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.61-68с.

3. Калмыков И.А., Хайватов А.Б., Никульников А.С. Устройство для обнаружения и исправления ошибок в полиномиальной системе класса вычетов. Решение о выдаче патента (№ 2004102274/09(002159). Приоритет от 26.01.2004. Бюл. №19 (II). с.568-569.

ПРИМЕНЕНИЕ НОРМИРОВАННОГО СЛЕДА ПОЛИНОМА ДЛЯ ПРОЦЕДУР ПОИСКА И КОРРЕКЦИИ ОШИБОК В МОДУЛЯРНЫХ КОДАХ

Калмыков И.А.

Северо-Кавказский государственный технический университет, Ставрополь

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет не только повысить скорость работы вычислительных устройств, но и обеспечивать требуемый уровень надежности функционирования специализированных процессоров (СП) [1,2]. Рассматривая процедуры обнаружения и коррекции ошибок, нельзя не отметить возможность применения для данных процедур позиционной характеристики - нормированного следа.

Теорема. Если в системе ПСКВ, содержащей k информационных и r избыточных оснований, в результате нулевизации $A(z)$ получен нормированный след полинома

$$(0,0,0,\mathbf{K},0,g_{k+1}(z),g_{k+2}(z),...,g_{k+r}(z)), \quad (1)$$

то номер интервала, в который попадет ошибочный полином $A^*(z)$, равен:

$$l_{инт}(z)=\left|\sum_{j=k+1}^{k+r}R_j(z)g_j(z)\right|^{+}_{P_{конт}(z)}, \quad (2)$$

где $R_j(z)=\lfloor B_j(z)/P_{раб}(z)\rfloor$;

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

Доказательство. Докажем в начале, что если хотя бы один $g_j(z)\neq 0$, где $j=k+1,\ldots,k+r$, то полином $A^*(z)$ является запрещенным. Заменим произведение r избыточных оснований ПСКВ одним составным модулем $P_{конт}(z)=\prod_{i=k+1}^{k+r}p_i(z)$. Тогда полином $A(z)=(a_1(z),a_2(z),...,a_{k+1}(z),...,a_{k+r}(z))$, примет вид:

$$A(z)=(a_1(z),a_2(z),...,a_k(z),a_{конт}(z)), \quad (3)$$

где $A(z)\equiv a_{конт}(z)\bmod P_{конт}(z)$.

Если в кодовой комбинации $A(z)$ произошла ошибка, то результатом операции параллельной нулевизации $A^*(z)$ с использованием псевдоортогональных базисов $A_{ik}(z)$ будет отличный от нуля нормированный след:

$$(0,0,0,...,0,g_{конт}(z)), \quad (4)$$

где

$$g_{конт}(z)=(a_{конт}(z)-\sum_{i=1}^{k}g^{i}_{конт}(z))\bmod P_{конт}(z);$$

$$g^{i}_{конт}(z)\equiv B_i^*(z)\bmod P_{конт}(z);$$

$B_i^*(z)$ - ортогональный базис безизбыточной ПСКВ.

С другой стороны, согласно китайской теореме об остатках (КТО):

$$g_{конт}(z)=\sum_{j=k+1}^{k+r}g^{j}_{конт}(z)U_j(z)\bmod P_{конт}(z), \quad (5)$$

где $g^{j}_{конт}(z)\equiv g(z)\bmod p_j(z)$; $U_j(z)$ – ортогональный базис ПСКВ с основаниями $p_{k+1}(z),\ldots,p_{k+r}(z)$.

Так как $g_{конт}(z)\neq 0$, то хотя бы один $g^{j}_{конт}(z)$ отличен от нуля. Таким образом, если в результате нулевизации $A^*(z)$ и псевдоортогональных базисов получен след полином:а

$$(0,\mathbf{K},0,g_{k+1}(z),...,g_{k+r}(z))\neq 0,$$

то полином - ошибочный.

Докажем теперь, что величина интервального номера $l_{инт}(z)$ определяется выражением (2). Пусть в результате процедуры нулевизации полинома $A^*(z)$ получим нормированный след:

$$g(z)=(0,0,0,...,0,g_{k+1}(z),g_{k+2}(z),...,g_{k+r}(z))$$

отличный от нуля. Известно

$$A^*(z)=A(z)+\Delta A_i(z), \quad (6)$$

где $\Delta A_i(z)=(\Delta a_i(z)B_i(z))\bmod P_{полн}(z)$;

$\Delta a_i(z)$ -глубина ошибки по i-ому основанию.

При этом:

$$\Delta A_i(z)=g(z)=(0,0,0,...,0,g_{k+1}(z)g_{k+2}(z),...,g_{k+r}(z))$$

Тогда на основании выражения (17) имеем:

$$l_{инт}(z)=\left[A^*(z)/P_{раб}(z)\right]=$$
$$=\left[A(z)+\Delta A_i(z)/P_{раб}(z)\right]=\left[g(z)/P_{раб}(z)\right]. \quad (7)$$

Согласно КТО и с учетом:

$$a_i(z)=0, i=1,2,...,k,$$

имеем:

$$g(z)=(\sum_{j=k+1}^{k+r}g_j(z)B_j(z))\bmod P_{полн}(z). \quad (8)$$

Подставляем (8) в равенство (7) получаем:

$$l_{инт}(z)=\left[\sum_{j=k+1}^{k+r}g_j(z)B_j(z)\Big/P_{раб}(z)\right]. \quad (9)$$

Учитывая подобие ортогональных базисов и делимость без остатка ортогональных базисов контрольных оснований на рабочий диапазон, имеем:

$$l_{инт}(z) = \left| \sum_{j=k+1}^{k+r} R_j(z) g_j(z) \right|^{+}_{P_{кат}(z)}, \qquad (10)$$

где $R_j(z) = \lfloor B_j(z) / \ P_{раб}(z) \rfloor$.Доказательство закончено.

В работе [3] представлена организация сети нейронной логики, реализующей вычисление номера согласно (10) расширенном поле Галуа $GF(2^4)$. С целью сокращения схемных затрат целесообразно перейти к многомерной обработке данных. Тогда

$$\begin{cases} l^{k+1}_{инт}(z) = \left\| \sum_{j=k+1}^{k+r} \left| R_j(z) g_j(z) \right|^{+}_{Pk+1(z)} \right|^{+}_{Pk+1(z)} \Bigg|^{+}_{PK+1(z)} \\ l^{k+2}_{инт}(z) = \left\| \sum_{j=k+1}^{k+r} \left| R_j(z) g_j(z) \right|^{+}_{Pk+2(z)} \right|^{+}_{Pk+2(z)} \Bigg|^{+}_{Pk+2(z)} \\ \vdots \\ l^{k+r}_{инт}(z) = \left\| \sum_{j=k+1}^{k+r} \left| R_j(z) g_j(z) \right|^{+}_{Pk+r(z)} \right|^{+}_{Pk+r(z)} \Bigg|^{+}_{Pk+r(z)} \end{cases} \qquad (11)$$

Таким образом, применение выражения (11) позволяет осуществить процедуру поиска и коррекции ошибок с использованием нормированного полинома.

Выводы: Из полученных данных наглядно видно, что вычислительное устройство, реализующее алгоритм (11), обеспечивает наибольшую эффективность при контроле и исправлении ошибок, возникающих в процессе функционирования спецпроцессора.

СПИСОК ЛИТЕРАТУРЫ

1. 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.

2. 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.

3. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронной сети для коррекции ошибок в непозиционном коде расширенного поля Галуа/Нейрокомпьютеры: разработка, применение. №8-9, 2003. С. 10-16.

ОБНАРУЖЕНИЕ И КОРРЕКЦИЯ ОШИБОК В КОДАХ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ НА ОСНОВЕ НУЛЕВИЗАЦИИ

Калмыков И.А.
Северо-Кавказский государственный технический университет, Ставрополь

Применение полиномиальной системы классов вычетов (ПСКВ), в которой в качестве оснований выбираются минимальные многочлены $p_i(z)$ поля $GF(p^n)$, позволяет полином $A(z)$, удовлетворяющий условию:

$$A(z) \in P_{пол},$$

$$P_{пол} = \prod_{i=1}^{k+r} p_i(z) = z^{p^n - 1} - 1, \qquad (1)$$

представить в виде:

$$A(z) = (a_1(z), a_2(z), ..., a_{k+r}(z)), \qquad (2)$$

где $a_i(z) = rest\left(A(z) / p_i(z) \right)$, $i = 1,2,...,k+r$.

Выполнение операций над операндами в поле Галуа $GF(p^n)$ производятся независимо по каждому из модулей $p_i(z)$. Независимость обработки информации по основаниям ПСКВ позволяет не только повысить скорость обработки, но так же и обеспечить обнаружение и коррекцию ошибок в процессе функционирования СП. 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 $P_{полн}(z)$ поля $GF(p^n)$ на два подмножества, первое из которых называется рабочим диапазоном

$$P_{раб}(z) = \prod_{i=1}^{k} p_i(z), \qquad (3)$$

а второе подмножество $GF(p^n)$, определяемое произведением $r = n - k$ контрольных оснований:

$$P_{конт}(z) = \prod_{i=k+1}^{k+r} p_i(z), \qquad (4)$$

задает совокупность запрещенных комбинаций. Многочлен $A(z)$ будет считаться разрешенным в том и только том случае, если он является элементом нулевого интервала полного диапазона $P_{полн}(z)$, то есть $A(z) \in P_{раб}(z)$.

Для определения местоположения $A(z) = (a_1(z), a_2(z), ..., a_{k+r}(z))$ используется метод нулевизации, заключающейся в переходе от исходного полинома к полиному вида:

$$(0, 0, ..., x_{k+1}(z), ..., x_{k+r}(z)), \qquad (5)$$