УДК 681.3

РАЗРАБОТКА СТРУКТУРЫ ВЫСОКОСКОРОСТНОГО УМНОЖИТЕЛЯ ПО МОДУЛЮ

[1]Саркисов А.Б., [1]Калмыков М.И., [2]Зыбин Ю.А., [2]Гончаров Р.Ю.

[1]ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kmi762@yandex.ru;

[2]Филиал Московского государственного университета приборостроения и информатики, Ставрополь, e-mail: kmi762@yandex.ru

Применение полиномиальной системы классов вычетов позволяет осуществлять цифровую обработку сигналов (ЦОС) в реальном масштабе времени. Это обусловлено тем, что операции ортогональных преобразований сигналов проводятся параллельно согласно выбранным основаниям. Одной из базовых операций ЦОС, эффективно реализуемой в полиномиальной системе классов вычетов, является умножение по модулю. В работе представлен новый алгоритм выполнения операции умножения по модулю, а также схемная реализация этого алгоритма.

Ключевые слова: полиномиальная система классов вычетов, система остаточных классов, цифровая обработка сигналов, модульные операции, умножитель по модулю

DEVELOPMENT OF STRUCTURE OF HIGH-SPEED MULTIPLIER MODULO

[1]Sarkisov A.B., [1]Kalmykov M.I., [2]Zybin Y.A., [2]Goncharov R.Y.

[1]Federal state Autonomous educational institution higher professional education «North-Caucasian federal university», Stavropol, e-mail:kmi762@yandex.ru;

[2]Filial Moscow state University of instrument engineering and informatics, Stavropol, e-mail:kmi762@yandex.ru

The use of a polynomial system of residue classes allows digital signal processing (DSP) in real time. This is due to the fact that the operation-orthogonal transformations are carried out in parallel signals according to the selected grounds. One of the basic operations of DSP effectively implemented in polynomial system of residue classes is multiplication modulo. This paper presents a new algorithm for the operation of multiplication modulo, as well as the circuit implementation of this algorithm.

Keywords: polynomial system of residue classes, residue number system, digital signal processing, modular operations, modulo multiplier

На современном этапе развития к системам цифровой обработки сигналов (ЦОС) предъявляются высокие требования к быстродействию. Обеспечение реального масштаба времени позволит проводить ЦОС уже на первом этапе обработки. Это позволит повысить эффективность выполнения ортогональных преобразований сигналов, снизить схемные затраты, а также будет способствовать повышению точности выполняемых вычислений. Решить данную проблему можно за счет перехода к параллельным вычислениям.

Применение непозиционных параллельных модулярных кодов является одним из основных направлений, позволяющим решить проблему обеспечения выполнения алгоритмов ЦОС в реальном масштабе времени.

Среди множества алгоритмов ЦОС, реализованных с помощью непозиционных модулярных кодов, можно выделить две группы. Основу первой группы составляют методы и алгоритмы ортогональных преобразований сигналов с использованием системы остаточных классов (СОК) [1–3]. В этом случае цифровое преобразование входного вектора сигнала $\{x(0), x(1)\, x(2),..., x(N-1)\}$ спектральное представление $\{X(0), X(1), X(2),..., X(N-1)\}$ можно представить в виде выражения

$$\begin{cases} X(k) \bmod p_1 = \left| \sum_{l=0}^{N-1} \left| x(l) \right|_{p_1}^{+} \left| W^{lk} \right|_{p_1}^{+} \right|_{p_1}^{+} \\ \vdots \\ X(k) \bmod p_n = \left| \sum_{l=0}^{N-1} \left| x(l) \right|_{p_n}^{+} \left| W^{lk} \right|_{p_n}^{+} \right|_{p_{n1}}^{+} \end{cases}, \quad (1)$$

где W^{lk} – поворачивающий коэффициент; $k = 0,1,2,\ldots, N\text{-}1$; $N = 2^{v}$; $p_1, p_2, \ldots, p_n$ – основания системы остаточных классов.

Анализ выражения (1) показывает, что к достоинствам системы остаточных классов можно отнести высокую производительность выполнения основных модульных операций, к которым относятся сложение, вычитание и умножение. Другими словами для двух чисел $A = (\alpha_1, \alpha_2,\ldots, \alpha_n)$ и $B = (\beta_1, \beta_2,\ldots, \beta_n)$, справедливы равенства

$$A+B=\left((\alpha_1+\beta_1)\bmod p_1,(\alpha_2+\beta_2)\bmod p_2,\ldots,(\alpha_n+\beta_n)\bmod p_n\right). \quad (2)$$

$$A-B=\left((\alpha_1-\beta_1)\bmod p_1,(\alpha_2-\beta_2)\bmod p_2,\ldots,(\alpha_n-\beta_n)\bmod p_n\right). \quad (3)$$

$$A\cdot B=\left((\alpha_1\cdot\beta_1)\bmod p_1,(\alpha_2\cdot\beta_2)\bmod p_2,\ldots,(\alpha_n\cdot\beta_n)\bmod p_n\right). \quad (4)$$

Основу второй группы непозиционных кодов, позволяющих эффективно реализовать алгоритмы цифровой обработки сигналов, являются коды полиномиальной системы классов вычетов (ПСКВ). Как показано в работах [4–6], использование ПСКВ позволяет не только повысить скорость выполнения алгоритмов, но и обеспечить высокую точность вычислений за счет обработки целочисленных данных. В этом случае выражение (1) будет представляться в следующем:

$$X_l^k(z)=\sum_{n=0}^{d-1}x_l^n(z)\beta_l^{kn}(z), \quad (5)$$

где $\{ X_l^k(z),x_l^n(z),\beta_l^{kn}(z) \}\in P_l(z)$, $l = 1, 2,\ldots, m$; $k = 0,1,\ldots d–1$; $\beta_j(z)$ – первообразный элемент порядка d для локального кольца $P_l(z)$; $p_1(z)$, $p_2(z),\ldots, p_l(z)$ неприводимые полиномы, порождающие кольцо $P_l(z)$.

Данную математическую модель цифровой обработки сигналов (5) можно представить в виде системы уравнений:

$$\begin{cases} X_1(l)=\sum_{j=0}^{d-1}x_1(j)\beta_1^{jl}\bmod p_1(z) \\ \vdots \\ X_n(l)=\sum_{j=0}^{d-1}x_n(j)\beta_n^{jl}\bmod p_n(z) \end{cases}, \quad (6)$$

Как и ранее, вычисления алгоритмов цифровой обработки сигналов организуются параллельно, помодульно и независимо друг от друга. Другими словами, для суммы, разности и произведения двух полиномов $A(z)$ и $B(z)$, имеющих соответственно модулярные коды $(\alpha_1(z),\alpha_2(z),...,\alpha_n(z))$ и $(\beta_1(z),\beta_2(z),...,\beta_n(z))$, справедливы соотношения при $i = 1,\ldots,n$:

$$A(z)+B(z)=\left((\alpha_1(z)+\beta_1(z))\bmod p_1(z),,\ldots,(\alpha_n(z)+\beta_n(z))\bmod p_n(z)\right). \quad (7)$$

$$A(z)-B(z)=\left((\alpha_1(z)-\beta_1(z))\bmod p_1(z),,\ldots,(\alpha_n(z)-\beta_n(z))\bmod p_n(z)\right). \quad (8)$$

$$A(z)\cdot B(z)=\left((\alpha_1(z)\cdot\beta_1(z))\bmod p_1(z),,\ldots,(\alpha_n(z)\cdot\beta_n(z))\bmod p_n(z)\right). \quad (9)$$

Анализ выражений (5) и (6) показывает, что одной из операций, которые используются в алгоритмах ЦОС, реализованных в кодах ПСКВ, является операция умножения по модулю. Поэтому разработка алгоритма и структуры умножителя по модулю, обладающего минимальными схемными затратами, является актуальной задачей.

В работах [7–9] приведен нейросетевой подход, позволяющий построить умножитель по модулю на основе нейросетевого базиса. Несмотря на то что нейронные сети, как и коды ПСКВ, обладают параллельной архитектурой, предложенный подход не позволил достичь минимальных схемных затрат не реализацию базовых модульных операций. В работе [10] предлагается снизить схемные затраты на реализацию модульных операций ПСКВ за счет применения генетического алгоритма. При этом использование мажоритарного генетического алгоритма с выделенной доминантой при обучении нейронной сети (НС), реализующей модульную операцию, не полностью позволило снизить затраты на реализацию НС. Это обусловлено тем, что в качестве синаптических весов в такой НС используются не только положительные значения.

Рассмотрим новый алгоритм реализации операции умножения по модулю. При проведении умножения по модулю $p(z)=z^4+z+1$, двух операндов $A(z)$ и $B(z)$, степени которых удовлетворяют условию:

$$\begin{aligned} &\deg A(z)<\deg p(z) \\ &\deg B(z)<\deg p(z)\text{,} \end{aligned} \quad (10)$$

могут быть получены результаты, которые являются элементами поля Галуа $GF(2^4)$. В табл. 1 приведены ненулевые элементы поля $GF(2^4)$, порождаемые неприводимым полиномом $p(z)=z^4+z+1$.

Так как операнды $A(z)$ и $B(z)$ представляют собой четырехразрядные комбинации, то максимальная степень их полиномиальной формы записи будет равна трем. Поэтому необходимо определить результаты каждого разряда первого операнда $A(z)$ на каждый разряд операнда $B(z)$. Пусть полином $A(z)$ последовательно принимает значения 1, z, z^2, z^3.

Результаты умножения $A(z)B(z)$ по модулю $p(z) = z^4 + z + 1$ приведены в табл. 2.

Обобщая данные, приведенные в табл. 2, можно определить, какие разряды операндов $A(z)$ и $B(z)$ участвуют в получении каждого разряда произведения $A(z)B(z) \bmod p(z)$. Результаты приведены в табл. 3.

Рассмотрим первую строку табл. 3. Для того чтобы получить произведение $A(z)B(z) \bmod p(z) = 1$, при условии, что операнд $A(z) = 1$, необходимо условие, что $B(z) = 1$. Таким образом, для выполнения операции умножения по модулю для данных разрядов операндов достаточно использовать двухвходовой элемент И. Аналогичный результат получается для строки 2, 3, 4, 5, 9, 10, 13, 14, 15 табл. 3.

Рассмотрим шестую строку табл. 3. Для того чтобы получить значения произведения $A(z)B(z) \bmod p(z) = z$ при условии, что первый операнд $A(z) = z$, значение второго операнда $A(z) = z$ может быть 1 или z^3. Это обусловлено равенствами

$$z \cdot 1 \bmod z^4 + z + 1 = z$$

$$z \cdot z^3 \bmod z^4 + z + 1 = z^4 \bmod z^4 + z + 1 = z + 1,$$

в произведениях которых присутствует значение z.

Если одновременно подать единичный сигнал на разряды 1 и z^3 второго операнда $B(z)$, при условии, что $A(z) = z$, то получаем результат:

$$A(z)B(z) \bmod z^4 + z + 1 = (z(z^3 + 1)) \bmod z^4 + z + 1 = (z^4 + z) \bmod z^4 + z + 1 = 1.$$

Этот результат получается, если сложить результаты двух произведений по модулю два

$$(z \cdot 1) \bmod z^4 + z + 1 + (z \cdot z^3) \bmod z^4 + z + 1 = z + z + 1 = 1.$$

Таблица 1

Элементы мультипликативной группы конечного поля $GF(2^4)$

Степень элемента	Полиномиальная форма	Двоичный код	Степень элемента	Полиномиальная форма	Двоичный код
β^0	1	0001	β^8	$z^2 + 1$	0101
β^1	z	0010	β^9	$z^3 + z$	1010
β^2	z^2	0100	β^{10}	$z^2 + z + 1$	0111
β^3	z^3	1000	β^{11}	$z^3 + z^2 + z$	1110
β^4	$z + 1$	0011	β^{12}	$z^3 + z^2 + z + 1$	1111
β^5	$z^2 + z$	0110	β^{13}	$z^3 + z^2 + 1$	1101
β^6	$z^3 + z^2$	1100	β^{14}	$z^3 + 1$	1001
β^7	$z^3 + z^1$	1011			

Таблица 2

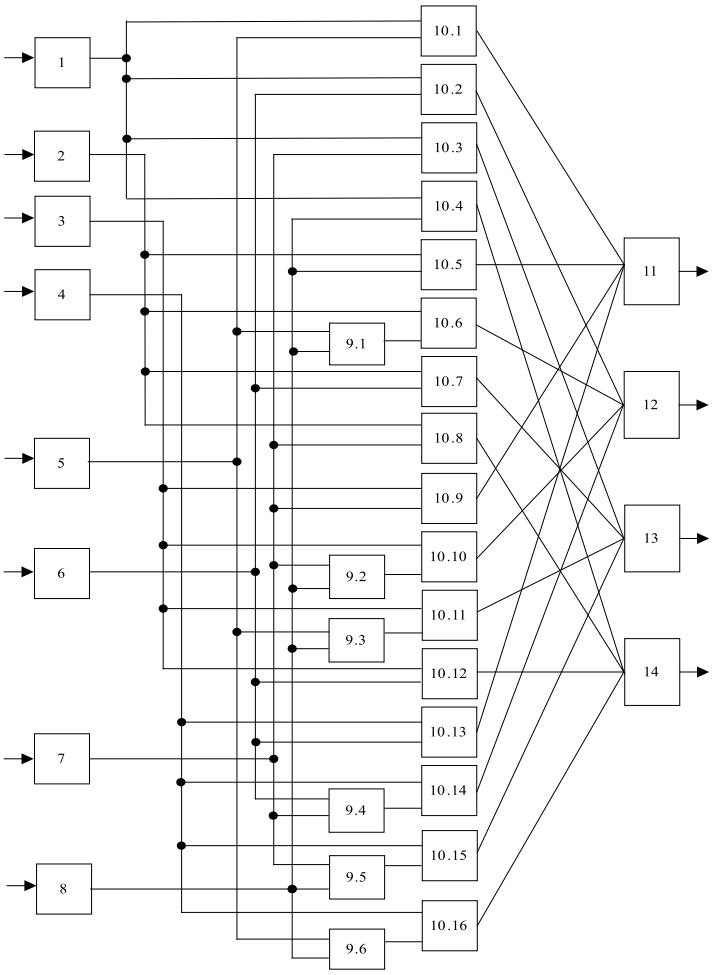
Результаты умножения $A(z)B(z) \bmod z^4 + z + 1$.

$A(z)$	$B(z)$	$A(z)B(z) \bmod p(z)$
1	1	1
	z	z
	z^2	z^2
	z^3	z^3
z	1	z
	z	z^2
	z^2	z^3
	z^3	$z + 1$
z^2	1	z^2
	z	z^3
	z^2	$z + 1$
	z^3	$z^2 + z$
z^3	1	z^3
	z	$z + 1$
	z^2	$z^2 + z$
	z^3	$z^3 + z^2$

Таблица 3

Результаты произведения $A(z)B(z) \bmod p(z)$

№ п/п	Разряды		
	$A(z)B(z) \bmod p(z)$	$A(z)$	$B(z)$
1	1	1	1
2	1	z	z^3
3	1	z^2	z^2
4	1	z^3	z
5	z	1	z
6	z	z	1, z^3
7	z	z^2	z^2, z^3
8	z	z^3	z, z^2
9	z^2	1	z^2
10	z^2	z	z
11	z^2	z^2	1, z^3
12	z^2	z^3	z^2, z^3
13	z^3	1	z^3
14	z^3	z	z^2
15	z^3	z^2	z
16	z^3	z^3	1, z^3



Структура умножителя по модулю $p(z) = z^4 + z + 1$

Значит, чтобы решить данную проблему, необходимо использовать двухвходовой сумматор по модулю два, на входы которого подаются сигналы с 1 и z^3 второго операнда $B(z)$. Выход этого сумматора по модулю два подключается на второй вход элемента И, на первый вход которого поступает сигнал в разряде z первого операнда $A(z)$. Аналогичный результат получается для строк 6, 7, 8, 11, 12, 16 табл. 3. На рисунке приведена структура умножителя по модулю.

Умножитель содержит входы 1–4, на которые поступает в двоичном коде первый операнд $A(z)$, входы 5–8, на которые подается двоичный код второго операнда $B(z)$, блок двухвходовых сумматоров по модулю два 9.1–9.6, блок двухвходовых элементов И 10.1–10.16, сумматоры по модулю два 11–14, выходы которых являются выходом умножителя по модулю. При этом младшие разряды «1» первого и второго операндов $A(z)$ и $B(z)$ поступают на входы 1 и 5 соответственно, а старший разряд z^3 – соответственно на входы 4 и 8. Выход сумматора по модулю два 11 соответствует младшему разряду произведения, а выход сумматора по модулю два 14 – старшему разряду произведения $A(z)B(z) \bmod p(z)$.

Рассмотрим работу умножителя по модулю. Пусть $A(z) = z^3 + z^2 + 1$ и $B(z) = z^3 + 1$. Тогда их произведение по модулю $p(z) = z^4 + z + 1$ равно

$$(z^3 + z^2 + 1)(z^3 + 1) \bmod z^4 + z + 1 =$$

$$= (z^6 + z^5 + z^3 + z^3 + z^2 + 1) \bmod z^4 +$$

$$+ z + 1 = (z^6 + z^5 + z^2 + 1) \bmod z^4 +$$

$$+ z + 1 = z^3 + z^2 + z + 1.$$

Следовательно, единичные сигналы должны появиться на выходах всех сумматоров по модулю два 11–14.

Рассмотрим работу схемы. В соответствии с выбранными значениями $A(z)$ и $B(z)$ единичный сигнал будет на входах 1, 3, 4, 5, 8 умножителей по модулю, а на остальных – нулевой сигнал. Тогда на выходах сумматоров по модулю два 9.2 и 9.5 будут получены единичные сигналы, а на всех остальных – нули.

Так как на 1 и 1 входы умножителя поступили единичные сигналы, то на выходе двухвходового элемента И 10.1 появится единичный сигнал. Так как на 1 и 8 входы умножителя поступили единичные сигналы, то на выходе двухвходового элемента И 10.4 также появится единичный сигнал. Так как на входы элемента И 10.10 поданы единичные сигналы с выхода элемента 9.2 и входа 3, то на его выходе также будет единичный сигнал. При этом т.к. на входы элемента И 10.15 поданы единичные сигналы с выхода элемента 9.5 и входа 4, то на его выходе также будет единичный сигнал.

Единичный сигнал с выходов элементов 10.1, 10.4, 10.10, 10.15 подается на соответствующие входы сумматоров по модулю два 11–14. В результате на выходах этих сумматоров появятся единичные сигналы. Полученные данные совпали с контрольным просчетом.

Выводы

Применение непозиционных модулярных кодов позволяет повысить скорость выполнения ортогональных преобразований сигналов. При этом наблюдается ситуация, когда происходит возрастание схемных затрат, необходимых для построения спецпроцессоров ЦОС. В работе предложен алгоритм выполнения операции по модулю, а также его схемная реализация. Использование данного умножителя позволяет обеспечить высокую скорость выполнения операции умножения по модулю при меньших схемных затратах.

Список литературы

1. Гончаров П.С., Калмыков М.И., Степанова Е.П. Непозиционный код класса вычетов в параллельных технологиях цифровой обработки сигналов // Успехи современного естествознания. РАЕ – 2014. – № 3. – С. 102–107; URL: www.rae.ru/use/?section=content&op=show_article&article_id=10002446.

2. Гапочкин А.В., Калмыков М.И., Айриян А.А. Коррекция ошибки в модулярном коде на основе алгоритма параллельного вычисления следа // Международный журнал экспериментального образования. – 2014. – № 8–3. – С. 34–38; URL:www.rae.ru/meo/?section=content&op=show_article&article_id=5926.

3. Гапочкин А.В., Калмыков М.И., Васильев П.С. Обнаружение и коррекция ошибки на основе вычисления интервального номера кода классов вычетов // Современные наукоёмкие технологии. – 2014. – № 6. – С. 9–14; URL: www.rae.ru/snt/?section=content&op=show_article&article_id=10003249.

4. Калмыков И.А., Зиновьев А.В., Емарлукова Я.В. Высокоскоростные систолические отказоустойчивые процессоры цифровой обработки сигналов для инфотелекоммуникационных систем // Инфокоммуникационные технологии. – 2009. – Т. 7, № 2. – С. 31–37.

5. 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.

6. Калмыков И.А., Резеньков Д.Н., Горденко Д.В., Саркисов А.Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. – Ставрополь, Фабула. 2014. – 180 с.

7. Калмыков И.А., Хайватов А.Б. Математическая модель отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов // Инфокоммуникационные технологии. – 2007. – Т. 5, № 3. – С. 39–42.

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

9. 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.

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