УДК 681.5

РАЗРАБОТКА АЛГОРИТМА ВОЗВЕДЕНИЯ В КВАДРАТ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Эрдниева Н.С.

аспирант

Северо-Кавказский федеральный университет

г. Ставрополь, Россия

Аннотация

Одной из важных проблем системы остаточных классов (СОК) является вычисление квадрата, которое применяется в приложениях ЦОС на основе СОК. Известно много методов, с помощью которых можно вычислить квадрат, но большинство из них имеют низкую скорость или требуют высоких затрат. В статье предлагается новый алгоритм, который может привести снижение скорости возведения в квадрат к задержке транзистора.

Ключевые слова: система остаточных классов, возведение в квадрат, Одно активное состояние системы.

THE DEVELOPMENT OF SQUARING ALGORITHM FOR RESIDUE NUMBER SYSTEM

Erdnieva N.S.

graduate student

North Caucasus Federal University

Stavropol, Russia

Abstract

Computing the square is one of the important problems in Residue Number System (RNS) that are applied in DSP applications based on RNS. There are many methods that can compute square but most of them have a low speed or need high space. A new algorithm is proposed in this paper that can decrease squaring speed to a transistor delay.

Keywords: Residue Number System, Squaring, One-Hot.

Введение

Поиск новых путей повышения производительности вычислительных устройств привели к выводу, что нейрокомпьютерная технология является одним из наиболее перспективных направлений развития вычислительной техники, основу которой составляют искусственные нейронные сети (ИНС) [1, с.13]. Для представления и обработки данных в ИНС могут быть использованы позиционные и непозиционные системы счисления [2, с. 24], наиболее востребованной из которых является система остаточных классов [3, с. 91]. Одна из важнейших характеристик системы заключается в отсутствии необходимости учета межразрядных переносов при выполнении арифметических операций над числами [4, с. 218].

СОК представляет собой набор модулей $\{m_1, m_2, m_3, \ldots, m_n\}$ - положительные целые числа, и каждые две пары из них взаимно просты. Самым большим возможным динамическим диапазоном является $[\alpha, \alpha + M)$ и M состоит из: $M = \prod_{i=1}^{n} m_i$. В СОК каждое число X в диапазоне $\alpha \le X \le \alpha + M$ имеет единственное представление, которое может быть представлено с набором остатков, как: $(x_1, x_2, x_3, \ldots, x_n)$ в то время как: $X_i = X \bmod m_i$, $i = 1,2,3,\ldots,n$

Для получения X из этих остатков $(x_1, x_2, x_3, \ldots, x_n)$ используется Китайская теорема об остатках и X получают по формуле (1):

$$X = \left(\sum_{i=1}^{n} \left(x_i N_i \right) m_i \times M_i \right)_M$$

$$M = \prod_{i}^{n} m_i, \; M_i = \frac{M}{m_i} \qquad (1)$$

$$N_i = \left(M_i^{-1} \right)_{m_i}, \; i = 1,2,3,\ldots,n$$

В формуле (1) $\left(M_i\right)^{-1}$ является мультипликативным обратным M_i с модулем m_i.

Возведение в квадрат

Предположим, мы хотим возвести в квадрат *A*, который является остатком *X* по модулю m, и $A < m$.

$$n = \left[\log_2^{(m)} \right] + 1, \; A = \sum_{i=0}^{n} a_i 2^i$$

Сейчас можно записать [3]

$$|Z|_m = |A \times A|_m = \left| \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i a_j 2^{i+j} \right|_m \quad (2)$$

Таким образом, для возведения в квадрат схемы по модулю *m* нужно вычислить $\left|A^2\right|_m$. Ранее возведение в квадрат использовалось в приложениях ЦОС, на основе СОК. Кроме того, произведение двух остатков по модулю *m* может быть вычислено путем возведения в квадрат [5, с.167] по формуле (3).

$$|XY|_m = \left| \frac{(X+Y)^2 - (X-Y)^2}{4} \right|_m \quad (3)$$

Одно активное состояние Системы остаточных классов

В СОК остатки числа по модулю *m* находятся в диапазоне от $[0, m-1]$. В Одном активном состоянии системы *m* линии сигнала предназначены для этих остатков, как и для остатков равных *k*, причем *k*-ые линии являются активными, а другие линии - неактивными. Например, Одно активное представление по модулю 5 показано ниже (рис. 1).

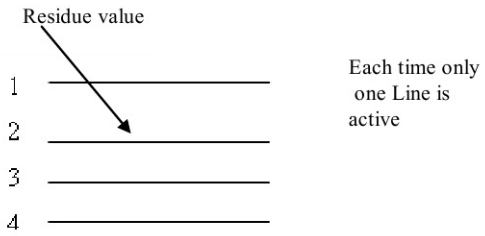

Рис. 1 – Одно активное представление по модулю 5

Низкое энергопотребление является одним из главных преимуществ Одно активного состояния системы. Потому что в данном представлении системы две линии максимально изменятся путем изменения входного значения.

Например, если в Одно активном состоянии системы по модулю пять, число входа изменится с 4 до 3, третий бит должен быть активирован, а четвертая линия должна быть дезактивирована, что приведёт к снижению потребления энергии.

Для реализации суммирования в Одном активном состоянии системы по модулю *m*, результаты первого суммирования должны быть рассчитаны для двух произвольных операторов СОК. Например, если *x* и *y* - это два операнда СОК в отношении 5, их результат суммирования по этому модулю $((x+y)_5)$ для различных значений *x* и *y* приведен в Таблице 1.

Таблица 1 – Результат суммирования по модулю 5 для различных значений *x* и *y*, $((x+y)_5)$

X	0	0	1	0	1	2	0	1	2	3	0	1	4	3	4
Y	0	1	1	2	2	2	3	3	3	3	4	4	2	4	4
$(X+Y)_5$	0	1	2	2	3	4	3	4	0	1	4	0	1	2	3

Так как оператор суммирования является коммутативным оператором, некоторые из случаев не показаны в данной таблице.

В определенный момент времени для каждых входов активна только одна линия, поэтому нужен только один транзистор для реализации каждых случаев суммирования (рис. 2).

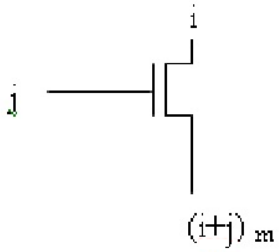

Рис. 2 – Пример суммирования в Одном активном состоянии системы

На данном рисунке *i*-тая линия первого операнда показывает номер *i*, а *j*-тая линия второго операнда показывает номер *j*, поэтому источник выводит транзистор к обозначению $(i+j)_m$. Значит, сумматор Одно активного состояния по модулю 5 может быть реализован следующим образом (рис. 3).

Для каждого случая уделяется один транзистор, как только источник этих транзисторов указывает на результат суммирования. Все те же самые выходы соединены друг с другом, но для упрощения эти связи не показаны на данном рисунке. Для определения к какой линии должны быть подключены выходы каждого транзистора зависит результат сложения по модулю.

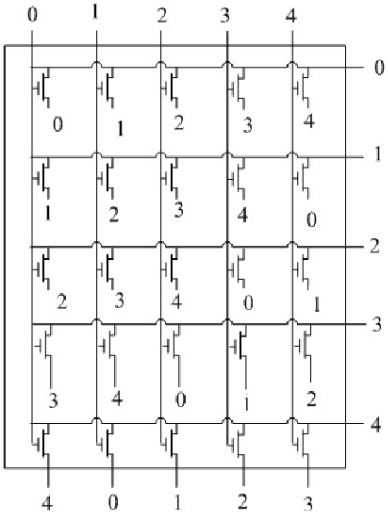

Рис. 3 – Одно активное состояние суммирования по модулю 5

Например, по модулю 5, результат $(4+3)_5$ равен 2, тогда выходы двух транзисторов, которые выполняют $(4+3)_5$ и $(3+4)_5$ соответственно, соединяются с выходом линии 2. Следует отметить, что эта задержка сумматора равна задержке одного транзистора.

Новая идея

Ранее в Одном активном состоянии системы для каждого входного числа активной была только одна строка. Предположим, требуется вычислить квадрат двух чисел с 3 битами $(X_2\ X_1\ X_0)$. Возможные случаи перечислены в Таблице 2.

Таблица 2 – Возведение в квадрат результатов по модулю 5

X	0	1	2	3	4

$\left(X^2\right)_5$	$(0)_5 = 0$	$(1)_5 = 1$	$(4)_5 = 4$	$(9)_5 = 4$	$(16)_5 = 1$

Схема возведения в квадрат по модулю 5 показана ниже (рис. 4).

В том случае, когда два входа равны, и в определенный момент времени в Одном активном состоянии системы активна только одна линия, тогда используются только транзисторы, размещенные по диаметру, а другие не нужны. Поэтому схема может быть упрощена следующим образом (рис. 5).

В конечном итоге эта схема может быть изображена так (рис. 6).

Отметим, что для возведения в квадрат по модулю 5 необходимо 5 транзисторов. В общем случае, для возведения в квадрат по модулю *m*, необходимо *m* транзисторов.

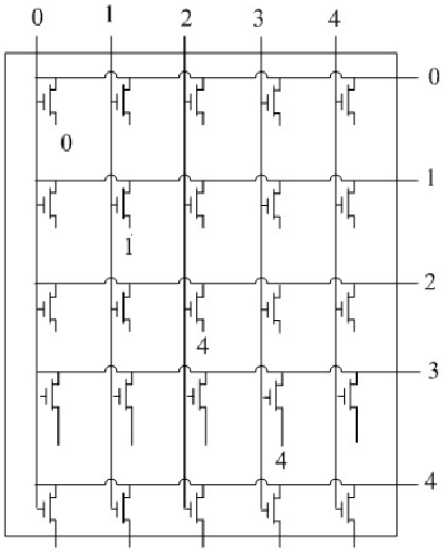

Рис. 4 – Схема возведение в квадрат по модулю 5

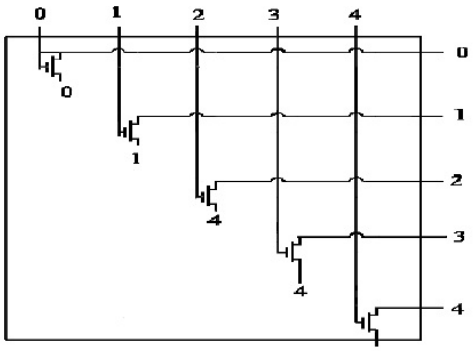

Рис. 5 – Упрощенная схема возведения в квадрат по модулю 5

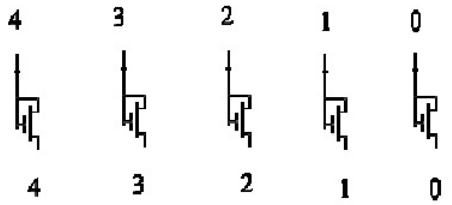

Рис. 6 – Итоговая упрощенная схема возведения в квадрат по модулю 5

Заключение

В данной статье проведены исследования возведения в квадрат в системе остаточных классов и в Одном активном состоянии системы остаточных классов. Предложен новый алгоритм возведения в квадрат на основе Одного активного состояния по модулю m. Одно активное состояние систем остаточных классов имеет некоторые преимущества, такие как: реализация схемы низкого энергопотребления и низкой задержки вычисления в одном транзисторе. С другой стороны, в новом алгоритме возведения в квадрат для каждого произвольного модуля m используется m транзисторов и операция возведения в квадрат выполняется с задержкой, равной задержки одного транзистора. Число транзисторов увеличивается пропорционально модулю за счет увеличения модуля, поэтому этот метод подходит только для маленьких модулей.

Таблица 3 – Необходимые аппаратные средства для реализации возведения в квадрат по модулю 2^5, 2^5+1, 2^5-1

Модуль	*NAND*	*AND*	*FA*	FA^{+1}	*HA*	*NOT*	Задержка
2^5	----	10	1	----	3	-	*3HA+AND*
2^5+1	6	4	5	2	3	2	*HA+FA+CPA+AND*
2^5-1	-10	10	5	----	0	-	*FA+CPA+AND*

Для проверки эффективности нового алгоритма, он сравнивается по модулю 2^n с [5, с. 169] и по модулю 2^n-1 и 2^{n+1} с [5, с. 171] и [6, с. 35]. Необходимые аппаратные средства для реализации возведения в квадрат схемы по модулю 2^n, 2^n-1 и 2^{n+1} приведены в Таблице 3 на основе [5, с. 173].

Таблица 4 – Необходимые аппаратные средства для реализации возведения в квадрат по модулю 2^5-1 с алгоритмом, упомянутым в [3].

AND	*FA*	*HA*	*MUX*	Задержка
6	1	3	4	*FA+MUX+CPA+AND*

В Таблице 4 на основе [6, с. 38] приведены аппаратные средства и вычисление задержки для возведения в квадрат по модулю 2^5-1. FA^+ - это Полный Сумматор с входным носителем равным 1 и задержкой, равной половине сумматора, его входная схема показана ниже (рис. 7) [5, с. 174].

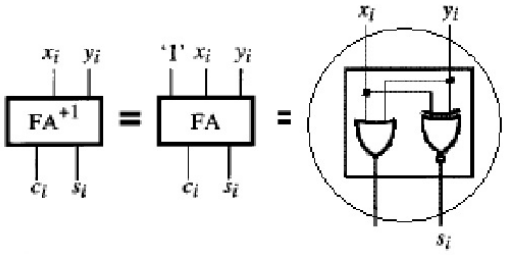

Рис. 7 – Внутренняя схема FA^{+1}

Выводы: продолжительность вычисления квадрата остатка СОК на основе Одно активного состояния системы равна задержке одного транзистора. Таким образом, у нового алгоритма задержка ниже, чем у других методов, упомянутых в Таблице 3 и 4. Значит, для нового предложенного метода требуется меньше транзисторов, чем в [5, с. 176] и [6, с. 39]. Для модуля m необходимо m транзисторов для вычисления квадрата в Одном активном состоянии системы, тогда для модулей 2^5-1, 2^5+1, 2^5 требуется транзисторов в отношении, 31, 33, 32 транзисторов.

Библиографический список:

1. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Макоха А.Н. Нейрокомпьютеры в системе остаточных классов. Кн. 11: Учебное пособие для вузов.- М.: Радиотехника, 2003, - с. 272.

2. Пронин С.В. Применение искусственных нейронных сетей для моделирования транспортных систем // Автомобильный транспорт (Харьков, ХНАДУ). - 2006. - №18.

3. Ермоленко А.Г., Ермоленко Г.Ю., Степанова М.А. Модифицированное дискретное преобразование Фурье // Вестник транспорта Поволжья. - 2011. - №3.

4. Jafarali Jassbi S., Hosseinzadeh M., Gorgin S., Navi K. One-Hot Multilevel Residue Number System // IEEE EWDTS. Yerevan. September 7-10, 2007.

5. Hariri A., Navi K., Rastegar R. Simplified Modul $\left(2^n-1\right)$ Squaring Scheme for Residue Number System // IEEE International Conference on Computer as a tool. Nov. 2005.

6. Piestrak S. Design of squarers modulo a with low-level pipelining // IEEE Transactions on Circuits and Systems II. - 2002. - V.49, №1. - p.31-41.

Оригинальность 89%