ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

(19) **BY** (11) **3299**

(13) **C1**

(51)[6] **G 06F 7/49**

ГОСУДАРСТВЕННЫЙ ПАТЕНТНЫЙ КОМИТЕТ РЕСПУБЛИКИ БЕЛАРУСЬ

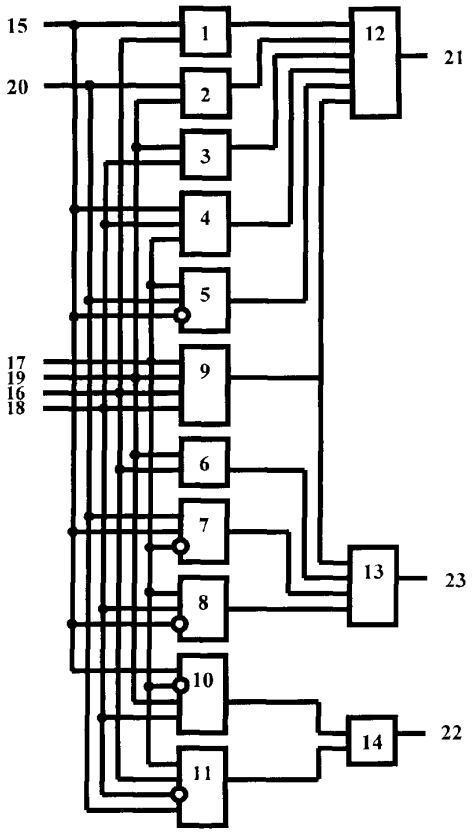
(54) УСТРОЙСТВО ДЛЯ УМНОЖЕНИЯ ПО МОДУЛЮ ПЯТЬ

(21) Номер заявки: 970287
(22) 1997.06.02
(46) 2000.03.30

(71) Заявитель: Белорусский государственный университет (BY)
(72) Авторы: Супрун В.П., Седун А.М. (BY)
(73) Патентообладатель: Белорусский государственный университет (BY)

(57)

Устройство для умножения по модулю пять, содержащее мажоритарный элемент с порогом три, два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ и восемь элементов И, первые входы первого, четвертого, седьмого из которых, а также инверсные входы пятого и восьмого элементов И, соединены со входом первого разряда первого сомножителя устройства, вход второго разряда первого сомножителя которого соединен с первыми входами пятого и восьмого элементов И, с первым входом первого мажоритарного элемента с порогом три, со вторым входом четвертого элемента И, с инверсным входом седьмого элемента И, вход третьего разряда первого сомножителя устройства соединен с первыми входами второго, третьего и шестого элементов И, со



Фиг. 1

вторым входом первого мажоритарного элемента с порогом три, вход первого разряда второго сомножителя устройства соединен со вторыми входами первого и шестого элементов И, с третьим входом первого мажоритарного элемента с порогом три, вход второго разряда второго сомножителя устройства соединен со вторыми входами третьего и восьмого элементов И, с третьим входом четвертого элемента И и с четвертым входом первого мажоритарного элемента с порогом три, а вход третьего разряда второго сомножителя устройства соединен со вторыми входами второго, пятого и седьмого элементов И, входы с первого по шестой первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ соединены соответственно с выходами первого, второго, третьего, четвертого и пятого элементов И и с выходом первого мажоритарного элемента с порогом три, входы с первого по четвертый второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ соединены соответственно с выходами шестого, седьмого и восьмого элементов И и с выходом первого мажоритарного элемента с порогом три, выходы первого и второго элементов ИСКЛЮЧАЮЩЕЕ ИЛИ соединены соответственно с выходами первого и третьего разрядов произведения устройства, **отличающееся** тем, что содержит элемент ИЛИ, второй и третий мажоритарные элементы с порогом три, первый вход второго мажоритарного элемента с порогом три соединен со входом первого разряда первого сомножителя устройства, вход второго разряда первого сомножителя которого соединен с первым входом третьего и инверсным входом второго мажоритарных элементов с порогом три, вход третьего разряда первого сомножителя устройства соединен со вторым входом второго мажоритарного элемента с порогом три, вход первого разряда второго сомножителя устройства соединен со вторым входом третьего мажоритарного элемента с порогом три, вход второго разряда второго сомножителя устройства соединен с третьим входом второго и с инверсным входом третьего мажоритарных элементов с порогом три, а вход третьего разряда второго сомножителя устройства соединен с третьим входом третьего мажоритарного элемента с порогом три, выход которого соединен с первым входом элемента ИЛИ, второй вход которого соединен с выходом второго мажоритарного элемента с порогом три, а выход — с выходом второго разряда произведения устройства.

(56)
1. А.с. СССР 1644131, МПК G 06F 7/49, 1991.
2. Патент РБ 1300, МПК G 06F 7/49, 1996 (прототип).

Изобретение относится к области вычислительной техники и автоматики и может быть использовано для построения систем передачи и переработки дискретной информации.

Известно устройство для умножения по модулю пять, содержащее тринадцать элементов И, восемь элементов ИЛИ, три элемента ЗАПРЕТА, шесть входов и три выхода [1].

Недостатком устройства для умножения по модулю пять является низкое быстродействие, определяемое глубиной схемы.

Наиболее близким по конструкции и функциональным возможностям техническим решением к предлагаемому является устройство для умножения по модулю пять [2], содержащее семь элементов И, четыре элемента ЗАПРЕТА, мажоритарный элемент с порогом три, три элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, шесть входов и три выхода.

Недостатком устройства для умножения по модулю пять является высокая конструктивная сложность по числу входов логических элементов.

Изобретение направлено на решение технической задачи понижения конструктивной сложности устройства для умножения по модулю пять.

Устройство для умножения по модулю пять содержит мажоритарный элемент с порогом три, два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ и восемь элементов И, первые входы первого, четвертого, седьмого из которых, а также инверсные входы пятого и восьмого элементов И, соединены со входом первого разряда первого сомножителя устройства. Вход второго разряда первого сомножителя устройства соединен с первыми входами пятого и восьмого элементов И, с первым входом первого мажоритарного элемента с порогом три, со вторым входом четвертого элемента И, с инверсным входом седьмого элемента И. Вход третьего разряда первого сомножителя устройства соединен с первыми входами второго, третьего и шестого элементов И, со вторым входом первого мажоритарного элемента с порогом три. Вход первого разряда второго сомножителя устройства соединен со вторыми входами первого и шестого элементов И, с третьим входом первого мажоритарного элемента с порогом три. Вход второго разряда второго сомножителя устройства соединен со вторыми входами третьего и восьмого элементов И, и с третьим входом четвертого элемента И и с четвертым входом первого мажоритарного элемента с порогом три. Вход третьего разряда второго сомножителя устройства соединен со вторыми входами второго, пятого и седьмого элементов И, входы с первого по шестой первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ соединены соответственно с выходами первого, второго, третьего, четвертого и пятого элементов И и с выходом первого мажоритарного элемента с порогом три. Входы с

первого по четвертый второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ соединены соответственно с выходами шестого, седьмого и восьмого элементов И и с выходом первого мажоритарного элемента с порогом три. Выходы первого и второго элементов ИСКЛЮЧАЮЩЕЕ ИЛИ соединены соответственно с выходами первого и третьего разрядов произведения устройства. В отличие от прототипа, устройство содержит элемент ИЛИ, второй и третий мажоритарные элементы с порогом три. Первый вход второго мажоритарного элемента с порогом три соединен со входом первого разряда первого сомножителя устройства. Вход второго разряда первого сомножителя устройства соединен с первым входом третьего и инверсным входом второго мажоритарных элементов с порогом три. Вход третьего разряда первого сомножителя устройства соединен со вторым входом второго мажоритарного элемента с порогом три. Вход первого разряда второго сомножителя устройства соединен со вторым входом третьего мажоритарного элемента с порогом три. Вход второго разряда второго сомножителя устройства соединен с третьим входом второго и инверсным входом третьего мажоритарных элементов с порогом три. Вход третьего разряда второго сомножителя устройства соединен с третьим входом третьего мажоритарного элемента с порогом три, выход которого соединен с первым входом элемента ИЛИ, второй вход которого соединен с выходом второго мажоритарного элемента с порогом три, а выход - с выходом второго разряда произведения устройства.

Названный технический результат достигается путем использования нового логического элемента (элемента ИЛИ), а также изменением межсоединений в логической схеме устройства.

На чертеже (фиг. 1) представлена схема устройства для умножения по модулю пять.

Устройство для умножения по модулю пять содержит восемь элементов И 1, 2,...,8, три мажоритарных элемента с порогом три 9, 10 и 11, два элемента ИСКЛЮЧАЮЩЕЕ ИЛИ 12, 13, элемент ИЛИ 14, шесть входов 15, 16,...,20 и три выхода 21, 22 и 23.

Умножаемые операнды X и Y задаются трехразрядными двоичными кодами $X = x_3x_2x_1$, $Y = y_3y_2y_1$, где x_1,y_1 - первые (младшие) разряды операндов; x_2,y_2 - вторые (средние) разряды операндов; x_3,y_3 - третьи (старшие) разряды операндов, т.е. $X = x_1 + 2x_2 + 4x_3$ и $Y = y_1 + 2y_2 + 4y_3$.

В соответствием с выбранным модулем P = 5 каждый операнд может принимать значения 0 (000), 1(001), 2 (010), 3 (011) и 4 (100). Результатом работы устройства для умножения по модулю пять является операнд Z, заданный трехразрядным двоичным кодом $Z = z_3z_2z_1$, где $Z = z_1 + 2z_2 + 4z_3$.

На входы 15,16 подаются значения младших разрядов x_1,y_1 операндов X и Y соответственно; на входы 17,18 - значения средних разрядов x_2,y_2 операндов X и Y соответственно; на входы 19,20 - значения старших разрядов x_3,y_3 операндов X и Y соответственно; на выходе 21 реализуется младший разряд z_1, на выходе 22 - средний разряд z_2, а на выходе 23 - старший разряд операнда Z, где $Z = X * Y \pmod 5$.

Логические функции z_1, z_2, z_3, значения которых представлены в таблице (фиг. 2), реализуются устройством согласно следующим аналитическим представлениям:

$$z_1 = F_6^1\left(x_1y_1, x_3y_3, x_3y_2, x_1x_2y_2, \overline{x_1}x_2y_3, M_4^3\left(x_2, x_3, y_1, y_2\right)\right);$$

$$z_2 = F_4^3\left(x_1, \overline{x_2}, x_3, y_2\right) \vee M_4^3\left(x_2, y_1, \overline{y_2}, y_3\right);$$

$$z_3 = F_4^1\left(x_1\overline{x_2}y_3, \overline{x_1}, x_2y_2, x_3y_1, M_4^3\left(x_2, x_3, y_1, y_2\right)\right),$$

где $M_4^3(t_1, t_2, t_3, t_4) = \begin{cases} 1, \text{ если } t_1 + t_2 + t_3 + t_4 \geq 3; \\ 0 - \text{в протитвном случае,} \end{cases}$

при $t_1, t_2, t_3, t_4 \in \{0,1\}$,

$$F_n^1(t_1, t_2, \ldots, t_n) = \begin{cases} 1, \text{ если } t_1 + t_2 + \cdots + t_n = 1; \\ 0 - \text{в противном случае,} \end{cases}$$

и $t_1, t_2, \ldots, t_n \in \{0,1\}$, $n \in \{4,6\}$.

Достоинством предлагаемого устройства для умножения по модулю пять является относительно невысокая конструктивная сложность. Так, его сложность по числу входов логических элементов равна 44 (сложность устройства - прототипа равна 46). Также отметим, что быстродействие предлагаемого устройства совпадает с быстродействием устройства-прототипа и равно 2τ, где τ - задержка на вентиль.

Входы						Выход		
X			Y			Z		
x_3	x_2	x_1	y_3	y_2	y_1	z_3	z_2	z_1
19	17	15	20	18	16	23	22	21
0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	1	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	1	0	1	1	0	0	1
0	0	1	0	1	0	0	1	0
0	0	1	0	0	1	0	1	1
0	0	1	1	0	0	1	0	0
0	1	0	0	1	0	0	0	0
0	1	0	0	1	1	0	1	0
0	1	0	0	0	0	1	0	0
0	1	0	0	0	1	0	0	1
0	1	0	1	1	0	0	1	1
0	1	1	0	1	0	0	0	0
0	1	1	0	0	1	0	1	1
0	1	1	0	0	0	0	0	1
0	1	1	0	1	1	1	0	0
0	1	1	1	1	0	0	1	0
1	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	0	0
1	0	0	0	1	0	0	1	1
1	0	0	0	1	1	0	1	0
1	0	0	1	0	0	0	0	1

Фиг. 2

Государственный патентный комитет Республики Беларусь.
220072, г. Минск, проспект Ф. Скорины, 66.