УДК 621.391.825

К ВОПРОСУ ОЦЕНКИ СЛОЖНОСТИ ПОСТРОЕНИЯ И БЫСТРОДЕЙСТВИЯ МНОГОРАЗРЯДНЫХ ПАРАЛЛЕЛЬНЫХ СУММАТОРОВ ПО МОДУЛЮ С ПОСЛЕДОВАТЕЛЬНЫМ ПЕРЕНОСОМ

Петренко В.И., Жук А.П., Кузьминов Ю.В., Тебуева Ф.Б.

ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, Россия (355029, г. Ставрополь, просп. Кулакова, 2), e-mail: info@ncfu.ru

В статье проведен анализ принципов построения многоразрядных сумматоров по модулю с последовательным переносом. Рассмотрены особенности построения данного класса устройств, а также способ формирования остатка от сложения двух чисел из диапазона (0...m) по произвольному модулю m. Установлено, что одноразрядные сумматоры по модулю, построенные с использованием предложенного способа, должны иметь шесть входов и три выхода, в отличие от обычных сумматоров. Предложена схема одноразрядного сумматора по модулю, для которого проведена оценка сложности построения сумматора по модулю с помощью оценки затрат оборудования по Квайну. На основании предложенного способа формирования остатка и схемы одноразрядного сумматора предложена схема многоразрядного параллельного сумматора по модулю с последовательным переносом с оценкой сложности построения и быстродействия устройства, а также алгоритм его работы.

Ключевые слова: суммирование по модулю, сумматор, быстродействие, последовательный перенос.

ON THE APPRAISAL DIFFICULTY OF CONSTRUCTION AND SPEED OF MULTI-BIT PARALLEL ADDER MODULO WITF SEQUENTIALLY TRANSFER

Petrenko V.I., Zhuk A.P., Kuzminov Y.V., Tebuyeva F.B.

FSAEI HPE «North-Caucasus Federal University», Stavropol, Russia (355029, Stavropol, Kulakov Prospect, 2), e-mail: info@ncfu.ru

This article analyzes the construction principles for multi-bit modulo adders with sequential shifting. On the article was analyzed the features of the construction for this class of devices, and a method for forming the remainder of the addition of two numbers in the range (0 ... m) for an arbitrary modulus m. Found that single-bit adders modulo constructed using the present method should have six inputs and three outputs, unlike conventional adders. Also, was proposed a scheme of one-bit adder module for which an assessment of the construction adder module with equipment costing by Quine. Based on the proposed method of forming a residue and the one-bit adder circuit, proposed a scheme of multibit parallel adder with serial transfer module with the complexity of construction and performance of the device and its ability to work.

Keywords: modulo adding, adding, perfomance, sequential transfer.

Введение

Современные системы хранения, передачи и обработки цифровой информации построены с использованием основных положений теории конечных полей. Так, большинство алгоритмов теоретико-числовых преобразований используют процедуры вычисления остатков в конечных полях. Настоятельность данной операции заключается в том, что при выполнении любых типовых арифметических операций в конечных полях результаты вычислений могут выходить за пределы диапазона значений конечного поля, что вызывает необходимость приведения этих результатов в область определений заданного конечного поля. При выполнении различных теоретико-числовых преобразований в системах хранения, передачи и обработки цифровой информации достаточно часто используется операция сложения чисел по модулю. Таким образом, актуальной является

задача оценки сложности и быстродействия многоразрядных параллельных сумматоров по модулю с последовательным переносом, которые могут быть использованы при реализации различных теоретико-числовых преобразований в системах хранения, передачи и обработки цифровой информации.

Принципы построения полных многоразрядных сумматоров по модулю состоят в следующем [3].

При сложении двух чисел, представленных в виде двоичных кодов A (a_1, ..., a_n) и B (b_1, ..., b_n) образуется сумма C (c_1, ..., c_{n+1}). Чтобы найти результат суммирования чисел A и B по модулю M(m_1, …m_{n+1}), необходимо найти решение разности C (c_1, ..., c_{n+1}) – M(m_1, …, m_{n+1}). Если полученное значение отрицательно, то S(s_1,…, s_{n+1})= C (c_1, ..., c_{n+1}), если положительное, то S(s_1,…, s_{n+1})= C (c_1, ..., c_{n+1}) – M(m_1, …, m_{n+1}). Иными словами, принцип построения сумматоров по модулю заключается в реализации следующего способа суммирования двух чисел $0 \le a < m$ и $0 \le b < m$ по модулю m. Если (a+b)<m, то выполняется обычное суммирование S=a+b, и эта сумма S является результатом. Если же (S=a+b)>m и по исходному условию сумма S при $0 \le a < m$ и $0 \le b < m$ не может превышать 2m-2, то из суммы S вычитается значение m и результат является суммой (a+b) mod m [4]. При этом на выходе переноса сумматора, осуществляющего вычитание, появляется сигнал. Данный сигнал является признаком превышения суммой S значения m и используется для выбора результата (a+b) или (a+b)-m. В соответствии с этим полный одноразрядный сумматор по модулю, из которого затем может быть составлен сумматор по модулю для произвольного числа разрядов, должен выполнить суммирование a_i и b_i разрядов с учетом разряда переноса p_{i-1} из младших разрядов и полученную сумму S_i выдать на выход устройства при отсутствии сигнала переноса модуля со старшего разряда или вычесть из нее разряд модуля m_i при наличии такового [2].

Таким образом, одноразрядные сумматоры по модулю должны иметь шесть входов и три выхода, в отличие от обычных сумматоров, которые имеют три входа и два выхода. Дополнительно ко входам разрядов слагаемых a_i и b_i и входу переноса из предыдущего разряда p_{i-1} в одноразрядном сумматоре по модулю добавляется вход модуля m_i, вход переноса модуля из предыдущего разряда pm_{i-1} и управляющий вход W. Дополнительно к выходу суммы S_i и выходу переноса в следующий разряд p_i добавляется выход переноса модуля в следующий разряд pm_i.

На рисунке 1 представлена схема одноразрядного параллельного сумматора по модулю с последовательным переносом. На рисунке 2 представлено условное графическое обозначение одноразрядного сумматора по модулю.

Полный одноразрядный сумматор по модулю содержит [1] 7 логических элементов «НЕ», 7 двухвходовых логических элементов «И», 4 четырехвходовых логических элементов «И», 4 трехвходовых логических элементов «И», 2 трехвходовых логических элементов «ИЛИ», 1 четырехвходовый логический элемент «ИЛИ», 1 пятивходовый логический элемент «ИЛИ». На вход 1 подается разряд первого числа суммирования a_i, на вход 2 – второго числа суммирования b_i. Вход 3 служит входом переноса числа p_{Ini}, вход 4 – входом переноса модуля pm_{Ini}. На вход 5 подается разряд модуля m_i. Вход 6 является управляющим входом W. Выход 7 является выходом переноса p_{Outi}, выход 8 – выходом переноса модуля pm_{Outi}. Выход 9 является информационным выходом S_i.

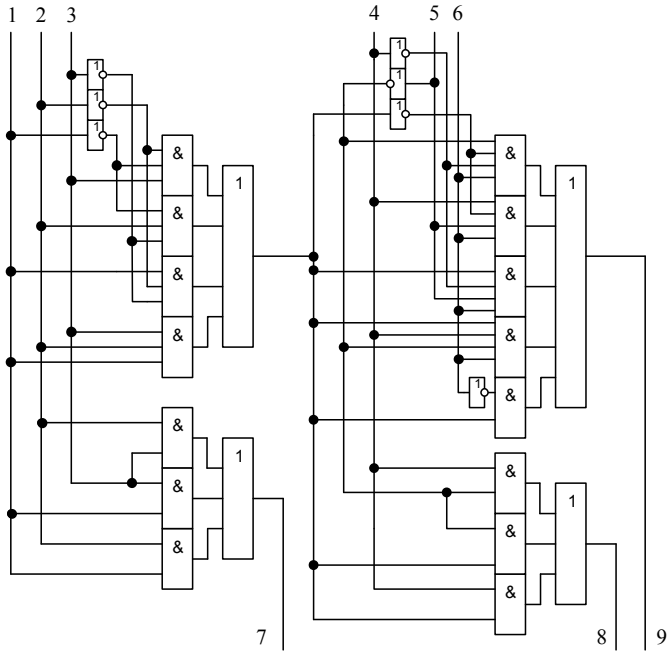

Рисунок 1. Одноразрядный сумматор по модулю

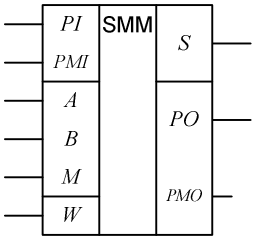

Рисунок 2. Условное графическое обозначение одноразрядного сумматора по модулю

Одноразрядный сумматор по модулю работает следующим образом. Полный одноразрядный сумматор по модулю состоит из логических элементов «НЕ», «И», «ИЛИ», соединенных таким образом, чтобы выполнялись следующие вычисления:

$$p_{Outi} = (b_i \wedge p_{Ini}) \vee (p_{Ini} \wedge a_i) \vee (b_i \wedge a_i);$$

$$S_{ab} = (\overline{b_i} \wedge \overline{a_i} \wedge p_{Ini}) \vee (\overline{a_i} \wedge b_i \wedge \overline{p_{Ini}}) \vee (a_i \wedge \overline{b_i} \wedge \overline{p_{Ini}}) \vee (a_i \wedge b_i \wedge p_{Ini});$$

$$pm_{Outi} = (pm_{Ini} \wedge \overline{m_i}) \vee (\overline{m_i} \wedge S_{ab}) \vee (pm_{Ini} \wedge S_{ab});$$

$$S_i = (\overline{m_i} \wedge \overline{S_{ab}} \wedge \overline{pm_{Ini}} \wedge W) \vee (pm_{Ini} \wedge \overline{S_{ab}} \wedge m_i \wedge W) \vee (S_{ab} \wedge \overline{pm_{Ini}} \wedge m_i \wedge W) \vee$$
$$\vee (S_{ab} \wedge pm_{Ini} \wedge \overline{m_i} \wedge W) \vee (\overline{W} \wedge S_{ab}),$$

где i=0,…,n. Данные выражения составлены в соответствии с таблицей истинности (табл. 1).

Таблица 1. Таблица истинности полного одноразрядного сумматора по модулю (фрагмент)

a_i	b_i	p_{Ini}	S_{ab}	p_{Ouit}	m_i	pm_{Ini}	W	pm_{Outi}	S_i
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	0	0	0	1
0	0	0	0	0	0	1	0	1	0
0	1	0	1	0	0	1	0	1	1
1	0	0	1	0	0	1	0	1	1
1	1	0	0	1	0	1	0	1	0
0	0	1	1	0	0	1	0	1	1
0	1	1	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0	1	0
1	1	1	1	1	0	1	0	1	1
0	0	0	0	0	1	1	0	0	0
0	1	0	1	0	1	1	0	1	1
1	0	0	1	0	1	1	0	1	1
1	1	0	0	1	1	1	0	0	0
0	0	1	1	0	1	1	0	1	1
0	1	1	0	1	1	1	0	0	0
1	0	1	0	1	1	1	0	0	0
1	1	1	1	1	1	1	0	1	1
0	0	0	0	0	0	0	1	0	1
0	1	0	1	0	0	0	1	1	0
1	0	0	1	0	0	0	1	1	0
1	1	0	0	1	0	0	1	0	1
0	0	1	1	0	0	0	1	1	0
0	1	1	0	1	0	0	1	0	1
1	0	1	0	1	0	0	1	0	1
1	1	1	1	1	0	0	1	1	0
0	0	0	0	0	1	0	1	0	0
0	1	0	1	0	1	0	1	0	1
1	0	0	1	0	1	0	1	0	1
1	1	0	0	1	1	0	1	0	0
0	0	1	1	0	1	0	1	0	1
0	1	1	0	1	1	0	1	0	0
1	0	1	0	1	1	0	1	0	0
1	1	1	1	1	1	0	1	0	1
0	0	0	0	0	0	1	1	1	0
0	1	0	1	0	0	1	1	1	1
1	0	0	1	0	0	1	1	1	1
1	1	0	0	1	0	1	1	1	0

a_i	b_i	p_{Ini}	S_{ab}	p_{Ouit}	m_i	pm_{Ini}	W	pm_{Outi}	S_i
0	0	1	1	0	0	1	1	1	1
0	1	1	0	1	0	1	1	1	0
1	0	1	0	1	0	1	1	1	0
1	1	1	1	1	0	1	1	1	1
0	0	0	0	0	1	1	1	0	1
0	1	0	1	0	1	1	1	1	0
1	0	0	1	0	1	1	1	1	0
1	1	0	0	1	1	1	1	0	1
0	0	1	1	0	1	1	1	1	0
0	1	1	0	1	1	1	1	0	1
1	0	1	0	1	1	1	1	0	1
1	1	1	1	1	1	1	1	1	0

Для оценки сложности построения сумматора по модулю применим оценку затрат оборудования по Квайну Q, определяемую числом входов всех элементов схемы [5]. Очевидно, что сложность полного одноразрядного сумматора по модулю будет равна Q=56. Оценим быстродействие данного сумматора. Перенос p_i и перенос модуля pm_i будут формироваться за время равное двум задержкам используемых логических элементов. Время выработки значения суммы S_i будет составлять четыре задержки используемых логических элементов. При оценке сложности время и аппаратные затраты на формирование инверсных значений кода входных переменных не учитывалось, так как обычно на шинах данных существуют как прямые, так и инверсные коды.

Предложенный одноразрядный сумматор по модулю является основой для построения многоразрядных параллельных сумматоров по модулю с последовательным переносом. На рисунке 3 представлена схема многоразрядного параллельного сумматора по модулю с последовательным переносом, составленная из полных одноразрядных сумматоров по модулю.

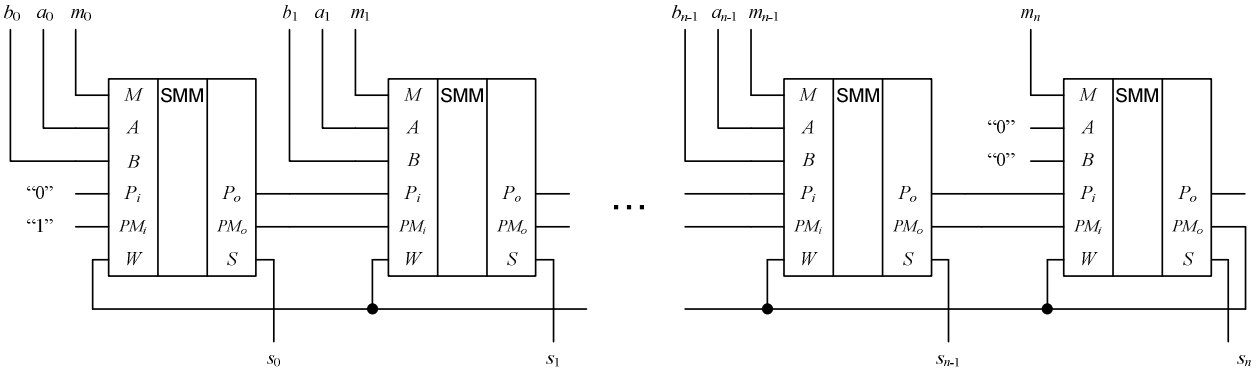

Рисунок 3. Многоразрядный параллельный сумматор по модулю с последовательным переносом

Многоразрядный параллельный сумматор по модулю с последовательным переносом содержит n+1 одноразрядных параллельных сумматоров по модулю, где n количество разрядов чисел суммирования. На вход А n сумматоров подается код числа A, на вход В n сумматоров подается код числа B. На входы А и Вn+1-ого сумматора подаются логические нули. На вход М всех сумматоров подается код числа M. На вход P_i первого сумматора подается логический ноль, на вход PM_i первого сумматора – логическая единица. Выход P_0j-го сумматора соединен со входом P_i (j+1)-го сумматора, выход PM_0j-го сумматора соединен со входом PM_i (j+1)-го сумматора, где j=1,…,n. Выход PM_0 (n+1)-го сумматора является выходом переноса модуля pm_{Out} устройства, который соединен с управляющим входом W всех n+1 сумматоров. Выходы S всех сумматоров являются информационными выходами устройства, на которые выдается сумма $C(c_1, ..., c_{n+1})$ чисел $A(a_1, ..., a_n)$ и $B(b_1, ..., b_n)$ по модулю $M(m_1, …, m_{n+1})$.

Многоразрядный параллельный сумматор по модулю с последовательным переносом работает следующим образом. На информационные входы сумматоров подаются в двоичном виде коды чисел суммирования $A(a_1, ..., a_n)$ и $B(b_1, ..., b_n)$ и код модуля $M(m_1, …, m_{n+1})$. Последовательно для каждого разряда каждым одноразрядным параллельным сумматором по модулю формируется перенос числа и перенос модуля. Если сигнал на выходе переноса модуля (n+1)-го одноразрядного параллельного сумматора по модулю равен единице, то из суммы (А+В) вычитается значение модуля, в противном случае два числа $A(a_1, ..., a_n)$ и B $(b_1, ..., b_n)$ суммируются обычным способом. При этом последовательно поразрядно формируется результат суммирования двух чисел $A(a_1, ..., a_n)$ и B $(b_1, ..., b_n)$ по модулю $M(m_1, …, m_{n+1})$.

Рассмотрим работу сумматора на примере.

Пусть $A=6_{10}=110_2$, $B=4_{10}=110_2$, $M=9_{10}=1001_2$. Воспользовавшись таблицей истинности полного одноразрядного сумматора 1 по модулю (табл.1), найдем промежуточные и конечный результаты суммирования по модулю. Устройство для данного примера будет содержать четыре одноразрядных параллельных сумматора по модулю.

На входы четырех сумматоров подаются коды чисел $A=110_2$, $B=110_2$, $M=1001_2$. На выходе первого сумматора $P_0=0$, $PM_0=0$. На выходе второго сумматора $P_0=0$, $PM_0=1$. На выходе третьего сумматора $P_0=1$, $PM_0=1$. На выходе четвертого сумматора $PM_0=1$ эта единица поступает на все входы W всех четырех сумматоров. В результате на выходе первого сумматора S=1, на выходе второго сумматора S=0, на выходе третьего сумматора S=0, на выходе четвертого сумматора S=0. На выходе устройства появляется число $0001_2=1_{10}$. Проверим: 6+4=10, 10≡1 mod 9.

Таким образом, оценка сложности и быстродействия многоразрядных параллельных сумматоров по модулю с последовательным переносом показывает, что сложность построения сумматоров составляет $56n$, а быстродействие оценивается $4n$, где n – количество разрядов сумматора.

Результаты, отраженные в данной статье, получены при финансовой поддержке ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009–2013 гг., соглашение №14.B37.21.0402.

Список литературы

1. Копытов В.В., Петренко В.И., Сидорчук А.В. Полный одноразрядный сумматор по модулю // Патент России№ 2439661.2012. Бюл. № 1.
2. Кузьминов Ю.В. Алгоритм вычисления остатка по произвольному модулю от произведения двух чисел // Актуальные вопросы современной техники и технологии: тезисы докл. 2-й международной научной заочной конференции (Липецк, 2 окт. 2010 г.). – Липецк, 2010.– С. 147-149.
3. Петренко В.И. Принципы построения многоразрядных параллельных сумматоров по модулю с последовательным переносом // Университетская наука – региону: тезисы докл. 56-й научно-методической конференции (Ставрополь, 5–30 апр. 2011 г.). – Ставрополь, 2011.– С. 167-170.
4. Петренко В.И., Копытов В.В., Сидорчук А.В. Устройство для формирования остатка по произвольному модулю от числа // Патент России№ 2445730.2012. Бюл. № 8.
5. Тарабрин Б.В. Справочник по интегральным микросхемам / Б.В. Тарабрин, С.В. Якубовский, Н.А. Барканов и др.; под ред. Б.В. Тарабрина. – 2-е изд., перераб. и дополн. – М.: Энергия, 1981. – 816 с.

Рецензенты:

Тищенко Е.Н., д.э.н., профессор, заведующий кафедрой информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Ростовский государственный экономический университет (РИНХ)», г. Ростов-на-Дону.

Шуваев А.В., д.э.н., профессор, профессор кафедры прикладной информатики Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Ставропольский государственный аграрный университет», г. Ставрополь.