УДК 681.3

РАЗРАБОТКА АЛГОРИТМА ВЫЧИСЛЕНИЯ РАНГА В НЕПОЗИЦИОННЫХ КОДАХ

Голошубов К.С., Солодкин И.Г., Гапочкин А.В., Калмыков М.И.
ФГАОУ ВПО «Северо-кавказский федеральный университет», Ставрополь, e-mail:kia762@yandex.ru

Современные модулярные коды нашли широкое применение во многих сферах деятельности человека. Среди таких областей можно выделить цифровую обработку сигналов, построение отказоустойчивых вычислительных устройств, способных сохранять работоспособное состояние при возникновении отказов, криптографические алгоритмы защиты данных. Одной из обязательных операций при использовании модулярных кодов является вычисление ранга. В работе представлен усовершенствованный алгоритм вычисления данной характеристики, а также нейросетевая схемная реализация.

Ключевые слова: модулярные коды, система остаточных классов, полиномиальная система классов вычетов, ранг, нейронные сети

DEVELOPMENT OF ALGORITHMS IN COMPUTING THE RANK NONPOSITIONAL CODES

Goloshubov K.S., Solodkin I.G., Gapochkin A.V , Kalmykov M.I.
Federal state Autonomous educational institution higher professional education «North-caucasian federal university, Stavropol, e-mail:kia762@yandex.ru

Modern modular codes have been widely used in many fields of human activity. Among these areas can be identified digital signal processing, the construction of fault-tolerant computing devices, capable of maintaining a healthy state in the event of failure, cryptographic algorithms to protect data. One of the required steps, the use of modular codes is to compute the rank. The paper presents an improved algorithm to compute-ment of the characteristics, as well as the circuit implementation of the neural network.

Keywords: modular codes, the system of residual classes, polynomial system of residue classes, rank, neural networks

Информационные технологии (ИТ) находят все большее применение в различных областях современного общества. Это обусловлено тем, что ИТ позволяют повысить эффективность работы специалистов во множестве отраслей хозяйства. Наиболее широкое применение IT-технологии нашли в области инфотелекоммуникационных систем. Особое внимание в таких системах уделяется цифровой обработке сигналов (ЦОС). Для обеспечения реального масштаба времени обработки сигналов применяются параллельные алгоритмы вычислений.

Обеспечить высокие требования к производительности вычислительных устройств возможно только за счет реализации алгоритмов ЦОС на основе специализированных процессоров (СП).

Высокие требованиями, предъявляемые к скорости обработки информации, обеспечили широкое использование параллельных алгоритмов вычислений в современных специализированных процессорах. Одним из перспективных направлений, позволяющим построить СП ЦОС реального масштаба времени, является использование непозиционных модулярных кодов [1–4]. Все множество модулярных кодов можно разбить на две группы. Основу первой группы составляют алгебраические структуры, обладающие свойством кольца. К ним можно отнести систему остаточных классов (СОК). В данной системе используются взаимно простые числа, которые выступают в роли оснований СОК. Тогда набор этих оснований образует рабочий диапазон

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

где p_i – основания системы остаточных классов.

В этом случае, числа, которые принадлежат рабочему диапазону, можно однозначно представить в виде набора остатков

$$A = (\alpha_1, \alpha_2, ..., \alpha_k), \qquad (1^*)$$

где. – $A < P_{раб}$; $\alpha_i \equiv A \bmod p_i$; $i = 1,2,...,k$.

Пусть даны два числа, представленные в коде СОК $\grave{A} = (\alpha_1, \alpha_2, ..., \alpha_k)$ и $\hat{A} = (\beta_1, \beta_2, ..., \beta_k)$. Тогда для суммы, разности и произведения двух чисел A и B, имеющих соответственно модулярные коды и справедливы соотношения при $i = 1,...,k$

$$\left|A * B\right|_p^+ = \left|\alpha_i * \beta_i\right|_{p_i}^+, \qquad (2)$$

где * – операции сложения, вычитания и умножения по модулю.

Тогда ортогональное преобразование сигнала и ему обратное преобразование будут определяться

$$\begin{cases} X_0(l) = \left(\sum_{j=0}^{N-1} x_1(j) W_1^{jl}, ..., \sum_{j=0}^{N-1} x_k(j) W_k^{jl} \right) \\ \vdots \\ X_{N-1}(l) = \left(\sum_{j=0}^{N-1} x_1(j) W_1^{jl}, ..., \sum_{j=0}^{N-1} x_k(j) W_k^{jl} \right) \end{cases}, \quad (3)$$

$$\begin{cases} x_0(l) = \left(\frac{1}{N} \sum_{j=0}^{N-1} X_1(j) W_1^{jl}, ..., \frac{1}{N} \sum_{j=0}^{N-1} X_k(j) W_k^{jl} \right) \\ \vdots \\ x_{N-1}(l) = \left(\frac{1}{N} \sum_{j=0}^{N-1} X_1(j) W_1^{jl}, ..., \frac{1}{N} \sum_{j=0}^{N-1} X_k(j) W_k^{jl} \right) \end{cases}, \quad (4)$$

где W – поворачивающий коэффициент дискретного преобразования Фурье $x_i(j) \equiv x(j) \bmod p_i$ – остаток по модулю отсчета входной последовательности $x = \{x(0), x(1),..., x(N-1)$; $X_i(j) \equiv X_i(j) \bmod p_i$ – остаток по модулю спектрального отсчета сигнала $X = \{X(0), X(1),..., X(N-1)\}$.

Основу второй группы составляют алгебраические структуры, работающие в кольце полиномов. К ним можно отнести полиномиальную систему классов вычетов (ПСКВ). В данной системе используются неприводимые полиномы $p_i(z)$, которые выступают в роли оснований GCRD. Тогда набор этих оснований образует рабочий диапазон

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

В этом случае, двоичный код числа представляется в полиномиальной форме. Тогда при выполнении условия $deg\ A < deg\ P_{раб}$, можно однозначно представить в виде набора остатков

$$A(z) = \left(\alpha_1(z), \alpha_2(z), ..., \alpha_k(z)\right), \quad (6)$$

где – $\alpha_i(z) \equiv A(z) \bmod p_i(z)$; $i = 1, 2,...,k$.

Пусть даны два числа, представленные вкодеПСКВ $\hat{A}(z) = \left(\alpha_1(z), \alpha_2(z), ..., \alpha_k(z)\right)$ и $\hat{A}(z) = \left(\beta_1(z), \beta_2(z), ..., \beta_k(z)\right)$. Тогда для суммы, разности и произведения двух чисел $A(z)$ и $B(z)$, имеющих соответственно модулярные коды и справедливы соотношения при $i = 1,...,k$

$$\left|A(z) * B(z)\right|^{+}_{p_i(z)} = \left|\alpha_i(z) * \beta_i(z)\right|^{+}_{p_i(z)}, \quad (7)$$

где * – операции сложения, вычитания и умножения по модулю.

Так как эти модулярные коды работают с остатками, то благодаря малоразрядности обрабатываемых остатков, реализация вычислений проводится в реальном масштабе времени. При этом такие вычисления осуществляются параллельно по независимым вычислительным каналам, которые определяются модулями кода. Благодаря этому модулярные коды нашли широкое применение не только в области цифровой обработки сигналов [1–3], построения отказоустойчивых вычислительных устройств [4–6], но и при реализации алгоритмов защиты данных от НСД [7–10].

Одним из основных факторов, снижающих эффективность применения непозиционных систем счисления, является отсутствие высокоэффективного алгоритма преобразования от ПСКВ к двоичному виду. Поэтому в настоящее время особое внимание уделяется разработке методов, обладающих параллельно-конвейерной структурой, которые бы позволили бы свести операцию преобразования кодов классов вычетов к позиционному на основе выполнения модульных операций.

Как правило, восстановление полученного результата из непозиционной системы счисления к двоичному позиционному виду на основе китайской теоремы об остатках (КТО) согласно

$$x(z) = \sum_{i=1}^{s} B_i(z) \alpha_i(z) \bmod P(z). \quad (8)$$

Основным недостатком данного выражения является необходимость выполнения операции суммирования парных произведений по модулю $P(z)$. При значительных

значениях динамического диапазона $P(z)$ построение сумматора по модулю $P(z)$ проблематично.

Одним из путей решения данной проблемы является вычисление ранг числа – $K(z)$. Тогда выражение (8) преобразуется к виду

$$x(z) = \sum_{i=1}^{s} \mathrm{B}_i(z)\alpha_i(z) \bmod P(z) - K(z)P(z)P(z). \quad (9)$$

Исходя их условия взаимной простоты модулей $p_i(z), i = 1, \ ..., \ S$, и равенства (9.) очевидно, что $K(z)$ является целочисленной функцией, определяемой из значений *x(z)*.

В отличие от выражения (8) , в котором значения *x(z)* нельзя вывести за пределы кольца *P(z)*, равенства (9) осуществляет смещение значения *x(z)* за пределы этого диапазона *P(z)*. На рис. 1 представлена геометрическая интерпретация выражений (8) и (9). Если диапазон *P(z)* представить в виде окружности, то равенства (9) может быть описано спирально, с радиусом равным радиусу *P(z)*.

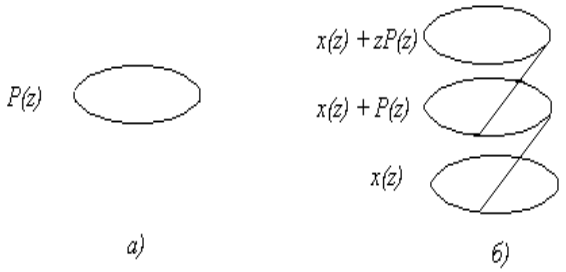

Рис. 1. Геометрическая модель: а) – выражения (8); б) – выражения (9)

Если *x(z)* является элементом *P(z)*, то значение ранга *K(z)*, должно удовлетворить условию

$$0 \le K(z) \le S(z) \quad (10)$$

где $S(z) = s_0 z^0 + s_1 z^1 + s_2 z^2 + ... + s_j z^j$ – полиноминальное представление *S*.

Следовательно, величина *K(z)* не зависит от величины оснований $p_i(z), i = 1, \ ..., \ \mathrm{s}$, а определяется только их количеством. Таким образом, для определения величины ранга *K(z)* удовлетворяющего условию (10), целесообразно ввести дополнительное основание $p_g(z)$, которое обеспечивает выполнение следующего равенства

$$\begin{aligned} &НОД(P(z),\ p_g(z)) = 1; \\ &\deg p_g(z) > \deg s(z); \end{aligned} \quad (11)$$

где $\deg p_g(z), \deg s(z)$ – порядок полиномов $p_g(z)$ и *s(z)* соответственно.

Введение дополнительного модуля $p_g(z)$ обеспечивает выполнение (12).

$$K(z) \equiv K(z) \bmod p_g(z). \quad (12)$$

Тогда из выражения (9), разделив обе части на *P(z)*, получаем

$$\frac{x(z)}{P(z)} = \frac{\sum_{i=1}^{S} \alpha_i(z) B_i(z)}{P(z)} - K(z). \quad (13)$$

Используя полученное равенство (13), а также условия (12), имеем

$$K(z) = \left\| \sum_{i=1}^{s} \left| \alpha_i(z) m_i(z) \right|_{p_i(z)}^{+} \left| p_i^{-1}(z) \right|_{p_g(z)}^{+} \right|_{P_g(z)}^{+} + \left\| P^{1}(z) \right|_{p_g(z)}^{+} \left| x(z) \right|_{p_g(z)}^{+} \Big|_{p_g(z)}^{+} \Big|_{p_g(z)}^{+}, \quad (14)$$

где $m_i(z)$ – вес *i*-го ортогонального базиса, такой что $\frac{P(z)m_i(z)}{p_i(z)} \equiv 1 \bmod p_i(z)$.

Таким образом, для вычисления значения ранга *K(z)* необходимо определить значения

$$\alpha_g(z) \equiv x(z) \bmod p_g(z). \qquad (15)$$

Следовательно, исходный полином *x(z)* можно представить в виде $(s+1)$ –мерного вектора

$$x(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_g(z)). \quad (16)$$

При этом дополнительный модуль $p_g(z)$ не входит в состав ПСКВ и не оказывает влияние на величину диапазона *P(z)*. Если $2 \le S \le 14$, что чаще всего оправдывает себя выбор $p_g(z)$, порядок которого не превышает четырех. Следовательно, для реализации (15) не требуется значительных аппаратных затрат.

Таким образом, надо определить величину ранга *K(z)* согласно (14), а затем на основании выражения (9) осуществить перевод *x(z)* из ПСКВ в позиционную систему счисления.

Пример 1. Пусть задано расширенное поле Галуа $GF(2^4)$, которое определяется следующими основаниями:

$$p_1(z) = z+1; p_2(z) = z^2+z+1; \quad p_3(z) = z^4+z^3+z^2+z+1; p_4(z) = z^4+z^3+1;$$
$$p_5(z) = z^4+z+1.$$

Полный диапазон системы составляет

$$P_5(z) = \prod_{i=1}^{5} p_i(z) = z^{15}-1$$

При этом ортогональные базисы данной алгебраической системы равны:

$$B_1(z) = z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^8+z^7+z^6+z^5+z^4+z^3+z^2+z+1;$$

$$B_2(z) = z^{14}+z^{13}+z^{11}+z^{10}+z^8+z^7+z^5+z^4+z^2+z;$$

$$B_3(z) = z^{14}+z^{13}+z^{12}+z^{11}+z^9+z^8+z^7+z^6+z^4+z^3+z^2+z;$$

$$B_4(z) = z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^7+z^6+z^3;$$

$$B_5(z) = z^{12}+z^9+z^8+z^6+z^4+z^3+z^2+z.$$

Так число оснований $s = 5$, то в полиноминальной форме это сложно представить как $s = z^2 + 1$. Тогда, согласно (11), выбираем дополнительное основание $p_g(z) = z^3$.

Воспользуемся выражением (9) и определим значение ранга *K(z)* полинома *x(z)* $= z^7 + z^6 + z^4 + z^3 + z + 1$, который в исходной ПСКВ представляется в виде

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

Для контроля рассчитаем преобразование ПСКВ в позиционную систему счисления по формуле (9)

$$x(z) = \sum_{i=1}^{5} \alpha_i(z) B_i(z) + K(z)P(z) = 0B_1(z) + (z+1)B_2(z) + zB_3(z) + (z^3+z)B_4 +$$
$$+(z^3+z^2+z+1)B_5(z) + K(z)(z^{15}+1) = z^7+z^6+z^4+z^3+z+1$$

Откуда следует, что

$$K(z) = z^2+z+1$$

Найдем теперь значение ранга *K(z)*, используя выражение (14). Очевидно, что для выбранной системы оснований значения $\left|\frac{1}{p_i(z)}\right|^{+}_{p_g(z)}$, где *i = 1, 2, 3, 4, 5*, определяется следующим образом:

$$\left|\frac{1}{p_1(z)}\right| \bmod(z^3) = z^2 + z + 1; \quad \left|\frac{1}{p_4(z)}\right| \bmod(z^3) = 1;$$

$$\left|\frac{1}{p_2(z)}\right| \bmod(z^3) = z^2 + z + 1; \quad \left|\frac{1}{p_5(z)}\right| \bmod(z^3) = z^2 + z + 1.$$

$$\left|\frac{1}{p_3(z)}\right| \bmod(z^3) = z + 1;$$

Значения весов ортогональных базисов полиномиальной системы классов вычетов поля $GF(2^4)$, определяются как

$$m_1(z) = 1; \quad m_2(z) = z; \quad m_3(z) = z^3 + z;$$
$$m_4(z) = z^3; \quad m_5(z) = z.$$

Так как дополнительное основание $p_g(z) = z^3$, то

$$\alpha_g(z) = x(z) \bmod(z^3) = z^7 + z^6 + z^4 + z^3 + z + 1 \bmod(z^3) = z + 1.$$

Подставляя в равенство (9) полученные значения имеем

$$K(z) = \left\| (0 \cdot 1)(z^2 + z + 1) \right|_{z^3}^{+} + \left\| z(z+1) \right|_{z^2+z+1}^{+} (z^2 + z + 1) \Big|_{z^3}^{+} + \left\| z(z^3 + z) \right|_{z^4+z^3+z^2+z+1}^{+} (z+1) \Big|_{z^3}^{+} +$$

$$+ \left\| z^3 (z^3 + z) \right|_{z^4+z^3+1}^{+} \Big|_{z^3}^{+} + \left\| z(z^3 + z^2 + z + 1) \right|_{z^4+z+1}^{+} (z+1) \Big|_{z^3}^{+} \Big|_{z^3}^{+} = z^2 + z + 1$$

Полученное значение ранга $K(z)$ совпадает со значением, непосредственно вычисляемым по формуле (9). Следовательно, предложенный алгоритм позволяет осуществлять выполнение операции вычисления ранга числа, используя только модульные процедуры. Нейросетевая реализация данного алгоритма приведена на рис. 2.

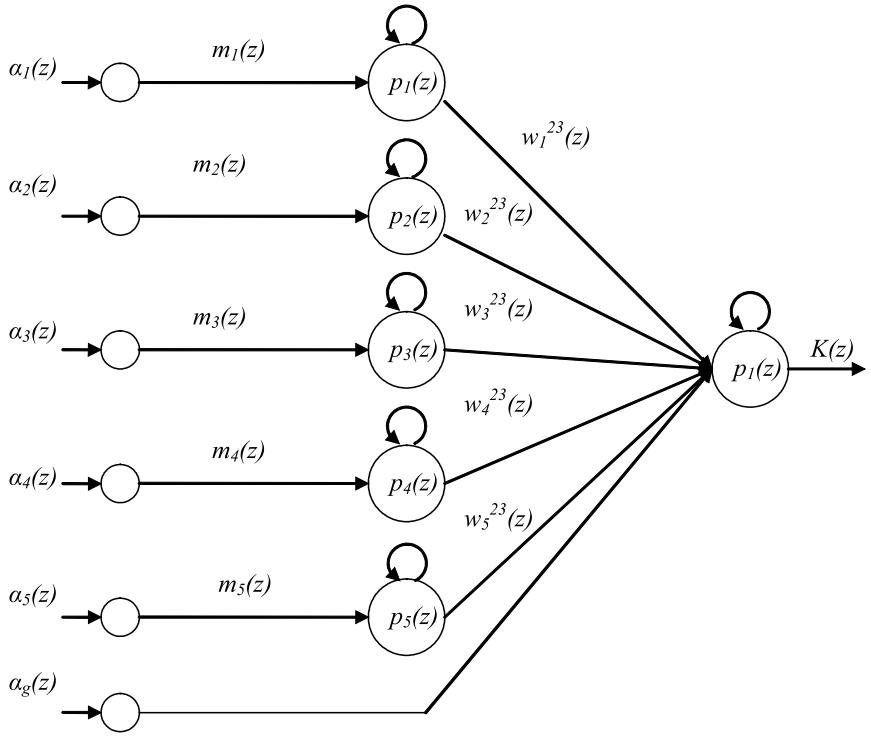

Рис. 2. Структура НС для вычисления ранга K(z)

Первый слой нейронной сети состоит из шести нейронов, которые осуществляют прием вектора

$x(z) = (\alpha_1(z), \alpha_2(z), \alpha_3(z), \alpha_4(z), \alpha_5(z), \alpha_6(z))$,

поданного на вход устройства. Синоптические веса связей $W_i^{12}(z)$, где i = 1, 2, 3, 4, 5, представляют собой веса ортогональных базисов $m_i(z)$ и вычисляются заранее.

Результат умножения $m_i(z)$ и $\alpha_i(z)$ преобразуется по модулю $p_i(z)$ во втором слое НС. Приведенные по модулю значения $\alpha_i(z)m_i(z) \bmod p_i(z)$, затем умножаются на $W_i^{23}(z) = \left| 1/p_i(z) \right|_{p_g(z)}^{+}$, и совместно с добавочным остатком подаются на выходной слой НС, где и происходит сложение по модулю $p_g(z)$. Полученный результат представляет собой ранг числа *K(z)*.

Заключение

Применение модулярных кодов позволяет обеспечить обработку данных в реальном масштабе времени. Одной из обязательных операций, используемых при выполнении процедур обратного преобразования, а также поиска и коррекции ошибок, является вычисление ранга. В работе приведен алгоритм вычисления ранга, а также схемная нейросетевая реализация этого алгоритма.

Список литературы

1. Калмыков И.А., Калмыков М.И. Структурная организация параллельного спецпроцессора цифровой обработки сигналов, использующего модулярные код// Теория и техника радиосвязи. – 2014. – № 2. – С. 60–66.

2. Чипига А.Ф., Калмыков И.А. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности// Наука. Инновации. Технологии. – 2004. – Т.38. – С. 46.

3. Калмыков И.А., Воронкин Р.А., Резеньков Д.Н., Емарлукова Я.В., Фалько А.А. Генетические алгоритмы в системах цифровой обработки сигналов// Нейрокомпьютеры: разработка и применение. – 2011. – № 5. – С. 20–27.

4. Калмыков И.А., Саркисов А.Б., Макарова А.В. Технология цифровой обработки сигналов с использованием модулярного полиномиального кода// Известия Южного федерального университета. Технические науки. – 2013. – № 12 (149). – С. 234–241.

5. Мартиросян А.Г., Калмыков М.И. Основные методы обеспечения отказоустойчивости специализированных вычислительных устройств цифровой обработки сигналов Современные наукоемкие технологии. – 2014. – № 3. – С. 62–67.

6. Калмыков И.А., Саркисов А.Б., Яковлева Е.М., Калмыков М.И. Модулярный систолический процессор цифровой обработки сигналов с реконфигурируемой структурой// Вестник Северо-Кавказского федерального университета. – 2013. – № 2 (35). – С. 30–35.

7. Калмыков И.А., Чипига А.Ф., Кихтенко О.А., Барильская А.В. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем// Известия Южного федерального университета. Технические науки. – 2009. – Т. 100, № 11. – С. 210–220.

8. Калмыков И.А., Дагаева О.И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции// Известия Южного федерального университета. Технические науки. – 2012. – Т. 137, № 12 (137). – С. 218–224.

9. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О.А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи// Инфокоммуникационные технологии. – 2010. – Т. 8, № 2. – С. 14–22.

10. Чипига А.Ф., Калмыков И.А., Яковлева Е.М., Калмыков М.И. Применение полиномиальной системы классов вычетов в схеме разделения секрета// Информационное противодействие угрозам терроризма. – 2012. – № 19. – С. 45–49.