

ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ



НАЦИОНАЛЬНЫЙ ЦЕНТР
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

(19) ВУ (11) 13288

(13) С1

(46) 2010.06.30

(51) МПК (2009)

G 06F 7/00

(54)

ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО УНИТАРНЫХ КОДОВ ПО МОДУЛЮ ТРИ

(21) Номер заявки: а 20080926

(22) 2008.07.15

(43) 2009.02.28

(71) Заявитель: Белорусский государственный университет (ВУ)

(72) Авторы: Городецкий Данила Андреевич; Седун Андрей Максимович; Супрун Валерий Павлович (ВУ)

(73) Патентообладатель: Белорусский государственный университет (ВУ)

(56) ВУ 10218 С1, 2008.

ВУ 10350 С1, 2008.

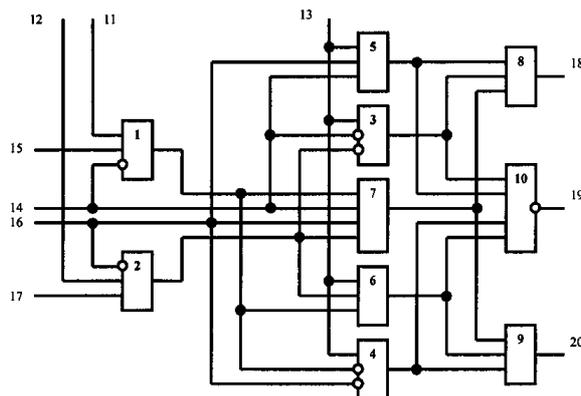
ВУ 9477 С1, 2007.

SU 1795452 А1, 1993.

SU 1798777 А1, 1993.

(57)

Вычислительное устройство унитарных кодов по модулю три, содержащее мажоритарный элемент с порогом два, три элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, два элемента ИЛИ и четыре элемента ЗАПРЕТ, вход запрета i -го элемента из которых, где $i = 1, 2$, соединен с i -м входом мажоритарного элемента с порогом два и с входом "равно нулю" i -го операнда, вход "равно двум" которого соединен с первым прямым входом i -го элемента ЗАПРЕТ, второй прямой вход которого соединен с i -м управляющим входом устройства, а выход - с $(i + 2)$ -м входом мажоритарного элемента с порогом два, при этом первые входы элементов ИЛИ соединены с третьим управляющим входом устройства и с прямыми входами третьего и четвертого элементов ЗАПРЕТ, первый вход запрета третьего элемента ЗАПРЕТ соединен с выходом первого элемента ЗАПРЕТ и со вторым входом первого элемента ИЛИ, третий вход которого соединен с выходом второго элемента ЗАПРЕТ и с первым входом запрета четвертого элемента ЗАПРЕТ, второй вход запрета которого соединен с входом "равно нулю" первого операнда и со вторым входом второго элемента ИЛИ, третий вход которого соединен со вторым входом запрета третьего элемента ЗАПРЕТ и со вторым входом мажоритарного элемента с порогом два, выход которого соединен с первыми входами первого и второго элементов СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, второй вход i -го элемента из которых соединен с выходом $(i + 2)$ -го элемента ЗАПРЕТ и с i -м входом третьего элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА с инверсным выходом, $(i + 2)$ -й



ВУ 13288 С1 2010.06.30

вход которого соединен с выходом i -го элемента ИЛИ и с третьим входом i -го элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, выход которого соединен с i -м выходом устройства, третий выход которого соединен с выходом элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА с инверсным выходом.

Изобретение относится к области вычислительной техники и микроэлектроники и может быть использовано для построения средств аппаратурного контроля и цифровых устройств, работающих в системе остаточных классов.

Известно вычислительное устройство, которое содержит два элемента ЗАПРЕТ, два элемента И, два элемента ИЛИ-НЕ, мажоритарный элемент с порогом два, три элемента РАВНОЗНАЧНОСТЬ, один управляющий вход, четыре информационных входа и три выхода [1]. Сложность устройства по числу входов логических элементов равна 24, а быстродействие, определяемое глубиной схемы, равно 3τ , где τ - усредненная задержка на один логический элемент.

Недостатком известного вычислительного устройства являются низкие функциональные возможности. Вычислительное устройство, как и изобретение, выполняет операции $A + B = S \pmod{3}$ и $A - B = R \pmod{3}$ в унитарных кодах по модулю три (в зависимости от значения управляющего сигнала), а также содержит два элемента ЗАПРЕТ и мажоритарный элемент с порогом два.

Наиболее близким по функциональным возможностям и конструкции техническим решением к предлагаемому является вычислительное устройство унитарных кодов по модулю три [2]. Сложность вычислительного устройства по числу входов логических элементов равна 20, а быстродействие - 3τ , где τ - задержка на логический элемент.

Устройство-прототип содержит два элемента ЗАПРЕТ, два элемента ИЛИ-НЕ, мажоритарный элемент с порогом два, три элемента РАВНОЗНАЧНОСТЬ, два управляющих входа, четыре информационных входа и три выхода. Входы "равно нулю" i -го операнда ($i = 1, 2$) соединены с i -м входом первого элемента ИЛИ-НЕ, с i -м входом мажоритарного элемента с порогом два и с входом запрета i -го элемента ЗАПРЕТ, первый прямой вход которого соединен с входом "равно двум" i -го операнда, второй вход - с i -м управляющим входом устройства, а выход - с $(2 + i)$ -м входом мажоритарного элемента с порогом два и с i -м входом второго элемента ИЛИ-НЕ, выход которого соединен первыми входами первого и второго элемента РАВНОЗНАЧНОСТЬ, второй вход первого элемента РАВНОЗНАЧНОСТЬ соединен с выходом первого элемента ИЛИ-НЕ и с первым входом третьего элемента РАВНОЗНАЧНОСТЬ, второй вход которого соединен с выходом мажоритарного элемента с порогом два и с вторым входом второго элемента РАВНОЗНАЧНОСТЬ, выход которого соединен с выходом устройства "равно нулю", выходы "равно единице" и "равно двум" которого соединены с выходами третьего и второго элементов РАВНОЗНАЧНОСТЬ соответственно.

Недостатком вычислительного устройства являются низкие функциональные возможности. Как и изобретение, устройство-прототип содержит два элемента ЗАПРЕТ и мажоритарный элемент с порогом два.

Изобретение направлено на решение технической задачи - расширение функциональных возможностей вычислительного устройства за счет выполнения операций в унитарных кодах $A^n + B^m = S \pmod{3}$ и $A^n - B^m = R \pmod{3}$, где n, m - произвольные натуральные числа.

Вычислительное устройство унитарных кодов по модулю три содержит мажоритарный элемент с порогом два, три элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, два элемента ИЛИ и четыре элемента ЗАПРЕТ, вход запрета i -го элемента из которых, где $i = 1, 2$, соединен с i -м входом мажоритарного элемента с порогом два и с входом "равно нулю" i -го операнда.

Вход "равно двум" i -го операнда соединен с первым прямым входом i -го элемента ЗАПРЕТ, второй прямой вход которого соединен с i -м управляющим входом устройства, а выход - с $(i + 2)$ -м входом мажоритарного элемента с порогом два.

При этом первые входы элементов ИЛИ соединены с третьим управляющим входом устройства и с прямыми входами третьего и четвертого элементов ЗАПРЕТ, первый вход

запрета третьего элемента ЗАПРЕТ соединен с выходом первого элемента ЗАПРЕТ и со вторым входом первого элемента ИЛИ.

Третий вход первого элемента ИЛИ соединен с выходом второго элемента ЗАПРЕТ и с первым входом запрета четвертого элемента ЗАПРЕТ, второй вход запрета которого соединен с входом "равно нулю" первого операнда и со вторым входом второго элемента ИЛИ.

Третий вход второго элемента ИЛИ соединен со вторым входом запрета третьего элемента ЗАПРЕТ и со вторым входом мажоритарного элемента с порогом два, выход которого соединен с первыми входами первого и второго элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА.

Второй вход i -го элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА соединен с выходом $(i + 2)$ -го элемента ЗАПРЕТ и с i -м входом третьего элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА с инверсным выходом, $(i + 2)$ -й вход которого соединен с выходом i -го элемента ИЛИ и с третьим входом i -го элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА.

Выход i -го элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА соединен с i -м выходом устройства, третий выход которого соединен с выходом элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА с инверсным выходом.

На чертеже (фигура) представлена схема вычислительного устройства унитарных кодов по модулю три.

Вычислительное устройство содержит четыре элемента ЗАПРЕТ 1...4, два элемента ИЛИ 5 и 6, мажоритарный элемент с порогом два 7, два элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА 8 и 9, элемент СЛОЖЕНИЕ ПО МОДУЛЮ ДВА с инверсным выходом 10, три управляющих входа 11, 12 и 13, четыре информационных входа 14...17 и три выхода 18, 19 и 20.

Вычислительное устройство унитарных кодов по модулю три работает следующим образом. На информационные входы 14 и 15 устройства поступают разряды "равно нулю" и "равно двум" первого операнда $A = (a_0, a_1, a_2)$, на входы 16 и 17 - разряды "равно нулю" и "равно двум" второго операнда $B = (b_0, b_1, b_2)$, где $a_0, a_1, a_2, b_0, b_1, b_2 \in \{0, 1\}$. При этом $a_k = 1$ ($b_k = 1$) тогда и только тогда, когда $A = k \pmod{3}$ ($B = k \pmod{3}$), где $k = 0, 1, 2$.

На управляющие входы 11, 12 и 13 подаются значения логических переменных u_1, u_2 и u_3 соответственно, где

$$u_1 = \begin{cases} 0, & \text{если } n - \text{четное;} \\ 1 - & \text{в противном случае} \end{cases} \quad \text{и} \quad u_2 = \begin{cases} 0, & \text{если } m - \text{четное;} \\ 1 - & \text{в противном случае.} \end{cases}$$

Если $u_3 = 0$, то на выходах вычислительного устройства 20, 18 и 19 формируется унитарный двоичный код $S = (s_0, s_1, s_2)$ результата выполнения операции $A^n + B^m = S \pmod{3}$; если $u_3 = 1$, то на выходах вычислительного устройства 19, 20 и 18 формируется унитарный двоичный код $R = (r_0, r_1, r_2)$ результата выполнения операции $A^n - B^m = R \pmod{3}$, где $s_0, s_1, s_2, r_0, r_1, r_2 \in \{0, 1\}$. Причем $s_k = 1$ и $r_k = 1$ тогда и только тогда, когда $A^n + B^m = k \pmod{3}$ и $A^n - B^m = k \pmod{3}$ соответственно, где $k = 0, 1, 2$.

Первообразная функция вычислительного устройства унитарных кодов по модулю три имеет вид

$$\begin{aligned} F_1(u_1, u_2, u_3) &= (u_3 \vee a_0 \vee b_0) \oplus u_3 \cdot \overline{a_0} \cdot \overline{g} \oplus M_4^2(a_0, b_0, f, g), \\ F_2(u_1, u_2, u_3) &= \overline{(u_3 \vee a_0 \vee b_0) \oplus u_3 \cdot \overline{a_0} \cdot \overline{g} \oplus (u_3 \vee g \vee f) \oplus u_3 \cdot \overline{b_0} \cdot \overline{f}}, \\ F_3(u_1, u_2, u_3) &= (u_3 \vee g \vee f) \oplus u_3 \cdot \overline{b_0} \cdot \overline{f} \oplus M_4^2(a_0, b_0, f, g), \end{aligned}$$

где $f(u_1, a_0, a_2) = u_1 \cdot \overline{a_0} \cdot a_2$, $g(u_2, b_0, b_2) = u_2 \cdot \overline{b_0} \cdot b_2$, $M_4^2(a_0, b_0, f, g)$ - функция, реализуемая на выходе 4-входового мажоритарного элемента с порогом два, т.е.

$$M_4^2(a_0, b_0, f, g) = \begin{cases} 1, & \text{если } a_0 + b_0 + f + g \geq 2; \\ 0 - & \text{в противном случае.} \end{cases}$$

Отметим, что здесь

$$F_1(u_1, u_2, u_3) = \begin{cases} s_1, & \text{если } u_3 = 0; \\ r_2 - & \text{в противном случае,} \end{cases}$$

BY 13288 C1 2010.06.30

$$F_2(u_1, u_2, u_3) = \begin{cases} s_2, & \text{если } u_3 = 0; \\ r_0 - & \text{в противном случае,} \end{cases}$$

$$F_3(u_1, u_2, u_3) = \begin{cases} s_0, & \text{если } u_3 = 0; \\ r_1 - & \text{в противном случае.} \end{cases}$$

Работа вычислительного устройства унитарных кодов по модулю три описывается таблицей истинности логических функций s_0, s_1, s_2, r_0, r_1 и r_2 (таблица).

Входы									Выходы		
Управляющие входы			Унитарный двоичный код первого операнда $A = (a_0, a_1, a_2)$			Унитарный двоичный код второго операнда $B = (b_0, b_1, b_2)$			Унитарный двоичный код результата суммы $S = (s_0, s_1, s_2)$		
u_1	u_2	u_3	a_0	a_1	a_2	b_0	b_1	b_2	s_0	s_1	s_2
11	12	13	14	-	15	16	-	17	20	18	19
0	0	0	1	0	0	1	0	0	1	0	0
0	0	0	1	0	0	0	1	0	0	1	0
0	0	0	1	0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0	0	0	1	0
0	0	0	0	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	1	0
0	0	0	0	0	1	1	0	0	0	1	0
0	0	0	0	0	1	0	1	0	0	0	1
0	0	0	0	0	1	0	0	1	0	0	1
1	0	0	1	0	0	1	0	0	1	0	0
1	0	0	1	0	0	0	1	0	0	1	0
1	0	0	1	0	0	0	0	1	0	1	0
1	0	0	0	1	0	1	0	0	0	1	0
1	0	0	0	1	0	0	1	0	0	0	1
1	0	0	0	1	0	0	0	1	0	1	0
1	0	0	0	0	1	1	0	0	0	0	1
1	0	0	0	0	1	0	1	0	1	0	0
1	0	0	0	0	1	0	0	1	1	0	0
0	1	0	1	0	0	1	0	0	1	0	0
0	1	0	1	0	0	0	1	0	0	1	0
0	1	0	1	0	0	0	0	1	0	0	1
0	1	0	0	1	0	1	0	0	0	1	0
0	1	0	0	1	0	0	1	0	0	0	1
0	1	0	0	1	0	0	0	1	1	0	0
0	1	0	0	0	1	1	0	0	0	1	0
0	1	0	0	0	1	0	1	0	0	0	1
0	1	0	0	0	1	0	0	1	1	0	0
1	1	0	1	0	0	1	0	0	1	0	0
1	1	0	1	0	0	0	1	0	0	1	0
1	1	0	1	0	0	0	0	1	0	0	1
1	1	0	0	1	0	1	0	0	0	1	0
1	1	0	0	1	0	0	1	0	0	0	1
1	1	0	0	1	0	0	0	1	1	0	0
1	1	0	0	0	1	1	0	0	0	0	1
1	1	0	0	0	1	0	1	0	1	0	0
1	1	0	0	0	1	0	0	1	0	1	0

BY 13288 C1 2010.06.30

Управляющие входы			Унитарный двоичный код первого операнда $A = (a_0, a_1, a_2)$			Унитарный двоичный код второго операнда $B = (b_0, b_1, b_2)$			Унитарный двоичный код результата разности $R = (r_0, r_1, r_2)$		
			a_0	a_1	a_2	b_0	b_1	b_2	r_0	r_1	r_2
u_1	u_2	u_3	14	-	15	16	-	17	19	20	18
11	12	13									
0	0	1	1	0	0	1	0	0	1	0	0
0	0	1	1	0	0	0	1	0	0	0	1
0	0	1	1	0	0	0	0	1	0	0	1
0	0	1	0	1	0	1	0	0	0	1	0
0	0	1	0	1	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0	1	1	0	0
0	0	1	0	0	1	1	0	0	0	1	0
0	0	1	0	0	1	0	1	0	1	0	0
0	0	1	0	0	1	0	0	1	1	0	0
1	0	1	1	0	0	1	0	0	1	0	0
1	0	1	1	0	0	0	1	0	0	0	1
1	0	1	1	0	0	0	0	1	0	0	1
1	0	1	0	1	0	1	0	0	0	1	0
1	0	1	0	1	0	0	1	0	1	0	0
1	0	1	0	1	0	0	0	1	1	0	0
1	0	1	0	0	1	1	0	0	0	0	1
1	0	1	0	0	1	0	1	0	0	1	0
1	0	1	0	0	1	0	0	1	0	1	0
0	1	1	1	0	0	1	0	0	1	0	0
0	1	1	1	0	0	0	1	0	0	0	1
0	1	1	1	0	0	0	0	1	0	1	0
0	1	1	0	1	0	1	0	0	0	1	0
0	1	1	0	1	0	0	1	0	1	0	0
0	1	1	0	1	0	0	0	1	0	0	1
0	1	1	0	0	1	1	0	0	0	1	0
0	1	1	0	0	1	0	1	0	1	0	0
0	1	1	0	0	1	0	0	1	0	0	1
1	1	1	1	0	0	1	0	0	1	0	0
1	1	1	1	0	0	0	1	0	0	0	1
1	1	1	1	0	0	0	0	1	0	1	0
1	1	1	0	1	0	1	0	0	0	1	0
1	1	1	0	1	0	0	1	0	1	0	0
1	1	1	0	1	0	0	0	1	0	0	1
1	1	1	0	0	1	1	0	0	0	0	1
1	1	1	0	0	1	0	1	0	0	1	0
1	1	1	0	0	1	0	0	1	1	0	0

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

Основным достоинством вычислительного устройства унитарных кодов по модулю три являются широкие функциональные возможности, поскольку устройство реализует операции $A^n + B^m = S \pmod{3}$ и $A^n - B^m = R \pmod{3}$.

