УДК 681.3

РЕАЛИЗАЦИЯ МОДУЛЬНЫХ ОПЕРАЦИЙ В КОЛЬЦЕ ПОЛИНОМОВ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Тимошенко Л.И.

Ставропольский филиал Краснодарского университета МВД России, Ставрополь, e-mail: lit-545@yandex.ru

Использование методов цифровой обработки сигналов позволяет относительно легко обеспечить высокую помехоустойчивость систем обработки данных, необходимую точность и разрешающую способность, стабильность параметров тракта обработки информации и ряд других преимуществ. При этом эффективность работы системы цифровой обработки сигналов во многом определяется математической моделью. Как правило задачи цифровой обработки сигналов требуют выполнения больших объемов вычислений над большими массивами данных в реальном масштабе времени. Возрастание требований к технико-экономическим характеристикам современных систем цифровой обработки сигналов, расширение их областей применения и усиливающаяся тенденция к параллельным методам их организации привели к активизации работ по разработке специализированных процессоров цифровой обработки сигналов, ориентированных на построение систем цифровой обработки сигналов с предельными значениями технических характеристик.

Ключевые слова: цифровая обработка сигналов, арифметические операции, суммирование по модулю, нейронная сеть, системе остаточных классов

REALIZATION OF MODULAR OPERATIONS IN THE RING OF POLYNOMS BY MEANS OF NEURAL NETWORKS

Timoshenko L.I.

Stavropol branch of the Ministry of Internal Affairs Krasnodar university of Russia, Stavropol, e-mail: lit-545@yandex.ru

Use of methods of digital processing of signals allows to provide rather easily a high noise stability of systems of data processing, necessary accuracy and the allowing ability, stability of parameters of a path of information processing and some other advantages. Thus overall performance of system of digital processing of signals in many respects is defined by mathematical model. As a rule problems of digital processing of signals demand performance of large volumes of calculations over big data files in real time. Increase of requirements to technical and economic characteristics of modern systems of digital processing of signals, expansion of their scopes and the amplifying tendency to parallel methods of their organization led to activization of works on development of specialized processors of digital processing of the signals focused on creation of systems of digital processing of signals with limit values of technical characteristics.

Keywords: digital processing of signals, arithmetic transactions, summation of the module, a neural network, system of residual classes

Для эффективной реализации математических моделей цифровой обработки сигналов (ЦОС) определённых в кольце полиномов необходимо, чтобы вычислительные устройства могли эффективно поддерживать арифметические операции этой алгебраической системы. Рассмотрим выполнение таких операций в полиномиальной системе классов вычетов. Для этого необходимо представить значения остатков операндов в виде полиномиальной записи [5, 6]. Пусть степень неприводимого полинома $ordp_i(z) = l_i, i = 1,...,n$. Тогда справедливо

$$\alpha_i(z) = \mu^i_{l_i-1} z^{l_{i-1}} + \mu^i_{l_i-2} z^{l_{i-2}} + ... + \mu^i_1 z^1 + \mu_0 z^0 . \qquad (1)$$

Аналогичным образом представим второй операнд

$$\beta_i(z) = \omega^i_{l_i-1} z^{l_{i-1}} + \omega^i_{l_i-2} z^{l_{i-2}} + ... + \omega^i_1 z^1 + \omega_0 z^0 . \qquad (2)$$

Известно, что сравнения по одному и тому же модулю можно почленно складывать, то для суммы двух полиномов $A(z)$ и $B(z)$, имеющих соответственно коды $(\alpha_1(z), \alpha_2(z), ..., \alpha_n(z))$ и $(\beta_1(z), \beta_2(z), ..., \beta_n(z))$ справедливо соотношения [9]

$$\left|A(z)+B(z)\right|^+_{p(z)} = \left(\left|\alpha_1(z)+\beta_1(z)\right|^+_2, ..., \left|\alpha_n(z)+\beta_n(z)\right|^+_2\right) =$$

$$= \left(\mu^1_0 \oplus \omega^1_0, \sum_i (\mu^2_{l_2-i} \oplus \omega^2_{l_2-i}) z^i, \sum_j (\mu^3_{l_2-j} \oplus \omega^3_{l_2-j}) z^j, ..., \sum_w (\mu^n_{l_2-w} \oplus \omega^n_{l_2-w}) z^w\right) \qquad (3)$$

где $\oplus$ – операция суммирования по модулю p.

Исходя из условия, что характеристика поля равна двум, то операция обратная суммированию выполняется аналогичным образом [8]:

$$\left|A(z)+B(z)\right|^{+}_{p(z)}=\left(\left|\alpha_1(z)-\beta_1(z)\right|^{+}_{2},...,\left|\alpha_n(z)-\beta_n(z)\right|^{+}_{2}\right)=$$

$$=\left(\mu_0^1\oplus\omega_0^1,\sum_i(\mu^2_{l_2-i}\oplus\omega^2_{l_2-i})z^i,\sum_j(\mu^3_{l_2-j}\oplus\omega^3_{l_2-j})z^j,...,\sum_w(\mu^n_{l_2-w}\oplus\omega^n_{l_2-w})z^w\right) \quad (4)$$

В результате выполнения (3) и (4) получаются элементы образующие циклическую группу по операции сложения. Для реализации операции сложения $ord\ p_i(z)$-разрядных операторов в поле $GF(2^v)$ по основанию $p_i(z)$ потребуется всего $ord\ p_i(z)$ двухвходовых сумматоров по модулю два. Причём базовая операция – сложение, реализуется за одну операцию и не требует применения итеративных методов построение нейронной сети (НС) конечного кольца, используемого в системе остаточных классов (СОК) [1,2].

Известно [10], что в силу дистрибутивности операции умножения операндов над кольцом на элементы этого кольца относительно операции сложения имеем

$$\left|A(z)\cdot B(z)\right|^{+}_{p(z)}=\left(\left|\alpha_1(z)\cdot\beta_1(z)\right|^{+}_{p_1(z)},...,\left|\alpha_n(z)\cdot\beta_n(z)\right|^{+}_{p_n(z)}\right)=$$

$$=(\mu_0^1\omega_0^1,\sum_{m=0}^{2l_2-2}q^2_{2l_2-2-l}z^{2l_2-2-m};\ldots;\sum_{j=0}^{2l_n-2}q^n_{2l_n-2-j}z^{2l_n-2-j}), \quad (5)$$

где $q_s^i=\sum_{k=0}^{s}\mu_k^i\omega_{s-k}^i$ – линейная свертка; $s=0,...,2l_i-2$; $i=0...n$.

Таким образом, выполнение операции умножения над операндами в кольце полиномов имеет вид

$$A(z)B(z)=\left(\sum_{k,l\geq 0}a_k b_l z^{k+l}_{пол}\right)\mathrm{mod}\,P(z), \quad (6)$$

Из выражений (5) и (6) наглядно видно, что реализация модульного умножения реализуется на основе умножения соответствующих остатков по основаниям $p_i(z)$ с последующих суммированием по модулю характеристики поля. Следовательно, разработка высокоскоростного устройства, реализующего базовую операция по модулю характеристики поля в нейросетевом базисе, позволит обеспечить эффективную работу в реальном масштабе времени всего СП ЦОС[3,4].

Характерной чертой рассмотренных выше арифметических устройств, реализующих операции конечных алгебраических систем является наличие многовходовых сумматоров по модулю два [7]. Исходя из данной структурной особенности, можно сформулировать основные требования к нейронной сети, выполняющей эту базовую операцию:

– использование параллелизма, причем распараллеливание должно производится на уровне побитовой обработки входного вектора;

– применение конвейерной организации вычисления;

– отказ от принципа рекуррентной редукции, от обратных связях в структуре НС конечного кольца;

– количество итераций в процессе выполнения операции должно быть минимальным;

– количество нейронов в слоях НС должно быть минимальным, обеспечивая требуемую скорость обработки входного вектора.

Для повышения эффективности и достижения высоких показателей отказоустойчивости нейросетевых спецпроцессоров цифровой обработки сигналов является их построение на базе использования избыточности и корректирующих способностей алгебраической системы, которая положена в основу математической модели цифровой обработки сигнала. Применение полиномиальной системы классов вычетов позволяет не только повысить скорость обработки данных, но и обеспечить требуемый уровень надежности функционирования нейросетевого вычислительного устройства цифровой обработки сигналов.

Список литературы

1. Адошев А.И., Аникуев С.В., Гальвас А.В., Жданов В.Г., Ивашина А.В., Кобозев В.А., Логачева Е.А., Привалов Е.Е., Тимошенко Л.И., Шарипов И.К. Современные технологии в образовании // Развитие системы образования – обеспечение будущего. – Одесса. – 2013. – С. 60-97.

2. Земцев А.М., Тимошенко Л.И. Информационная составляющая безопасной эксплуатации электроустановок // Методы и средства повышения эффективности технологических процессов в АПК: Опыт, проблемы и перспективы. – 2013. – С. 76-78.

3. Калмыков И.А., Тимошенко Л.И. Нейросетевые модели многовходовых сумматоров по модулю два // Фундаментальные исследования. – 2008. – № 3. – С. 73-74.

4. Калмыков И.А., Тимошенко Л.И. Систолическая матрица для цифровой фильтрации в модулярной арифметике // Современные наукоемкие технологии. – 2007. – № 11. – С. 98-100.

5. Калмыков И.А., Хайватов А.Б., Тимошенко Л.И., Гахов В.Р. Применение полиномиальной системы классов вычетов для повышения скорости функционирования спецпроцессора адаптивных средств защиты информации // Успехи современного естествознания. – 2007. – № 5. – С. 76.

6. Кузьменко И.П., Тимошенко Л.И. Систолические принципы организации вычислений в спецпроцессоре цифровой обработки сигналов с параллельно-конвейерным распределением вычислительного процесса // Культура и общество: история и современность: материалы II Всероссийской (с международным участием) научно-практической конференции. – Ставрополь. – 2013. – С. 76-78.

7. Тимошенко Л.И. Нейросетевая реализация вычислений в полиномиальной системе классов вычетов // Фундаментальные исследования. – 2008. – № 3. – С. 71-73.

8. Тимошенко Л.И. Информатика. Курс лекций: Учебное пособие / Филиал РГСУ в г. Ставрополе. Ставрополь. – 2014. – Том Часть 2.

9. Тимошенко Л.И. Анализ основных методов прямого преобразования из позиционной системы счисления в модулярный полиномиальный код // Современные наукоемкие технологии. – 2007. – № 9. – С. 23-24.

10. Тимошенко Л.И. Применение математической модели обладающей свойством кольца, для реализации цифровой обработки сигналов // Современные наукоемкие технологии. – 2007. – № 9. – С. 22-23.