ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 68872** **(13) U**

(51) МПК (2012.01)
G06F 7/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2011 12596**

(22) Дата подання заявки: **27.10.2011**

(24) Дата, з якої є чинними права на корисну модель: **10.04.2012**

(46) Публікація відомостей про видачу патенту: **10.04.2012, Бюл.№ 7**

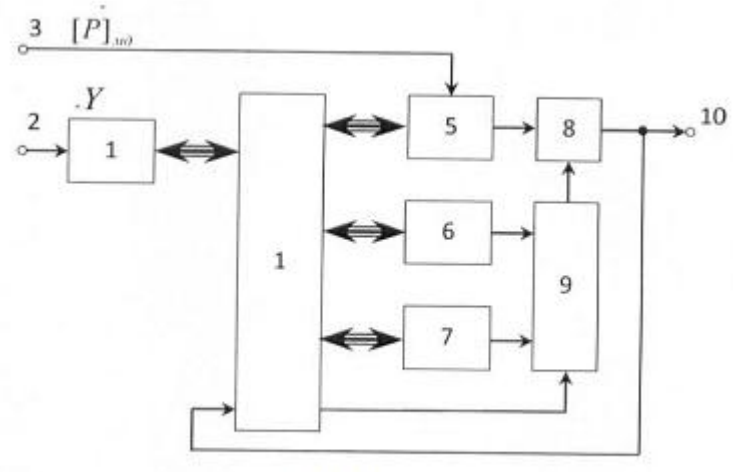
(72) Винахідник(и):
Николайчук Ярослав Миколайович (UA),
Якименко Ігор Зіновійович (UA),
Воронич Артур Романович (UA),
Волинський Орест Ігорович (UA)

(73) Власник(и):
ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ НАФТИ І ГАЗУ, вул. Карпатська, 15, м. Івано-Франківськ, 76019 (UA)

(54) ПРИСТРІЙ ВИЗНАЧЕННЯ ЗАЛИШКУ БАГАТОРОЗРЯДНОГО ЧИСЛА

(57) Реферат:

Пристрій визначення залишку багаторозрядного числа містить n-розрядний регістр зсуву, вхід якого підключений до шини запису кодового представлення числа. В нього додатково введено шину запису кодового представлення модуля P, яка підключена до першого входу додатково введеного к+1-розрядного регістра зсуву, другий адресний вхід, якого підключений до першого виходу додатково введеного блока управління.



Фіг. 1

UA 68872 U

Корисна модель належить до пристроїв опрацювання та перетворення даних, і може бути використана в системах передавання інформації, а також захисту даних від помилок та несанкціонованого доступу.

Відомий пристрій визначення залишку шляхом згортки по непарному модулю $P = 2^n-1$, який містить и-розрядний регістр і логічні схеми [1].

Недоліком такого пристрою є велика апаратна складність та функціональна обмеженість, що ускладнює його застосування при визначенні залишку багаторозрядних двійкових чисел з числом розрядів $2^{10}…2^{30}$, а також не забезпечує визначення залишку по довільному цілочисельному багаторозрядному модулю Р.

Відомий також пристрій обчислення залишку шляхом згортки унітарного коду числа, який містить лічильник і логічні схеми [2].

Недоліком такого пристрою є низька швидкодія, що обмежує його функціональні можливості при визначенні залишку багаторозрядних чисел.

Найбільш близьким за технічною суттю до корисної моделі, що заявляється, є пристрій визначення залишку шляхом згортки по непарному модулю, який містить лічильник, n-розрядний регістр зсуву і k-розрядний суматор, охоплений зворотнім зв'язком, шину запису кодового представлення числа [1].

Недоліком пристрою є велика апаратна складність обумовлена наявністю багаторозрядного двійкового суматора з числом розрядів рівним довжині коду k, багаторозрядного модуля Р та обмежені функціональні можливості визначення залишку тільки по непарному модулю.

В основу корисної моделі поставлена задача зменшення апаратної складності та розширення функціональних можливостей пристрою обчислення залишку багаторозрядного двійкового по довільному цілочисельному багаторозрядному модулю р.

Поставлена задача вирішується завдяки тому, що, згідно з корисною моделлю, пристрій, який містить n-розрядний регістр зсуву, вхід якого підключений до шини запису кодового представлення числа, додатково введено шину запису кодового представлення модуля Р, яка підключена до першого входу додатково введеного k+1-розрядного регістра зсуву, другий адресний вхід, якого підключений до першого виходу додатково введеного блока управління, другий і третій виходи якого відповідно підключені до перших входів додатково введених третього і четвертого k+1-розрядних регістрів зсуву, виходи, яких відповідно підключені до першого і другого входів додатково введеного мультиплексора, третій вхід якого підключений до четвертого виходу блока управління, а вихід підключений до першого входу додатково введеного накопичувального суматора, другий вхід якого підключений до виходу другого k+1-розрядного регістра зсуву, а вихід з'єднаний з другим входом блока управління і додатково введеною вихідною шиною кодового представлення залишку.

Суть корисної моделі пояснюється тим, що в основу роботи пристрою поставлено алгоритм обчислення залишку багаторозрядного двійкового числа Y по багаторозрядному цілочисельному модулю Р згідно з рекурсивним виразом:

$$b_i = [p]_{м∂} + 2b_{i-1} + a_i \quad i = n, n-1,…,1, \quad (1)$$

де и - розрядність числа Y, з якого визначається залишок b_i, a_i - біти двійкового числа Y, починаючи зі старшого розряду a_n, $[P]_{м∂}$ - k +1 розрядна мантиса доповнюючого коду модуля Р, b_i - текуче кодове значення залишку ($b_{i-1} = 0$).

Корисна модель ілюструється кресленнями, де показано структурну схему пристрою, де, 1 - перший n-розрядний регістр зсуву, 2 - шина запису кодового представлення числа Y, 3 - шина запису кодового представлення модуля Р, 4 - блок управління, 5 - другий k+1-розрядний регістр зсуву, 6 - третій k+1-розрядний регістр зсуву, 7 - четвертий k+1-розрядний регістр зсуву, 8 - однорозрядний накопичувальний суматор, 9 - мультиплексор, 10 - вихідна шина кодового представлення залишку b_i.

Пристрій працює таким чином.

На початку циклів визначення залишку числа Y у перший n-розрядний регістр зсуву 1 і другий k+1-розрядний регістр зсуву 5, згідно з адресними сигналами блока управління 4, відповідно записуються двійковий код числа Y та мантиса доповнюючого коду модуля Р, а в третій 6 і четвертий 7 k+1-розрядні регістри зсуву записуються нулі. На початку кожного наступного циклу роботи пристрою на четвертому виході блока управління 4 формується сигнал "1", що дозволяє зсув на один розряд в бік старших розрядів на коду залишку b_{i-1} у регістрі 6 та запис старшого біта числа Y a_i у молодший розряд третього регістра 6, що відповідає запису в цей регістр 2 $b_{i-1} + a_i$

В кожному текучому циклі роботи пристрою одночасно через мультиплексор 9 на входи однорозрядного накопичувального суматора 8, порозрядно зчитується код мантиси модуля Р($[P]_{м∂}$) розрядністю k + 1 та код відповідного регістра 6 або 7. При цьому одночасно

відбувається запис нового залишку b_i у відповідний регістр 7 або 6 згідно адресних входів блока управління 4.

У результаті на протязі k + 1 такту у однорозрядному накопичувальному суматорі 8 порозрядно формується сума кодів згідно виразу (1), яка завершується формуванням на виході суматора 8 останнього біта "0" або "1", значення якого надходить на другий вхід блока управління 4. При цьому, якщо вказаний біт є "1", то це означає, що текучий залишок b_i у регістрі 6 менший значення модуля p ($b_i < P$) і відбувається зсув інформації в регістрі 6 на один розряд в бік старших розрядів, а в молодший розряд записується наступний молодший біт числа Y. При формуванні на виході суматора сигналу "0", це означає, що $b_i \geq P$ і на вхід мультиплексора 9 подається сигнал "0", який формується на четвертому виході блока управління 4 і починається новий цикл сумування у суматорі 8 кодів $[P]_{мд}$ другого регістра 5 та четвертого регістра 7, та запис інформації у регістр 6 до появи біта "0" в кінці k+1 такту на виході суматора 8. У результаті виконується попередній цикл.

Після зчитування останнього молодшого біта числа Y a_i в одному з регістрів 6 або 7 формується код залишку b_i, який зчитується через мультиплексор 9 і суматор 8 на вихідну шину 10 пристрою, при цьому на виході другого регістра 5 формується сигнал "0".

Приклад, визначення залишку по непарному модулю:

Припустимо $Y = 100_{(10)}$ $1100100_{(2)}$, $P = 11_{(10)} = 1011$.

Тоді $b_1 = res100(mod11) = 1$.

Потрібно визначити b_1 над двійковими кодами Y та P:

1. У перший регістр 1 записуємо число $Y = 1100100_{(2)}$

2. У другий регістр 5 записуємо k+1 розрядну мантису доповнюючого коду $[P]_{мд} = 10101$, яку отримуємо наступним чином:

код числа P записуємо з нульовим бітом у старшому розряді:

$P = 01011_{(2)}$

інвертуємо цей код: P = 10100

додаємо до цього коду "1":

$$[P]_{мд} = \frac{\begin{array}{r}10100\\ +1.\end{array}}{10101}$$

3. У третій регістр 6 і четвертій 7 регістри записуємо нулі, тобто $b_i = 00000$ $b_{i-1} = 00000$; i = n, n-1,…1.

4. Блок управління 4 формує біт "0" на керуючий вхід мультиплексора 9, що дозволяє відповідно записувати та зчитувати інформацію з другого регістра 5 і третього регістра 6(b_i) та четвертого регістра 7(b_{i-1}) та записувати коди порозрядно вихідні коди суматора у четвертій регістр 7.

5. В кожному циклі роботи пристрою виконується сумування мантиси доповнюючого коду модуля P з значенням текучого залишку b_{i-m}. У нашому випадку має місце така операція

$$\begin{array}{rr}[p]_{мд} & 10101\\ 2b_i + a_i & {}^{+}\,00001\\ \hline [b_{i-m+1}]_{мд} & 11110\end{array} \quad i = n-1$$

6. Отримуємо мантису доповнюючого коду цієї операції додавання. Код цієї мантиси записуємо у регістр 6(b_i) або 7(b_{i-1}). Отримане значення "1" в k + 1 такті сумування показує, що $b_{i-1} < P$. Тоді відбувається зсув інформації у відповідному регістрі 6 або 7 і запис у молодший розряд a_{i-1}, біта числа Y, тобто

$$\begin{array}{rr} & 10101\\ P > b_i & {}^{+}\underline{00011}\\ & 11100\end{array} \quad i = n-2$$

$$\begin{array}{rr} & 10101\\ P > b_i & {}^{+}\underline{00010}\\ & 11011\end{array} \quad i = n-3$$

$$\begin{array}{rr} & 10101\\ P > b_i & {}^{+}\underline{01100}\\ & 00011\end{array} \quad i = n-4$$

7. Отриманий біт "0" надходить в блок управління, який запам'ятовує його і переключає мультиплексор 9, що приводить до подвоєння коду залишку в регістрі 7(b_{i-1}) та запису в молодший розряд текучого біта числа Y.

8. Після цього використовується операція сумування згідно з розрахунками:

$$\begin{array}{lll} 10101 & 10101 & 10101 \\ \underline{{}^{+}00011}\rightarrow & \underline{{}^{+}00110}\rightarrow & {}^{+}01100 \\ 10100 & 11011 & 00001 = b_1 \end{array}$$

Тобто $b_i = 00001_{(2)} = 1_{(10)}$, що відповідає $b_i = res100(mod11) = 1$.

Аналогічні розрахунки можна виконати при визначенні залишку по парному модулю:

Припустимо $Y = 25_{(10)} = 11001_{(2)}$, $p = 6_{(10)} = 110$.

Запишемо $[P]_{м\partial} = 0110 \xrightarrow{\bar{p}} 1001 \xrightarrow{+1} 1010$.

Виконаємо наступні операції:

$$\begin{array}{lll} 1010 & 1010 & 1010 \\ \underline{{}^{+}0001}\rightarrow & \underline{{}^{+}0011}\rightarrow & {}^{+}0110 \\ 1011 & 1101 & 0000 \end{array}$$

Оскільки в старшому розряді "0", то цей залишок зсувається на біт і додається новий біт числа:

$$\begin{array}{ll} 1010 & 1010 \\ \underline{{}^{+}0000}\rightarrow & {}^{+}0001 = b_1 \\ 1010 & 1011 \end{array}$$

Оскільки використані всі біти числа Y і $b_i < P$, то $b_1 = 0001_{(2)}$, що відповідає $b_1 = res25(mod6) = 1$.

При реалізації пристрою доцільно як регістри використати багаторозрядну флеш-пам'ять.

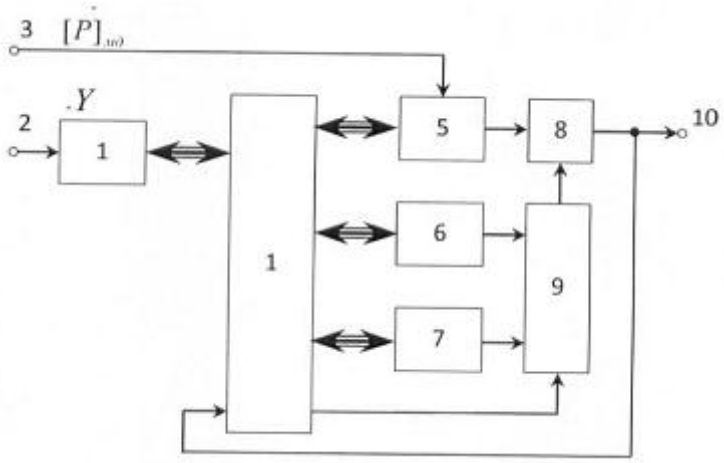
Джерела інформації:

[1] Хетагуров Я.А., Руднев Ю.П. Повышение надежности цифровых устройств методами избыточного кодирования. - М.: Энергия, 1974. - 272с.

[2] Новиков Л.Г., Шурыгин И.Т. Счётчики импульсов с коэффициентами счёта, управляемыми с помощью двоичного кода. Журнал "Приборы и системы управления" № 6, 1972. - С. 30-31.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій визначення залишку багаторозрядного числа, який містить n-розрядний регістр зсуву, вхід якого підключений до шини запису кодового представлення числа, який **відрізняється** тим, що додатково введено шину запису кодового представлення модуля Р, яка підключена до першого входу додатково введеного к+1-розрядного регістра зсуву, другий адресний вхід, якого підключений до першого виходу додатково введеного блоку управління, другий і третій виходи якого відповідно підключені до перших входів додатково введених третього і четвертого к+1-розрядних регістрів зсуву, виходи, яких відповідно підключені до першого і другого входів додатково введеного мультиплексора, третій вхід якого підключений до четвертого виходу блока управління, а вихід підключений до першого входу додатково введеного накопичувального суматора, другий вхід якого підключений до виходу другого к+1-розрядного регістра зсуву, а вихід з'єднаний з другим входом блока управління і додатково введеною вихідною шиною кодового представлення залишку.



Комп'ютерна верстка Д. Шеверун

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601