ПРИМЕНЕНИЕ ИЗБЫТОЧНЫХ КОДОВ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ ДЛЯ ПРОЦЕДУР ПОИСКА И КОРРЕКЦИИ ОШИБОК

Резеньков Д.Н.

Ставропольский военный институт связи Ракетных войск

Ставрополь, Россия

В отличие от оптимальных кодов, обладающих минимальной избыточностью, корректирующие коды характеризуются введением дополнительной избыточности. Целенаправленное введение избыточности позволяет обнаружить и исправить ошибки, возникающие в результате отказов элементов вычислительных трактов спецпроцессоров (СП) полиномиальной системы классов вычетов (ПСКВ). [1,2,3]

Если на диапазон возможного изменения кодируемого множества полиномов наложить ограничения, то есть выбрать $к$ из n оснований ПСКВ $(к<n)$, то это позволит осуществить разбиение полного диапазона $P_{полн}(z)$ расширенного поля Галуа $GF(p^v)$ 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 [2]

$$A(z)\in P_{пол}(z),$$

Второе подмножество $GF(p^v)$, определяется 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 двух данных 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, использующих одно контрольное основание [1]. В упорядоченной системе оснований ПСКВ в качестве контрольного основания выбирается модуль, удовлетворяющий условию

$$ord\ p_i(z) \geq ord\ p_{k+1}(z) \qquad (3)$$

где $i=1,2,\ldots,k$

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 арифметической операции в расширенном поле Галуа $GF(p^v)$

C(z)=A(z)◦B(z)

где ◦ - арифметическая операция, лежит внутри диапазона $P_{раб}(z)$, то полином $C(z)=g_1(z),g_2(z),\ldots,g_{k+1}(z)$ не содержит ошибок. В противном случае , результат $C(z)$ является ошибочным.

Переход из множества разрешенных комбинаций ПСКВ во множество запрещенных осуществляется в результате искажения значения остатка $\gamma_i(z)$, $i=1,\ldots,k+1$ и преобразования его к виду $\gamma_i^*(z)\neq\gamma_i(z)$

Заметим, что если полиномом $C(z)$ является элементом рабочего диапазона, то справедливо:

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

В тоже самое время, для упорядоченной системы оснований ПСКВ, выбор контрольного основания $p_{k+1}(z)$, удовлетворяющего условию (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 ПСКВ 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 условия (6), получаем

$C^*(z)> P_{полн}(z)/\ p_{k+1}(z)$

Следовательно, полином $C^*(z)$ не принадлежит рабочему диапазону $P_{раб}(z)$, и он содержит ошибку [3].

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

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

$$C(z)=\left|\ \gamma_1(z)B_1(z)+\ldots+\gamma_i^*(z)B_i(z)+\ldots+\gamma_{k+1}(z)\ B_{k+}1(z)\ \right|^{+}_{\text{Рпол(z)}} \qquad (8)$$

В то же самое время существует элемент последовательности $C_{IR}(z)$, который отличается от $C^*(z)$ значением по i-ому основанию $\gamma_i^* = \gamma_i + \Delta\gamma_i(z)$ принадлежит $P_{раб}(z)$.

$C(z)=\left| \gamma_1(z)B_1(z)+\ldots + y_i(z)B_i(z)+\ldots+y_{k+1}(z)B_{k+1}(z) \right|^{*}_{\text{Рпол(z)}}$ (9) Следовательно

$$[C^*(z)/ P_{раб}(z)]= [C(z)/ P_{раб}(z)] \quad (10)$$

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

$$B_1(z) = m_i(z)P_{полн}(z)/p_i(z) = m_i(z)P_{раб}(z)p_{n+1}(z)/p_i(z), \quad (11)$$

получаем $y_l(z)m_i(z)p_{n+1}(z)/p_i(z) =(\gamma_i +\Delta\gamma_i(z))\, m_i(z)\, p_{n+1}(z)/p_i(z).$ (12)

Равенство (12) выполняется при условии $\gamma_i(z) =(\gamma_i(z) + \Delta \gamma_i(z))$, т.е.

$\Delta \gamma_i(z)=0$

Но согласно, исходным данным $\gamma_i^*(z)\neq\gamma_i(z)$. Следовательно, $C^*(z)$ содержит ошибку по i-ому основанию полиномиальной системы классов вычетов [1].

Таким образом была установлена возможность применения избыточных кодов ПСКВ для процедур поиска и коррекции ошибок. Важнейшим фактом является то, что любое искажение остатка по любому основанию превращает исходный полином в неправильный и тем самым позволяет обнаружить ошибку.

ЛИТЕРАТУРА

1. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе класса вычетов.- М.: ФИЗМАТЛИТ,2005.-274с.

2. 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. – Физика волновых процессов и радиотехнические системы. Том 6, №5, с. 30-34.

3. И.А. Калмыков, Л.И. Тимошенко, Д.Н. Резеньков. Непозиционное кодирование информации в конечных полях для отказоустойчивых спецпроцессоров цифровой обработки сигналов. - Инфокоммуникационные технологии. №3 2007 года, с.36-39.