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

Калмыков И.А.

Северо-Кавказский государственный технический университет

г. Ставрополь, Россия, kia762@yandex.ru

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

$$A(z) \in P_{пол},$$

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

представить в виде

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

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

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

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

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

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

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

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

при помощи последовательных преобразований, при которых не имеет место ни один выход за пределы рабочего диапазона системы. Нулевизация заключается в последовательном вычитании из исходного полинома, представленного в модулярном коде, констант нулевизации, с целью получения

$$A_k(z)=A_{k-1}(z)-M_k(z)=(0,0,...,x_{k+1}(z),...,x_{k+r}(z)). \tag{6}$$

Если в результате выполнения процедуры нулевизации будет получен нулевой результат, то это свидетельствует, что комбинация $A(z)$ не содержит ошибок. В противном случае – модулярный код $A(z)$ – содержит ошибки.

Повысить скорость выполнения процедуры нулевизации можно за счет модификации констант нулевизации $M_i(z)$. Оставляя неизменным условие невыхода константы нулевизации $M_i(z)$ за пределы рабочего диапазона $P_{раб}(z)=\prod_{i=1}^{k} p_i(z)$, возьмем в качестве последних значения произведение остатков рабочих оснований на величину ортогональных базисов безизбыточной системы оснований

$$\begin{cases} a_1(z)B_1^*(z) \bmod P_{раб}(z)=(a_1(z),0,0,...,0,x_{k+1}^1(z),x_{k+2}^1(z),...,x_{k+1}^1(z)); \\ a_2(z)B_2^*(z) \bmod P_{раб}(z)=(0,a_2(z),0,...,0,x_{k+1}^2(z),x_{k+2}^2(z),...,x_{k+1}^2(z)); \\ \text{M} \\ a_k(z)B_k^*(z) \bmod P_{раб}(z)=(0,0,0,...,a_k(z),x_{k+1}^k(z),x_{k+2}^k(z),...,x_{k+1}^k(z)). \end{cases} \tag{7}$$

где $B_i^*(z)$ - ортогональный базис, безизбыточной системы оснований; $i=1,2,\ldots,k$.

Тогда если положить условие, что $A(z) \in P_{раб}(z)$, где $P_{раб}(z) = \prod_{i=1}^{k} p_i(z)$, то полином $A(z) = (a_1(z), a_2(z), \ldots, a_k(z))$ согласно китайской теореме об остатках (КТО) можно представить в виде

$$A(z) = (a_1,(z),0,0,\ldots,0) + (0,a_2(z),0,\ldots,0) + \ldots(0,0,0,\ldots,a_k(z)). \quad (8)$$

Каждое слагаемое выражения (9) представляет собой

$$(0,0,\ldots 0,a_i(z),0,\ldots,0) = a_i(z) B_i^*(z) \bmod P_{раб}(z), \quad (9)$$

Подставим выражения (8) в равенство (10). Получаем

$$\begin{aligned} A(z) &= (a_1(z),0,0,\ldots 0,(z),x_{k+1}^1(z),x_{k+2}^1(z),\ldots,x_{k+r}^1(z)) + \\ &+ (0,a_2(z),0,\ldots 0,x_{k+1}^2(z),x_{k+2}^2(z),\ldots,x_{k+r}^2(z)) + \ldots + \\ &+ (0,0,0,\ldots,a_k(z),x_{k+1}^k(z),x_{k+2}^k(z),\ldots,x_{k+r}^k(z)). \end{aligned} \quad (10)$$

Разность полинома $A(z)$ и модифицированных констант нулевизации $M_i(z)$, $i=1, 2,\ldots, k$, псевдоортогональных форм, задаёт величину нормированного следа полинома

$$\begin{cases} x_{k+1}(z) = (a_{k+1}(z) - \sum_{j=1}^{k} x_{k+1}^j(z)) \bmod p_{k+1}(z), \\ \text{M} \\ x_{k+r}(z) = (a_{k+r}(z) - \sum_{j=1}^{k} x_{k+r}^j(z)) \bmod p_{k+r}(z). \end{cases} \quad (11)$$

Рассмотрим ПСКВ, определяемую в поле $GF(2^5)$. В таблице 1 помещены значения рабочих и контрольных оснований ПСКВ, а также динамический диапазон.

Таблица 1 – Основания и динамический диапазон поля $GF(2^5)$

Основания ПСКВ		Рабочий диапазон ПСКВ
Рабочие	Контрольные	
$p_1(z) = z+1$	$p_6(z) = z^5 + z^2 + 1$	$z^{21} + z^{19} + z^{16} + z^{13} + z^{11} + z^9 + z^8 + z^6 + z^3 + z^2 + z + 1$
$p_2(z) = z^5 + z^3 + 1$	$p_7(z) = z^5 + z^3 + z^2 + z + 1$	
$p_3(z) = z^5 + z^4 + z^2 + z + 1$		
$p_4(z) = z^5 + z^4 + z^3 + z + 1$		
$p_5(z) = z^5 + z^4 + z^3 + z^2 + 1$		

Определим все значения произведений степеней z^j на ортогональные базисы $B_i^*(z)$, учитывая невозможность выхода за пределы рабочего диапазона $P_{раб}(z) = z^{21} + z^{19} + z^{16} + z^{13} + z^{11} + z^9 + z^8 + z^6 + z^3 + z^2 + z + 1$. Полученные значения модифицированных констант нулевизации представлены в таблице 2.

Таблица 2 – Константы нулевизации для поля GF(2^5)

	$\alpha_1(z)$	$\alpha_2(z)$	$\alpha_3(z)$	$\alpha_4(z)$	$\alpha_5(z)$	$\alpha_6(z)$	$\alpha_7(z)$
$z^0 B_1^*(z)$	1	0	0	0	0	z^2	z
$z^0 B_2^*(z)$	0	1	0	0	0	1	1
$z^1 B_2^*(z)$	0	z	0	0	0	z	z
$z^2 B_2^*(z)$	0	z^2	0	0	0	z^2	z^2
$z^3 B_2^*(z)$	0	z^3	0	0	0	z^3	z^3
$z^4 B_2^*(z)$	0	z^4	0	0	0	z^4	z^4
$z^0 B_3^*(z)$	0	0	1	0	0	z^4+z	z^4+1
$z^1 B_3^*(z)$	0	0	z	0	0	z^3+z^2+1	z^3+z+1
$z^2 B_3^*(z)$	0	0	z^2	0	0	z^4+z^3+z	z^4+z^2+z
$z^3 B_3^*(z)$	0	0	z^3	0	0	z^4+1	$z+1$
$z^4 B_3^*(z)$	0	0	z^4	0	0	z^2+z+1	z^2+z
$z^0 B_4^*(z)$	0	0	0	1	0	z^2	$z+1$
$z^1 B_4^*(z)$	0	0	0	z	0	z^3	z^2+z
$z^2 B_4^*(z)$	0	0	0	z^2	0	$z^4+z^3+z^2$	z^3+z
$z^3 B_4^*(z)$	0	0	0	z^3	0	z^4+1	z^4+z^2
$z^4 B_4^*(z)$	0	0	0	z^4	0	z^3+z+1	z^3+z^2+1
$z^0 B_5^*(z)$	0	0	0	0	1	z^4+z	z^4
$z^1 B_5^*(z)$	0	0	0	0	z	1	z^3+z^2+z+1
$z^2 B_5^*(z)$	0	0	0	0	z^2	z	$z^4+z^3+z^2+z$
$z^3 B_5^*(z)$	0	0	0	0	z^3	z^2	z^4+z+1
$z^4 B_5^*(z)$	0	0	0	0	z^4	z^3	z^3+1

. Пусть в поле $GF(2^5)$ задан полином $A(z)=z^6+z^5+z^4+1$. Данный полином принадлежит $P_{раб}(z)$. Представим его в модулярном коде

$A(z)=z^6+z^5+z^4+1= (0, z^3+z, z^4+z^3+z^2+z+1, z^2+z+1, z^3+z+1, z^4+z^3+z^2+z, 0).$

Проведем процедуру нулевизации.

1 этап

$A(z) = (0, z^3+z, z^4+z^3+z^2+z+1, z^2+z+1, z^3+z+1, z^4+z^3+z^2+z, \quad 0 \quad)$

$\underline{M_2(z)=(0, z^3+z, \quad 0 \quad , \quad 0 \quad , \quad 0 \quad , \quad z^3+z \quad , z^3+z \,)}$

$A_2(z)=(0, \quad 0 \quad , z^4+z^3+z^2+z+1, z^2+z+1, z^3+z+1, \quad z^4+z^2 \quad , z^3+z \,)$

2 этап

$A_2(z) =(0, 0, z^4+z^3+z^2+z+1, z^2+z+1, z^3+z+1, \quad z^4+z^2 \quad , z^3+z)$

$\underline{M_3(z)=(0, 0, z^4+z^3+z^2+z+1, \quad 0 \quad , \quad 0 \quad , \quad z^4+z+1, z^3+1)}$

$A_3(z)=(0, 0, \quad 0 \quad , z^2+z+1, z^3+z+1, \quad z^2+z+1, z+1 \,)$

3 этап

$A_3(z) =(0, 0, 0, z^2+z+1, z^3+z+1, \quad z^2+z+1 \quad , z+1 \,)$

$\underline{M_4(z)=(0, 0, 0, z^2+z+1, \quad 0 \quad , \quad z^4 \quad , z^3+z^2+z+1)}$

$A_4(z)=(0, 0, 0, \quad 0 \quad , z^3+z+1, z^4+z^2+z+1, z^3+z^2 \,)$

4 этап

$A_4(z) =(0, 0, 0, 0, z^3+z+1, z^4+z^2+z+1, z^3+z^2)$

$\underline{M_5(z)=(0, 0, 0, 0, z^3+z+1, z^4+z^2+z+1, z^3+z^2)}$

$A_5(z)=(0, 0, 0, 0, \quad 0 \quad , \quad 0 \quad , \quad 0 \quad)$

Таким образом, полином $A(z)$ не содержит ошибки.

Пусть ошибка произошла по 1 основанию

$A^*(z)= (1, z^3+z, z^4+z^3+z^2+z+1, z^2+z+1, z^3+z+1, z^4+z^3+z^2+z, 0).$

В результате проведения процедуры нулевизации получен результат

$A_5(z)=(0, 0, 0, 0, \quad 0 \quad , \quad z^2 \quad , \quad z \quad)$, что свидетельствует о наличии ошибки в модулярном коде.

Литература

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.