Применение полиномиальной системы классов вычетов для коррекции ошибок в модулярных кодах

Калмыков И.А., Руденко А.С.

Северо-Кавказский государственный технический университет

г. Ставрополь, kia762@yandex.ru, mail_to_cooper@mail.ru

Проблема исследований: Параллельная обработка данных в вычислительных трактах по модулям системы полиномиальной системы классов вычетов (ПСКВ) может служить базисом в реализации процедур коррекции ошибок.

Решение проблемы исследований:

В последние годы в вычислительной технике, в частности цифровой обработке сигналов (ЦОС), появилась практическая потребность в аппаратной реализации алгоритмов, обладающих повышенной вычислительной сложностью. Для обеспечения обработки сигналов в реальном масштабе времени в работе [1] предложено использовать полиномиальную систему класса вычетов (ПСКВ). В то же время высокие требования предъявляются к надежности работы спецпроцессоров (СП) ЦОС. Из существующих подходов к решению задачи построения отказоустойчивых вычислительных структур все большее применение находят методы теории кодирования.

Целенаправленное введение избыточности позволяет обнаружить и исправить ошибки, возникающие в результате отказов элементов вычислительных трактов СП ПСКВ. Если на диапазон возможного изменения кодируемого множества полиномов наложить ограничения, то есть выбрать k из n оснований ПСКВ ($k < n$), то это позволит осуществить разбиение полного диапазона $P_{полн}(z)$ расширенного поля Галуа $GF(p^n)$ на два непересекающихся подмножества. Первое подмножество называется рабочим диапазоном и определяется выражением

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

Многочлен $A(z)$ с коэффициентами из поля $GF(p)$ будет считаться разрешенным в том и только том случае, если он является элементом нулевого интервала полного диапазона $P_{полн}(z)$, то есть принадлежит рабочему диапазону $A(z) \in P_{раб}(z)$. Второе подмножество $GF(p^n)$, определяемое произведением $r = n - k$ контрольных оснований

$$P_{конт}(z)=\prod_{i=k+1}^{k+r} p_i(z), \qquad (2)$$

задает совокупность запрещенных комбинаций. Если $A(z)$ является элементом второго подмножества, то считается, что данная комбинация содержит ошибку. Таким образом, местоположение полинома $A(z)$ относительно подмножеств позволяет однозначно определить, является ли кодовая комбинация $A(z)=(a_1(z),\ a_2(z),\ \ldots,a_n(z))$ разрешенной, или она содержит ошибочные символы.

Рассмотрим корректирующие способности кодов ПСКВ, с одним контрольным основанием. В упорядоченной системе оснований ПСКВ в качестве контрольного выбирается модуль, удовлетворяющий условно

$$ord\ p_i(z) \le ord\ p_{k+1}(z), \text{ где } i = 1, 2, \ldots, k. \qquad (3)$$

Считаем, что если исходные операнды $A(z)=(a_1(z),a_2(z),\ldots,a_{k+1}(z))$ и $B(z)=(b_1(z),b_2(z),\ldots,b_{k+1}(z))$, как и результат выполнения **o** арифметической операции $C(z) = A(z)\,\mathbf{o}\,B(z)$, лежат внутри диапазона $P_{раб}(z)$, то полином $C(z)=(g_1(z),g_2(z),\ldots,g_{k+1}(z))$ не содержит ошибки. В противоположном случае, результат $C(z)$ является ошибочным.

Переход из множества разрешенных комбинаций во множество запрещенных осуществляется в результате искажения значения остатка $g_i(z),\ i=1,\ldots,k+1$ и преобразования его к виду $g_i^*(z) \ne g_i(z)$. Если полином $C(z)$ является элементом рабочего диапазона, то согласно [1], имеем

$$C(z) < P_{полн}(z) / p_{k+1}(z). \qquad (4)$$

Для упорядоченной системы оснований ПСКВ, выбор контрольного основания $p_{k+1}(z)$, удовлетворяющего (3), обеспечивает выполнение

$$P_{полн}(z)/p_i(z) \geq P_{полн}(z)/p_{k+1}(z). \qquad (5)$$

Тогда, на основании (4) справедливо

$$C(z) < P_{полн}(z)/p_i(z). \qquad (6)$$

Но искажение остатка по *i*-ому основанию приводит к тому, что полином *C(z)* не может находиться в интервале $[0, P_{полн}(z)/p_i(z)]$. Следовательно

$$C^*(z) > P_{полн}(z)/p_i(z). \qquad (7)$$

Тогда, исходя из (6), получаем $C^*(z) > P_{полн}(z)/p_{k+1}(z)$. Следовательно, полином *C*(z)* не принадлежит $P_{раб}(z)$, и он содержит ошибку.

Теорема. Если в упорядоченной системе оснований $p_1(z),\ldots,p_{k+1}(z)$ ПСКВ расширенного поля Галуа $GF\ (2^v)$ полином $C^*(z) \notin P_{раб}(z)$, то модулярный код данного полинома содержит как минимум одну ошибку.

Доказательство. Положим, что *C*(z)* не содержит ошибки. Согласно китайской теореме об остатках имеем

$$C^*(z) = \left| g_1(z)B_1(z) + \ldots + g_i^*(z)B_i(z) + \ldots + g_{k+1}(z)B_{k+1}(z) \right|^+_{P_{полн}(z)}. \quad (8)$$

В то же время, согласно теореме, приведенной в [3] существует элемент последовательности $C_{IR}(z)$, который отличается от $C^*(z)$ значением по *i*-ому основанию $g_i^* = g_i + Dg_i(z)$ и принадлежит $P_{раб}(z)$.

$$C^*(z) = \left| g_1(z)B_1(z) + \ldots + g_i(z)B_i(z) + \ldots + g_{k+1}(z)B_{k+1}(z) \right|^*_{P_{полн}(z)}. \quad (9)$$

Следовательно

$$\left\lfloor C^*(z)/P_{раб}(z) \right\rfloor = \left\lfloor C(z)/P_{раб}(z) \right\rfloor. \qquad (10)$$

Подставим (8) и (9) в равенство (10) и, преобразовав их с учетом

$$B_i(z) = m_i(z)P_{полн}(z)/p_i(z) = m_i(z)P_{раб}(z)p_{n+1}(z)/p_i(z), \qquad (11)$$

получаем

$$g_i(z)m_i(z)p_{n+1}(z)/p_i(z) = (g_i(z) + Dg_i(z))m_i(z)p_{n+1}(z)/p_i(z). \qquad (12)$$

Равенство (12) выполняется при условии $g_i(z)=(g_i(z)+Dg_i(z))$, т.е. когда $Dg_i(z)=0$.Но согласно, исходным данным $g_i^*(z)\neq g_i(z)$. Следовательно, *C*(z)* содержит ошибку по *i*-ому основанию полиномиальной системы классов вычетов. Доказательство закончено.

Благодаря представленной теореме, была установлена возможность применения избыточных кодов ПСКВ для процедур поиска и коррекции ошибок.

Литература

1. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2005. - 276 с.

2. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронных сетей для исследования ортогональных преобразований в расширенных полях Галуа/Нейрокомпьютеры: разработка, применение. №6, 2003. с.61-68.

3. Калмыков И.А., Щелкунова Ю.О., Гахов В.Р., Шилов А.А. Математическая модель коррекции ошибок в полиномиальной системе класса вычетов на основе определения корней интервального полинома/Волновые процессы. №5, т.6, Самара, 2003 – С.30-34.

4. Элементы применения компьютерной математики и нейроинформатики/Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.

Работа представлена на заочную электронную конференцию «Прикладные исследования и разработки по приоритетным направлениям науки и техники, 15-20 января 2008г.» Поступила в редакцию 01.07.2008г.