

(19)



**Евразийское
патентное
ведомство**

(11) **033823**(13) **B1**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2019.11.29

(51) Int. Cl. **G06F 7/52 (2006.01)**

(21) Номер заявки
201800204

(22) Дата подачи заявки
2018.02.06

(54) УСТРОЙСТВО ДЛЯ УМНОЖЕНИЯ ПО МОДУЛЮ ВОСЕМЬ

(43) **2019.08.30**

(56) RU-C1-2589361
RU-C1-2143722
RU-C1-2181904
US-A1-20100235414
US-B1-6272513

(96) **2018/EA/0008 (BY) 2018.02.06**

(71)(73) Заявитель и патентовладелец:
**БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ (БГУ) (BY)**

(72) Изобретатель:
**Супрун Валерий Павлович,
Городецкий Данила Андреевич (BY)**

(57) Изобретение относится к области вычислительной техники и микроэлектроники и может быть использовано для построения средств аппаратного контроля и цифровых устройств, работающих в системе остаточных классов. Вычислительное устройство предназначено для реализации операции умножения $A \cdot B = R \pmod{8}$. Устройство содержит семь элементов И, два элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, шесть входов и три выхода. Сложность устройства (по числу входов логических элементов) равна 22, а быстродействие, определяемое глубиной схемы, составляет 2τ , где τ - задержка на один логический элемент. Устройство для умножения по модулю восемь работает следующим образом. На входы устройства поступают значения двоичных переменных $a_1, b_1, a_2, b_2, a_3, b_3$, принимающие значения младших, средних и старших разрядов операндов A и B , где $A = a_1 + 2a_2 + 4a_3$ и $B = b_1 + 2b_2 + 4b_3$. На выходах устройства реализуются логические функции R_1, R_2, R_3 , принимающие значения младшего r_1 , среднего r_2 и старшего r_3 разрядов результата выполнения операции $A \cdot B = R \pmod{8}$, где $R = r_1 + 2r_2 + 4r_3$.

B1**033823****033823****B1**

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

Известно устройство для умножения по модулю семь, которое содержит девять элементов РАВНОЗНАЧНОСТЬ, три элемента ИЛИ, шесть входов и три выхода [1]. Сложность устройства (по числу входов логических элементов) равна 45.

Недостатком известного устройства являются низкие функциональные возможности, поскольку устройство не позволяет вычислять операцию умножения по модулю восемь.

Наиболее близким по функциональным возможностям и конструкции техническим решением к предлагаемому устройству является устройство для умножения по модулю семь, содержащее пять элементов И, восемь элементов СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, шесть входов и три выхода [2].

Устройство-прототип предназначено для реализации арифметической операции $A \cdot B = R \pmod{7}$. Сложность устройства равна 32, а его быстродействие, определяемое глубиной схемы, составляет 3τ , где τ - усредненная задержка на один логический элемент.

Устройство-прототип, как и заявляемое устройство, содержит пять элементов И и два элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, выходы которых соединены с выходами среднего и старшего разрядов результата умножения операндов.

Недостатком устройства-прототипа являются низкие функциональные возможности, поскольку устройство не позволяет вычислять операцию $A \cdot B = R \pmod{8}$.

Изобретение направлено на решение следующей технической задачи: расширение функциональных возможностей устройства для умножения по модулю семь.

Устройство для умножения по модулю восемь содержит первый и второй элементы СЛОЖЕНИЕ ПО МОДУЛЮ ДВА и с первого по седьмой элементы И, выход первого из которых соединен с выходом первого разряда результата умножения операндов.

Выход второго разряда умножения операндов соединен с выходом первого элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, i -й вход которого, где $i = 1, 2$, соединен с выходом $(i+1)$ -го элемента И.

Выход третьего разряда умножения операндов соединен с выходом второго элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, j -й вход которого, где $j = 1, 2, 3, 4$, соединен с выходом $(j+3)$ -го элемента И.

Вход первого разряда первого операнда соединен с первыми входами первого, третьего, пятого и седьмого элементов И.

Вход второго разряда первого операнда соединен с первыми входами второго, четвертого элементов И и со вторым входом пятого элемента И.

Вход третьего разряда первого операнда соединен с первым входом шестого элемента И.

Вход первого разряда второго операнда соединен со вторыми входами первого, второго, шестого элементов И и с третьим входом шестого элемента И.

Вход второго разряда второго операнда соединен со вторыми входами третьего, четвертого элементов И и с четвертым входом пятого элемента И.

Вход третьего разряда второго операнда соединен со вторым входом седьмого элемента И.

Основной технический результат изобретения заключается в повышении функциональных возможностей устройства для умножения по модулю семь. Названный эффект достигается путем использования новых логических элементов (элементов И и элементов СЛОЖЕНИЕ ПО МОДУЛЮ ДВА), а также изменением соединений между элементами логической схемы устройства-прототипа.

Заявляемое устройство ориентировано на реализацию (выполнение) операции умножения $A \cdot B = R \pmod{8}$. При этом входные операнды A и B , а также выходной операнд R задаются трехразрядными двоичными кодами $A = (a_1, a_2, a_3)$, $B = (b_1, b_2, b_3)$ и $R = (r_1, r_2, r_3)$, где

$$A = a_1 + 2a_2 + 4a_3, B = b_1 + 2b_2 + 4b_3 \text{ и } R = r_1 + 2r_2 + 4r_3.$$

На чертеже представлена логическая схема устройства для умножения по модулю восемь. Устройство содержит семь элементов И 1-7, два элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА 8 и 9, шесть входов 10-15, три выхода 16, 17 и 18.

Устройство для умножения по модулю восемь работает следующим образом.

На входы 10, 11 и 12 устройства поступают значения первого (младшего) a_1 , второго (среднего) a_2 и третьего (старшего) a_3 разрядов первого операнда A соответственно; на входы 13, 14 и 15 устройства - значения первого b_1 , второго b_2 и третьего b_3 разрядов второго операнда B соответственно.

На выходах 16, 17 и 18 устройства реализуются значения первого r_1 , второго r_2 и третьего r_3 разрядов выходного операнда R соответственно.

Двоичные функции R_1 , R_2 , R_3 , реализуемые на выходах заявляемого устройства для умножения по модулю восемь, представлены посредством таблицы истинности.

ВХОДЫ						ВЫХОДЫ		
a_3	a_2	a_1	b_3	b_2	b_1	R_3	R_2	R_1
12	11	10	15	14	13	18	17	16
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	0	1	0	1	0	0	0
0	0	0	1	1	0	0	0	0
0	0	0	1	1	1	0	0	0
0	0	1	0	0	0	0	0	0
0	0	1	0	0	1	0	0	1
0	0	1	0	1	0	0	1	0
0	0	1	0	1	1	0	1	1
0	0	1	1	0	0	1	0	0
0	0	1	1	0	1	1	0	1
0	0	1	1	1	0	1	1	0
0	0	1	1	1	1	1	1	1
0	1	0	0	0	0	0	0	0
0	1	0	0	0	1	0	1	0
0	1	0	0	1	0	1	0	0
0	1	0	0	1	1	1	1	0
0	1	0	1	0	0	0	0	0
0	1	0	1	0	1	0	1	0
0	1	0	1	1	0	1	0	0
0	1	0	1	1	1	1	1	0
0	1	1	0	0	0	0	0	0
0	1	1	0	0	1	0	1	1
0	1	1	0	1	0	1	1	0
0	1	1	0	1	1	0	0	1
0	1	1	1	0	0	1	0	0
0	1	1	1	0	1	1	1	1
0	1	1	1	1	0	0	1	0
0	1	1	1	1	1	1	0	1
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	0	0
1	0	0	0	1	1	1	0	0
1	0	0	1	0	0	0	0	0
1	0	0	1	0	1	1	0	0
1	0	0	1	1	0	0	0	0
1	0	0	1	1	1	1	0	0
1	0	1	0	0	0	0	0	0
1	0	1	0	0	1	1	0	1
1	0	1	0	1	0	0	1	0
1	0	1	0	1	1	1	1	1
1	0	1	1	0	0	0	1	0
1	0	1	1	0	1	1	0	0
1	0	1	1	1	0	1	1	0
1	0	1	1	1	1	0	1	1
1	1	0	0	0	0	0	0	0
1	1	0	0	0	1	1	1	0
1	1	0	0	1	0	1	0	0
1	1	0	0	1	1	0	1	0
1	1	0	1	0	0	0	0	0
1	1	0	1	0	1	1	1	0
1	1	0	1	1	0	1	0	0
1	1	0	1	1	1	0	1	0
1	1	1	0	0	0	0	0	0
1	1	1	0	0	1	1	1	1
1	1	1	0	1	0	1	1	0
1	1	1	0	1	1	1	0	1
1	1	1	1	0	0	1	0	0
1	1	1	1	0	1	0	1	1
1	1	1	1	1	0	0	1	0
1	1	1	1	1	1	0	0	1

Логическая схема заявляемого устройства (см. чертеж) синтезирована на основе применения следующих аналитических представлений двоичных функций R_1 , R_2 , R_3 :

$$R_1 = a_1 b_1, \quad R_2 = a_1 b_2 \oplus a_2 b_1,$$

$$R_3 = a_2 b_2 \oplus a_1 a_2 b_1 b_2 \oplus a_1 b_3 \oplus a_3 b_1.$$

Основным достоинством устройства для умножения по модулю восемь являются широкие функциональные возможности. Кроме того, устройство имеет простую логическую схему, сложность которой равна 22.

Источники информации, принятые во внимание при экспертизе.

1. Патент РБ 7881, МПК G06F 7/49, 7/52, БИ № 1 (48), 2006, с. 137.
2. Патент РБ 5354, МПК G06F 7/49, БИ № 3 (38), 2003, с. 215 (прототип).

ФОРМУЛА ИЗОБРЕТЕНИЯ

Устройство для умножения по модулю восемь, содержащее первый и второй элементы СЛОЖЕНИЕ ПО МОДУЛЮ ДВА и с первого по седьмой элементы И, выход первого из которых соединен с выходом первого разряда результата умножения операндов, выход второго разряда умножения операндов соединен с выходом первого элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, i -й вход которого, где $i = 1, 2$, соединен с выходом $(i+1)$ -го элемента И, выход третьего разряда умножения операндов соединен с выходом второго элемента СЛОЖЕНИЕ ПО МОДУЛЮ ДВА, j -й вход которого, где $j = 1, 2, 3, 4$, соединен с выходом $(j+3)$ -го элемента И, вход первого разряда первого операнда соединен с первыми входами первого, третьего, пятого и седьмого элементов И, вход второго разряда первого операнда соединен с первыми входами второго, четвертого элементов И и со вторым входом пятого элемента И, вход третьего разряда первого операнда соединен с первым входом шестого элемента И, вход первого разряда второго операнда соединен со вторыми входами первого, второго, шестого элементов И и с третьим входом шестого элемента И, вход второго разряда второго операнда соединен со вторыми входами третьего, четвертого элементов И и с четвертым входом пятого элемента И, вход третьего разряда второго операнда соединен со вторым входом седьмого элемента И.

