ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **BY** (11) **18674**

(13) **C1**

(46) **2014.10.30**

(51) МПК

G 06F 7/38 (2006.01)

(54) ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО ПО МОДУЛЮ ТРИ

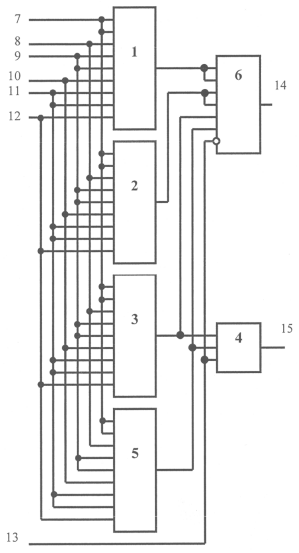
(21) Номер заявки: a 20111624
(22) 2011.11.30
(43) 2013.06.30

(71) Заявитель: Государственное научное учреждение "Объединенный институт проблем информатики Национальной академии наук Беларуси" (BY)
(72) Авторы: Седун Андрей Максимович; Городецкий Данила Андреевич (BY)
(73) Патентообладатель: Государственное научное учреждение "Объединенный институт проблем информатики Национальной академии наук Беларуси" (BY)

(56) BY a20100458, 2011.
BY 14479 C1, 2011.
BY 14614 C1, 2011.
BY 14629 C1, 2011.
RU 2090924 C1, 1997.

(57)

Вычислительное устройство по модулю три, содержащее элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, первый элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, первый и второй входы которых соединены со входом устройства "равно двум" первого операнда, первый вход устройства "равно единице" соединен с третьими входами элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, четвертый и пятый входы которых соединены со входом устройства "равно двум" второго операнда, второй вход "равно единице" устройства соединен с шестыми входами элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один,



BY 18674 C1 2014.10.30

первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, седьмой и восьмой входы которых соединены со входом устройства "равно двум" третьего операнда, третий вход устройства "равно единице" соединен с девятыми входами элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, **отличающееся** тем, что устройство дополнительно содержит второй элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два и мажоритарный элемент с порогом два, выход которого соединен с первым выходом устройства "равно единице", первый и второй входы соединены с выходом элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, третий и четвертый входы соединены с выходом элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре, выход первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два соединен с пятым входом мажоритарного элемента с порогом два и с первым входом второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, выход элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять соединен со вторым входом второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два и с шестым входом мажоритарного элемента с порогом два, вход устройства "равно единице" показателя степени соединен с инверсным входом мажоритарного элемента с порогом два и с третьим входом второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, выход которого соединен с выходом устройства "равно двум".

Изобретение относится к области вычислительной техники, автоматики и микроэлектроники и может быть использовано для построения систем передачи и переработки дискретной информации, построения систем аппаратного контроля, а также для построения вычислительных устройств, реализующих алгоритмы модулярной арифметики, работающих в системе остаточных классов.

Известно вычислительное устройство по модулю три, содержащее два мажоритарных элемента с порогом два, два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ и элемент И, пять входов и два выхода [1]. Недостатками известного устройства по модулю три являются низкие функциональные возможности, так как оно не выполняет операцию $(A + B + C)^D = S(\mathrm{mod}\ 3)$, и низкое быстродействие, определяемое глубиной схемы, равное 4τ, где τ - задержка на логический элемент.

Наиболее близким по конструкции и функциональным возможностям техническим решением к предлагаемому является вычислительное устройство по модулю три [2], содержащее элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, два элемента ИЛИ, шесть входов и два выхода. Недостатком известного вычислительного устройства по модулю три являются низкие функциональные возможности, так как он не выполняет операцию $(A + B + C)^D = S(\mathrm{mod}\ 3)$.

Задачей изобретения является расширение функциональных возможностей устройства за счет выполнения операции $(A + B + C)^D = S(\mathrm{mod}\ 3)$.

Задача решается следующим образом. Вычислительное устройство по модулю три, содержащее элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, первый элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, первый и второй входы которых соединены со входом устройства "равно двум" первого операнда, первый вход устройства "равно единице" соединен с третьими входами элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом

один, первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, четвертый и пятый входы которых соединены со входом устройства "равно двум" второго операнда, второй вход "равно единице" устройства соединен с шестыми входами элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, седьмой и восьмой входы которых соединены со входом устройства "равно двум" третьего операнда, третий вход устройства "равно единице" соединен с девятыми входами элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре и элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять, дополнительно введен второй элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два и мажоритарный элемент с порогом два, выход которого соединен с первым выходом устройства "равно единице", первый и второй входы соединены с выходом элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один, третий и четвертый входы соединены с выходом элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре, выход первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два соединен с пятым входом мажоритарного элемента с порогом два и с первым входом второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, выход элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять соединен со вторым входом второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два и с шестым входом мажоритарного элемента с порогом два, вход устройства "равно единице" показателя степени соединен с инверсным входом мажоритарного элемента с порогом два и с третьим входом второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два, выход которого соединен с выходом устройства "равно двум".

На фигуре представлена схема вычислительного устройства по модулю три.

Вычислительное устройство по модулю три содержит элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом один 1, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом четыре 2, первый и второй элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом два 3 и 4, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом пять 5, мажоритарный элемент с порогом два 6, семь входов 7,…, 13 и два выхода 14 и 15.

Операнды A, B, C, а также показатель степени D задаются двухразрядными двоичными векторами $A = (a_2, a_1)$, $B = (b_2, b_1)$, $C = (c_2, c_1)$ и $D = (d_2, d_1)$, где a_2, b_2, c_2 и d_2 - старшие разряды, a_1, b_1, c_1 и d_1 - младшие разряды, т.е. $A = 2a_2 + a_1$, $B = 2b_2 + b_1$, $C = 2c_2 + c_1$ и $D = 2d_2 + d_1$.

В соответствии с выбранным модулем P = 3 операнды и показатель степени могут принимать значения 0 (00), 1 (01), 2 (10). Результат выполнения операции $(A + B + C)^D = S(\mathrm{mod}\ 3)$ задается двухразрядным двоичным кодом $S = (s_2, s_1)$, где $S = 2s_2 + s_1$.

Вычислительное устройство по модулю три работает следующим образом. На входы устройства 7 и 8 поступают двоичные переменные a_2 и a_1, на входы 9 и 10 - переменные b_2 и b_1, на входы 11 и 12 - переменные c_2 и c_1, представляющие старшие и младшие разряды первого $A = (a_2, a_1)$, второго $B = (b_2, b_1)$ и третьего $C = (c_2, c_1)$ входных операндов соответственно. На вход 13 поступает переменная d_1, представляющая младший разряд показателя степени $D = (d_2, d_1)$. На выходах устройства 14 и 15 реализуются логические функции S_1 и S_2 - младший и старший разряды функции выхода $S = (s_2, s_1)$, представляющие результат выполнения операции $(A + B + C)^D = S(\mathrm{mod}\ 3)$.

ВХОДЫ								ВЫХОДЫ	
Первый операнд $A(a_2, a_1)$		Второй операнд $B(b_2, b_1)$		Третий операнд $C(c_2, c_1)$		Показатель степени $D(d_2, d_1)$		Функция выхода $S(s_2, s_1)$	
a_2	a_1	b_2	b_1	c_2	c_1	d_2	d_1	s_2	s_1
7	8	9	10	11	12	-	13	15	14
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	1
0	0	0	0	0	1	0	1	0	1
0	0	0	0	0	1	1	0	0	1
0	0	0	0	1	0	0	0	0	1
0	0	0	0	1	0	0	1	1	0
0	0	0	0	1	0	1	0	0	1
0	0	0	1	0	0	0	0	0	1
0	0	0	1	0	0	0	1	0	1
0	0	0	1	0	0	1	0	0	1
0	0	0	1	0	1	0	0	0	1
0	0	0	1	0	1	0	1	1	0
0	0	0	1	0	1	1	0	0	1
0	0	0	1	1	0	0	0	0	0
0	0	0	1	1	0	0	1	0	0
0	0	0	1	1	0	1	0	0	0
0	0	1	0	0	0	0	0	0	1
0	0	1	0	0	0	0	1	1	0
0	0	1	0	0	0	1	0	0	1
0	0	1	0	0	1	0	0	0	0
0	0	1	0	0	1	0	1	0	0
0	0	1	0	0	1	1	0	0	0
0	0	1	0	1	0	0	0	0	1
0	0	1	0	1	0	0	1	0	1
0	0	1	0	1	0	1	0	0	1
0	1	0	0	0	0	0	0	0	1
0	1	0	0	0	0	0	1	0	1
0	1	0	0	0	0	1	0	0	1
0	1	0	0	0	1	0	0	0	1
0	1	0	0	0	1	0	1	1	0
0	1	0	0	0	1	1	0	0	1
0	1	0	0	1	0	0	0	0	0
0	1	0	0	1	0	0	1	0	0
0	1	0	0	1	0	1	0	0	0
0	1	0	1	0	0	0	0	0	1
0	1	0	1	0	0	0	1	1	0
0	1	0	1	0	0	1	0	0	1
0	1	0	1	0	1	0	0	0	0
0	1	0	1	0	1	0	1	0	0
0	1	0	1	0	1	1	0	0	0

Продолжение таблицы

ВХОДЫ								ВЫХОДЫ	
Первый операнд $A(a_2, a_1)$		Второй операнд $B(b_2, b_1)$		Третий операнд $C(c_2, c_1)$		Показатель степени $D(d_2, d_1)$		Функция выхода $S(s_2, s_1)$	
a_2	a_1	b_2	b_1	c_2	c_1	d_2	d_1	s_2	s_1
7	8	9	10	11	12	-	13	15	14
0	1	0	1	1	0	0	0	0	1
0	1	0	1	1	0	0	1	0	1
0	1	0	1	1	0	1	0	0	1
0	1	1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	1	0	0
0	1	1	0	0	0	1	0	0	0
0	1	1	0	0	1	0	0	0	1
0	1	1	0	0	1	0	1	0	1
0	1	1	0	0	1	1	0	0	1
0	1	1	0	1	0	0	0	0	1
0	1	1	0	1	0	0	1	1	0
0	1	1	0	1	0	1	0	0	1
1	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0	1
1	0	0	0	0	0	1	0	0	1
1	0	0	0	0	1	0	0	0	0
1	0	0	0	0	1	0	1	0	0
1	0	0	0	0	1	1	0	0	0
1	0	0	0	1	0	0	0	0	1
1	0	0	0	1	0	0	1	0	1
1	0	0	0	1	0	1	0	0	1
1	0	0	1	0	0	0	0	0	0
1	0	0	1	0	0	0	1	0	0
1	0	0	1	0	0	1	0	0	0
1	0	0	1	0	1	0	0	0	1
1	0	0	1	0	1	0	1	0	1
1	0	0	1	0	1	1	0	0	1
1	0	0	1	1	0	0	0	0	1
1	0	0	1	1	0	0	1	1	0
1	0	0	1	1	0	1	0	0	1
1	0	1	0	0	0	0	0	0	1
1	0	1	0	0	0	0	1	0	1
1	0	1	0	0	0	1	0	0	1
1	0	1	0	0	1	0	0	0	1
1	0	1	0	0	1	0	1	1	0
1	0	1	0	0	1	1	0	0	1
1	0	1	0	1	0	0	0	0	0
1	0	1	0	1	0	0	1	0	0
1	0	1	0	1	0	1	0	0	0

Логическая схема вычислительного устройства по модулю три синтезирована по следующим аналитическим представлениям функций S_1 и S_2:

$$S_1 = \begin{cases} 1, \text{если } 2g_1 + g_2 + 2g_3 + g_4 + \overline{d_1} \geq 2; \\ 0 - \text{в противном случае,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{если } g_2 + g_4 + d_1 = 2; \\ 0 - \text{в противном случае,} \end{cases}$$

где

$$g_1 = \begin{cases} 1, \text{ если } 2a_2 + a_1 + 2b_2 + b_1 + 2c_2 + c_1 = 1; \\ 0 - \text{в противном случае,} \end{cases}$$

$$g_2 = \begin{cases} 1, \text{ если } 2a_2 + a_1 + 2b_2 + b_1 + 2c_2 + c_1 = 2; \\ 0 - \text{в противном случае,} \end{cases}$$

$$g_3 = \begin{cases} 1, \text{ если } 2a_2 + a_1 + 2b_2 + b_1 + 2c_2 + c_1 = 4; \\ 0 - \text{в противном случае,} \end{cases}$$

$$g_4 = \begin{cases} 1, \text{ если } 2a_2 + a_1 + 2b_2 + b_1 + 2c_2 + c_1 = 5; \\ 0 - \text{в противном случае .} \end{cases}$$

Фиг. 2 представляет таблицу истинности логических функций S_1 и S_2, описывающих работу вычислительного устройства по модулю три.

Отметим, что при реализации операции возведения в степень возникает неопределенность вида 0°. Так как в модулярной арифметике $0 = p \pmod p$, то $0 = p^p = 0 \pmod p$. Следовательно, здесь $0^0 = 0 \pmod 3$.

Достоинствами вычислительного устройства являются широкие функциональные возможности, так как оно выполняет операцию $(A + B + C)^D = S \pmod 3$, и высокое быстродействие, определяемое глубиной схемы, равное 2τ. Число внешних выводов схемы равно 9, а конструктивная сложность (по числу входов логических элементов) - 46.

Источники информации:

1. Патент РБ 12977, МПК G 06F 7/00, 2010.
2. Патент РБ 14479, МПК G 06F 7/38, 2011 (прототип).

Национальный центр интеллектуальной собственности.
220034, г. Минск, ул. Козлова, 20.