих на вход устройства коррекции ошибок, можно определить синдром ошибки согласно выражения

$$\begin{cases} \theta_{k+1}(z) = \left|\alpha_{k+1}(z) - \alpha_{k+1}^*(z)\right|_{p_{k+1}(z)}^{+} = \left(\alpha_{k+1}(z) - \sum_{j=1}^{k} \gamma_{k+1}^{j}(z)\right) \bmod p_{k+1}(z): \\ \vdots \\ \theta_{k+r}(z) = \left|\alpha_{k+r}(z) - \alpha_{k+r}^*(z)\right|_{p_{k+r}(z)}^{+} = \left(\alpha_{k+r}(z) - \sum_{j=1}^{k} \gamma_{k+r}^{j}(z)\right) \bmod p_{k+r}(z). \end{cases} \quad (11)$$

Тогда каждое слагаемое выражения (4) представляет собой

$$(0,0,...,\alpha_i(z),...,0) \equiv \alpha_i(z)B_i^*(z) \bmod P_{раб}(z), \quad (9)$$

где $B_i^*(z)$ – ортогональный базис безизбыточной системы оснований МПК.

Подставив выражение (6) в равенство (8), и учитывая, что в процессе выполнения операции не бывает выход за пределы $P_{раб}(z)$, получаем

$$A(z) = (\alpha_1(z),0,...,0,\gamma_{k+1}^1(z),...,\gamma_{k+r}^1(z) + (0,\alpha_2(z),...,0,\gamma_{k+1}^2(z),...,\gamma_{k+r}^2(z) + ... + (0,0,...,\alpha_k(z),\gamma_{k+1}^k(z),...,\gamma_{k+r}^k(z)).$$

Если разность равна нулю, т.е. $\theta_{k+1}(z) = 0,...,\theta_{k+r}(z) = 0$, то исходный полином является разрешенным и не содержит ошибки. В противном случае модулярная комбинация является запрещенной. Тогда в зависимости от величины синдрома ошибки осуществляется коррекция ошибки, т.е.

$$A(z) = (\alpha_1(z),...,\alpha_i'(z),...,\alpha_k(z) + (0,...,\Delta\alpha_i(z),...,0) = (\alpha_1(z),...,\alpha_i'(z) + \Delta\alpha_i(z),...,\alpha_k(z) = (\alpha_1(z),...,\alpha_i(z),...,\alpha_k(z) \quad (12)$$

где $(0,...,\Delta\alpha_i(z),...,0)$ – вектор ошибки модулярного кода; $\Delta\alpha_i(z)$ – глубина ошибки по i-му модулю МПК.

В работе [6] представлена структура устройства для преобразования числа из полиномиальной системы классов вычетов в позиционный код с коррекцией ошибки, в процессе функционирования которого используется данный алгоритм. Следует отметить, что этот алгоритм поиска и коррекции ошибок позволяет осуществить поиск и коррекцию всех однократных ошибок с использованием двух контрольных оснований и 90 процентов двоичных ошибок.

Вывод

В работе показана возможность осуществления цифровой обработки сигналов с использованием математической модели ЦОС, обладающей свойством кольца и поля. Применение полиномиальных кодов позволяет повысить скорость обработки данных за счет применения малоразрядных остатков и их параллельной архитектуре вычислений. Кроме того, МПК могут использоваться для повышения отказоустойчивости вычислительных систем. В работе рассмотрен алгоритм вычислений позиционной характеристики на основе ортогональных базисов, у которых нарушена ортогональность по контрольным основаниям.

Список литературы

1. Бережной В.В., Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Нейросетевая реализация в полиномиальной системе классов вычетов операций ЦОС повышенной разрядности // Нейрокомпьютеры: разработка и применение. – 2004. – № 5-6. – С. 94.

2. Бережной В.В., Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Архитектура отказоустойчивой нейронной сети для цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. – 2004. – № 12. – С. 51-57.

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

4. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Нейросетевая реализация в полиномиальной системе классов вычетов операций ЦОС повышенной разрядности // Нейрокомпьютеры: разработка и применение. – 2004. – № 5-6. – С. 94.

5. Калмыков И.А., Чипига А.Ф. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности // Вестник Ставропольского государственного университета. – 2004. – Т.38. – С. 46.

6. 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. Бюл. № 30 от 27.10.2007.

7. Калмыков И.А., Гахов В.Р., Емарлукова Я.В. Устройство обнаружения и коррекции ошибок в кодах полиномиальной системы классов вычетов // Патент России № 2300801. 30.06.2005. Бюл. № 16 от 10.06.2007.

8. Хайватов А.Б., Калмыков И.А. Математическая модель отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов // Инфокоммуникационные технологии. – 2007. – Т.5. – №3. – С.39-42.

9. Червяков Н.И., Калмыков И.А., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронной сети для коррекции ошибок в непозиционном коде расширенного поля Галуа // Нейрокомпьютеры: разработка и применение. – 2003. – № 8-9. – С. 10-17.

10. Чипига А.А., Калмыков И.А., Лободин М.В. Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов // Патент России № 2301441. Бюл. № 17 от 20.06.2007.