РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 744 815**(13) **C1**

(51) МПК
*G06F 7/72* (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
*G06F 7/72 (2021.01)*

(21)(22) Заявка: **2020120649, 22.06.2020**

(24) Дата начала отсчета срока действия патента:
**22.06.2020**

Дата регистрации:
**16.03.2021**

Приоритет(ы):
(22) Дата подачи заявки: **22.06.2020**

(45) Опубликовано: **16.03.2021** Бюл. № **8**

Адрес для переписки:
**355017, Ставропольский край, г. Ставрополь, ул. Пушкина, 1, Северо-Кавказский федеральный университет, Управление науки и технологий, Лиховид Андрей Александрович**

(72) Автор(ы):
**Бабенко Михаил Григорьевич (RU),**
**Кучуков Виктор Андреевич (RU),**
**Черных Андрей Николаевич (RU),**
**Кучеров Николай Николаевич (RU)**

(73) Патентообладатель(и):
**Федеральное государственное автономное образовательное учреждение высшего образования "Северо-Кавказский федеральный университет" (RU)**

(56) Список документов, цитированных в отчете о поиске: **RU 2256226 C2, 10.07.2005. RU 2275741 C2, 27.04.2006. RU 2187886 C1, 20.08.2002. US 6049858 A, 11.04.2000. EP 0992885 B1, 28.12.2005.**

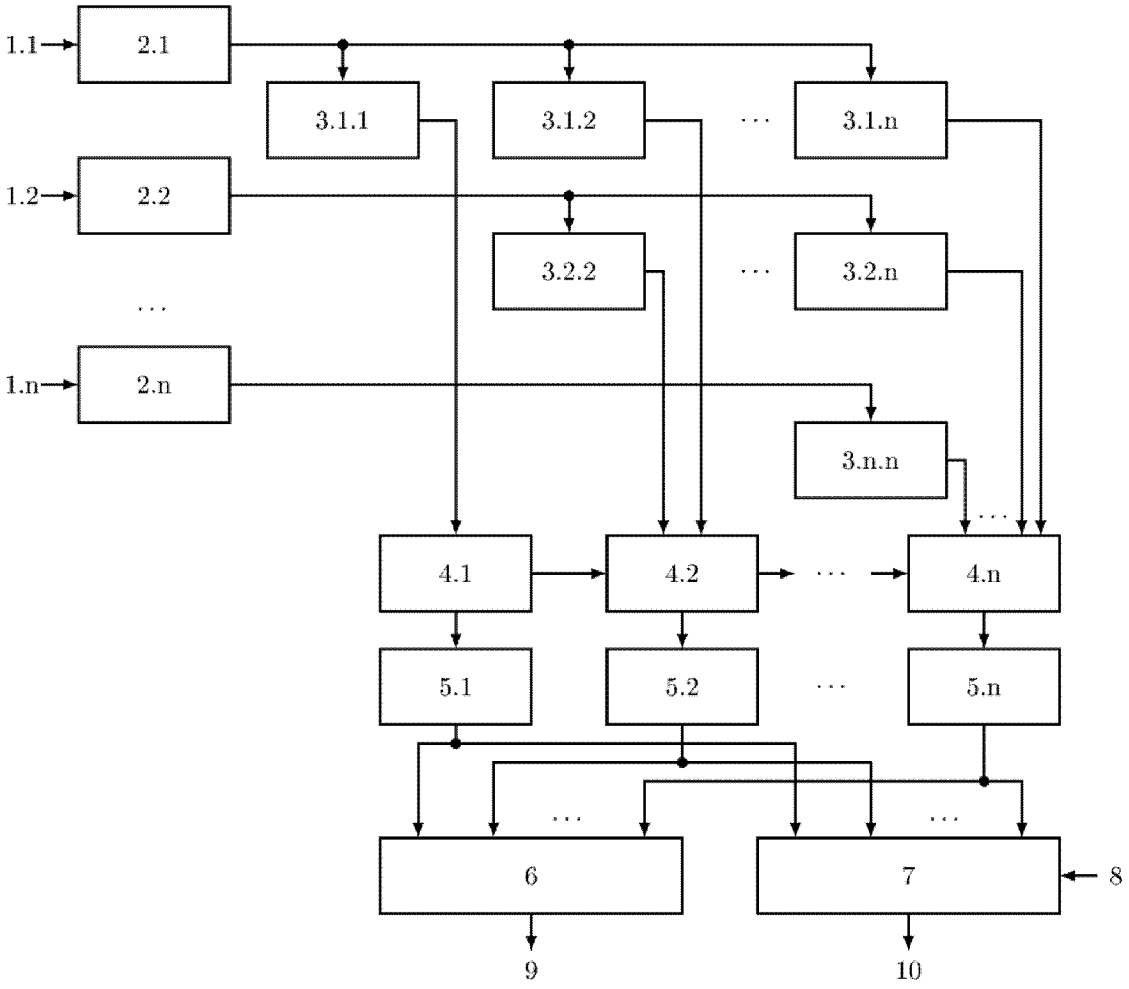
## (54) Устройство для перевода чисел из системы остаточных классов и расширения оснований

(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано в системах связи и обработки информации, функционирующих в системе остаточных классов (СОК). Техническим результатом заявляемого изобретения является расширение функциональных возможностей, а именно возможность получить остаток от деления по произвольному дополнительному модулю, а также восстановленное число в позиционной системе счисления. Данный технический результат достигается тем, что в устройство для перевода чисел из системы остаточных классов и расширения оснований с модулями $p_1, p_2, \dots, p_n$, содержащее n входов остатков, выход остатка по расширенному основанию, n регистров хранения остатков, (n-1) модулярный сумматор по модулю, треугольную матрицу из $\frac{n \cdot (n+1)}{2}$ умножителей, где умножители производят умножение на коэффициенты $\hat{b}_{j,i}$ ортогональных базисов $B_i$ системы остаточных классов (СОК), где $B_i = P_i \cdot \left|P_i^{-1}\right|_{p_i}$, $P_i = P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ – мультипликативная инверсия, $i = \overline{1,n}$, $P = \prod_{i=1}^{n} p_i$ - рабочий диапазон СОК, представленных в обобщенной позиционной системе счисления (ОПСС) с основаниями $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, дополнительно ввели модулярный сумматор по модулю $p_1$, n умножителей на основания ОПСС $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, сумматор с выходом восстановленного числа и модулярный сумматор с входом расширенного основания. 1 ил.

RU 2744815 C1

RU 2744815 C1




Структурная схема устройства

Фиг. 1

RU 2744815 C1

RU 2744815 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 744 815**(13) **C1**

(51) Int. Cl.
*G06F 7/72* (2006.01)

## (12) ABSTRACT OF INVENTION

(52) CPC
*G06F 7/72 (2021.01)*

(21)(22) Application: **2020120649, 22.06.2020**

(24) Effective date for property rights:
**22.06.2020**

Registration date:
**16.03.2021**

Priority:
(22) Date of filing: **22.06.2020**

(45) Date of publication: **16.03.2021** Bull. № **8**

Mail address:
**355017, Stavropolskij kraj, g. Stavropol, ul. Pushkina, 1, Severo-Kavkazskij federalnyj universitet, Upravlenie nauki i tekhnologij, Likhovid Andrej Aleksandrovich**

(72) Inventor(s):
**Babenko Mikhail Grigorevich (RU),**
**Kuchukov Viktor Andreevich (RU),**
**Chernykh Andrei Nikolaevich (RU),**
**Kucherov Nikolai Nikolaevich (RU)**

(73) Proprietor(s):
**Federalnoe gosudarstvennoe avtonomnoe obrazovatelnoe uchrezhdenie vysshego obrazovaniia "Severo-Kavkazskii federalnyi universitet" (RU)**

RU 2744815 C1

(54) **Device for transferring numbers from residue number system and base-radix extensions**

(57) Abstract:

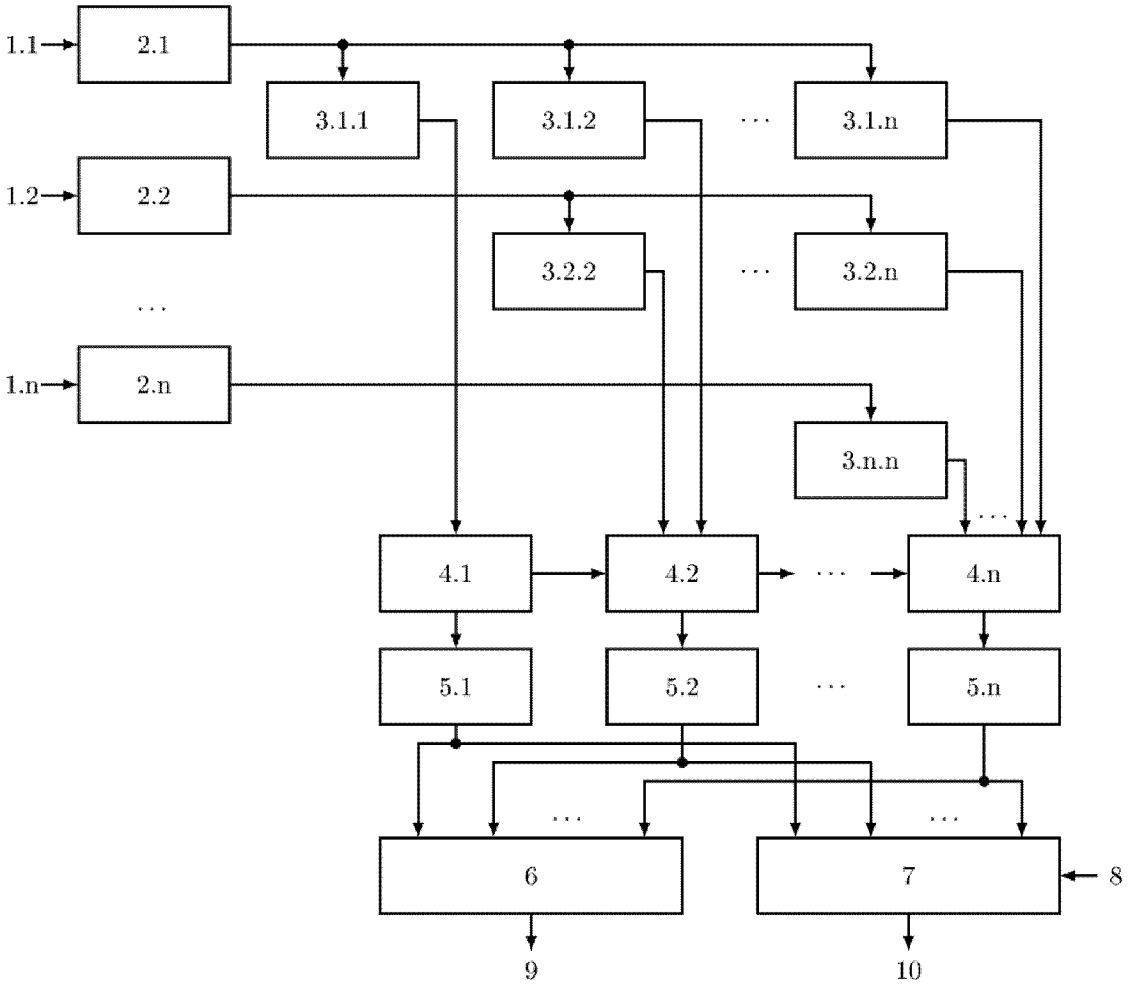
FIELD: computer technology.

SUBSTANCE: invention relates to computer technology and can be used in communication and information processing systems operating in the residue number system (RNS). The technical result of the claimed invention is to expand the functionality, namely the ability to obtain a residue of division by a random additional module, as well as the restored number in the radix numbering system. This technical result is achieved by the following: in a device for transferring numbers from the residue number system and base-radix extensions with modules $p_1, p_2, \dots, p_n$ containing n inputs of residues, the output of the residue in an extended base, n residue storage registers, (n-1) adder modulo, the triangular matrix $\frac{n \cdot (n+1)}{2}$ of multipliers, wherein the multipliers multiply by the coefficients $\hat{b}_{j,i}$ of the orthogonal bases $B_i$ of the residue number system (RNS), wherein $B_i = P_i \cdot \left|P_i^{-1}\right|_{p_i}$, $P_i = P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ is multiplicative inversion, $i = \overline{1,n}$, $P = \prod_{i=1}^{n} p_i$ is the operating range of RHS, generalized radix numeration system (GRNS) with base-radixes $\hat{w}_j = \prod_{i=1}^{j-1} p_i, j = \overline{1,n}$, a modulo-two adder $p_1$ was introduced, n multipliers by GRNS base radixes $\hat{w}_j = \prod_{i=1}^{j-1} p_i, j = \overline{1,n}$, an adder with an output of a restored number and an adder modulo with an input of an extended base-radix.

EFFECT: technical result of the claimed invention is to expand the functionality, namely the ability to obtain a residue of division by a random additional modulo, as well as the restored number in the radix numbering system.

1 cl, 1 dwg

RU 2744815 C1




Структурная схема устройства

Фиг. 1

RU 2744815 C1

RU 2744815 C1

Изобретение относится к вычислительной технике и может быть использовано в системах связи и обработки информации, функционирующих в системе остаточных классов (СОК).

Известно устройство для преобразования числа из системы остаточных классов в позиционный код (патент РФ №2293437, опубл. 10.02.2007), содержащее группу сдвиговых регистров, группу постоянных запоминающих устройств, причем информационные входы группы сдвиговых регистров являются соответствующими информационными входами устройства, при этом выходы группы сдвиговых регистров соединены с адресными входами группы постоянных запоминающих устройств, каждое из которых содержит пару констант $|a_{i-1} \cdot B_{i-1} + a_i \cdot B_i|_P$ разрядностью $]\log_2 P[$, причем количество постоянных запоминающих устройств в группе составляет $]n/2[$, и если $n$ - нечетное число, то количество констант в последнем постоянном запоминающем устройстве группы составляет $p_n - 1$, выходы группы постоянных запоминающих устройств соединены с соответствующими входами разрядно-параллельно сумматора по модулю, выходы которого являются выходами устройства, где $F$ - произведение всех модулей системы остаточных классов; $B_i$ - ортогональные базисы системы остаточных классов; $a_i$ - остаток по $i-$ му модулю системы остаточных классов; $n$ - количество модулей системы остаточных классов, при этом $1 \le i \le n$; $p$ - n-ый модуль системы остаточных классов.

Недостатком данного устройства является аппаратная избыточность и сложность нахождения остатков от деления по большому модулю $P$. Также недостатком является ограниченная функциональность, а именно невозможность расширения оснований.

Известно устройство для преобразования чисел из кода системы остаточных классов в позиционный код с контролем ошибок (авторское свидетельство №1797119, опубл. 23.02.1993), основанное на использовании Китайской теоремы об остатках и методе проекций.

Недостатком данного устройства является сложность алгоритма перевода в позиционную систему счисления и нахождение остатков от деления по большому модулю. Также недостатком является ограниченная функциональность, а именно невозможность расширения оснований.

Наиболее близким к заявленному изобретению является нейронная сеть для расширения кортежа числовой системы вычетов (патент РФ №2256226), содержащая входной слой нейронов для фиксирования числа нейронов и вычисления значений вычетов по модулям $p_1, p_2, \ldots, p_n$, усеченную треугольную матрицу нейронных сетей конечного кольца по модулям системы остаточных классов, нейронной сети конечного кольца по модулям системы остаточных классов, при этом упомянутые нейронные сети конечного кольца предназначены для вычисления значения $|\alpha_i \; b_{ij}|^{+}_{p_i}$ с учетом переноса, где $b_{ij}$ - коэффициенты обобщенной позиционной системы счисления, $\alpha_i$ - вычеты из числа А по $mod\ p_i$, в нее введены нейронные сети конечного кольца для выполнения модульного суммирования по всем основаниям и дополнительному расширяемому модулям и нейронная сеть для выполнения финального шага вычисления вычета по дополнительно расширяемому модулю, при этом в ней выходы нейронов входного слоя разветвлены на входы нейронных сетей конечного кольца усеченной треугольной матрицы, выполненной в виде распределенной памяти, выходы которых соединены с входами нейронных сетей конечного кольца с единичными синаптическими весами для

выполнения модульного суммирования по всем основным и дополнительно расширяемому модулям, выходы переносов которых $i$ модулей, где $i = 2,3,\dots n$, соединены с входами $i+1$ модулей, а выход суммы $n+1$ модуля соединен с входом нейронной сети для выполнения финального шага вычисления вычета по дополнительно расширяемому основанию.

Общим с прототипом является использование обобщенной позиционной системы счисления (ОПСС), треугольной матрицы коэффициентов базисов ОПСС.

Недостатком прототипа является необходимость нахождения большого числа остатков от деления, а также невозможность перевода в позиционную систему счисления.

Техническим результатом заявляемого изобретения является расширение функциональных возможностей, а именно возможность получить остаток от деления по произвольному дополнительному модулю, а также восстановленное число в позиционной системе счисления.

Данный технический результат достигается тем, что в устройство для перевода чисел из системы остаточных классов и расширения оснований с модулями $p_1, p_2, \dots, p_n$, содержащее n входов остатков, выход остатка по расширенному основанию, n регистров хранения остатков, (n-1) модулярный сумматор по модулю, треугольную матрицу из $\frac{n\cdot(n+1)}{2}$ умножителей, где умножители производят умножение на коэффициенты $\hat{b}_{j,i}$ ортогональных базисов $B_i$ системы остаточных классов (СОК), где $B_i = P_i \cdot |P_i^{-1}|_{p_i}$, $P_i = \frac{P}{p_i}$, $|P_i^{-1}|_{p_i}$ - мультипликативная инверсия, $i = \overline{1,n}$, $P = \prod_{i=1}^{n} p_i$ - рабочий диапазон СОК, представленных в обобщенной позиционной системе счисления (ОПСС) с основаниями $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, причем входы остатков соединены с соответствующими регистрами хранения остатков, выход первого регистра хранения остатка одновременно подключен к n умножителям, в которых происходит умножение на коэффициенты $\hat{b}_{1,i}$, $i = \overline{1,n}$, выход второго регистра хранения остатка одновременно подключен к (n-1) умножителю, в которых происходит умножение на коэффициенты $\hat{b}_{2,i}, i = \overline{2,n}$, и так далее, наконец выход n-го регистра хранения остатка подключен к умножителю, в котором происходит умножение на коэффициенты $\hat{b}_{n,n}$, выходы умножителей, в которых происходит умножение на $\hat{b}_{i,2}$, $i = \overline{1,2}$, подключены ко входам модулярного сумматора по модулю $p_2$, выход переноса которого подключен к ко входу переноса модулярного сумматора по модулю $p_3$, на входы которого поступают значения с выходов умножителей, в которых происходит умножение на $\hat{b}_{i,3}$, $i = \overline{1,3}$, а выход переноса соединен с входом переноса следующего модулярного сумматора, и так далее, наконец, выходы умножителей, в которых происходит умножение на $\hat{b}_{i,n}$, $i = \overline{1,n}$, подключены ко входам модулярного сумматора по модулю $p_n$, дополнительно введены модулярный сумматор по модулю $p_1$, n умножителей на основания ОПСС $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, сумматор с выходом восстановленного числа и модулярный сумматор с входом расширенного основания, причем выход умножителя, в котором происходит умножение на $\hat{b}_{1,1}$, подключен к входу модулярного сумматора по модулю $p_1$, выход переноса которого подключен ко входу переноса модулярного сумматора по модулю $p_2$, выходы

n модулярных сумматоров по модулю подключены к n соответствующим умножителям на основания ОПСС, выходы которых подключены одновременно ко входам сумматора и модулярного сумматора, выход которого является выходом остатка по расширенному основанию.

Сущность изобретения основана на следующем математическом аппарате. В системе остаточных классов любое число $X < P$ однозначно представляется набором остатков $x_i$ от деления числа $X$ на взаимно простые модули СОК $p_i$, называемые также основаниями, где $x_i \equiv X \bmod p_i$, $P = \prod_{i=1}^{n} p_i$ - рабочий диапазон СОК, $i = \overline{1,n}$. СОК позволяет выполнять операции сложения и умножения по каждому остатку независимо, без переносов между разрядами, как в позиционной системе счисления. Однако в ряде случаев, например, для обнаружения переполнения диапазона или при обнаружении и исправлении ошибок необходимо добавление одного или нескольких дополнительных модулей. Пусть добавлен модуль $p_{n+1}$, тогда новый диапазон позволит отображать любое число $X < P \cdot p_{n+1}$. Также в ряде случаев необходимо восстановить позиционное представление числа из системы остаточных классов. Основным методом восстановления числа $X$ из СОК в позиционную систему счисления является Китайская теорема об остатках

$$X = \left| \sum_{i=1}^{n} B_i \cdot x_i \right|_P,$$

где $B_i = P_i \cdot \left|P_i^{-1}\right|_{p_i}$, - ортогональные базисы СОК, $P_i = \frac{P}{p_i}$, $\left|P_i^{-1}\right|_{p_i}$ - мультипликативная инверсия. Однако данный метод подразумевает нахождение остатка от деления по большому модулю $P$, что является вычислительно сложной задачей.

Работа устройства основана на следующем алгоритме. Задается система остаточных классов с модулями $p_1, p_2, \ldots, p_n$, для которых вычисляют ортогональные базисы СОК $B_i$, $i = \overline{1,n}$. Вычисляются основания ОПСС $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, при этом $\hat{w}_0 = 1$. Ортогональные базисы СОК представляются в ОПСС как вектор значений $\hat{b}_{i,j}$, для которых $B_i = \sum_{j=1}^{n} \hat{b}_{i,j} \cdot \hat{w}_j$. При этом значения $\hat{b}_{i,j}$ образуют треугольную матрицу.

Пусть задано число $X = (x_1, x_2, \ldots, x_n)$ и надо по представлению в СОК $(x_1, x_2, \ldots, x_n)$ восстановить число $X$ в позиционной системе счисления, а также найти остаток от деления X по дополнительному модулю $p_{n+1}$, который будем обозначать $|X|_{p_{n+1}}$. Для этого $(x_1, x_2, \ldots, x_n)$ умножается на треугольную матрицу, т.е. находятся $U_i = \sum_{j=1}^{i} x_j \hat{b}_{j,i}$, $i = \overline{1,n}$. Затем вычисляются $\hat{x}_i = |\sigma_{i-1} + U_i|_{p_i}$ и $\sigma_i = \left\lfloor \frac{\sigma_{i-1} + U_i}{p_i} \right\rfloor$, при этом полагает, что $\sigma_0 = 0$. Можно заменить, что $\hat{x}_i$ и $\sigma_i$ соотносятся как остаток от деления суммы $(\sigma_{i-1} + U_i)$ на модуль $p_i$ и ранг суммы, т.е. перенос, во сколько раз значение суммы превосходит модуль.

Затем для перевода числа из СОК в позиционную систему счисления находят значение

выражения $X = \sum_{i=1}^{n} \hat{x}_i \cdot \hat{w}_i$, а для расширения оснований находят $|X|_{p_{n+1}} = \left| \sum_{i=1}^{n} \hat{x}_i \cdot \hat{w}_i \right|_{p_{n+1}}$.

Рассмотрим пример, иллюстрирующий работу алгоритма. Пусть задана система остаточных классов с 4 основаниями $p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11$. Тогда

$$P = \prod_{i=1}^{4} p_i = 1155.$$

Вычислим $P_i = \frac{P}{p_i}$, $|P_i^{-1}|_{p_i}$ и $B_i = P_i \cdot |P_i^{-1}|_{p_i}$:

$P_1 = 5 \cdot 7 \cdot 11 = 385$, $|P_1^{-1}|_{p_1} = |385^{-1}|_3 = 1$, следовательно $B_1 = 385$,

$P_2 = 3 \cdot 7 \cdot 11 = 231$, $|P_2^{-1}|_{p_2} = |231^{-1}|_5 = 1$, следовательно $B_2 = 231$,

$P_3 = 3 \cdot 5 \cdot 11 = 165$, $|P_3^{-1}|_{p_3} = |165^{-1}|_7 = 2$, следовательно $B_3 = 165 \cdot 2 = 330$,

$P_4 = 3 \cdot 5 \cdot 7 = 105$, $|P_4^{-1}|_{p_4} = |105^{-1}|_{11} = 2$, следовательно $B_3 = 105 \cdot 2 = 210$.

Вычислим $\hat{w}_j = \prod_{i=1}^{j-1} p_i$:

$\hat{w}_1 = 1$,

$\hat{w}_2 = 3$,

$\hat{w}_3 = 3 \cdot 5 = 15$,

$\hat{w}_4 = 3 \cdot 5 \cdot 7 = 105$.

Вычислим представление $B_i$ в ОПСС:

$B_1 \xleftarrow{\text{ОПСС}} \hat{B}_1 = [\hat{b}_{1,1}, \hat{b}_{1,2}, \hat{b}_{1,3}, \hat{b}_{1,4}] = [1, 3, 4, 3]$, проверка $1 + 3 \cdot 3 + 4 \cdot 15 + 3 \cdot 105 = 385$,

$B_2 \xleftarrow{\text{ОПСС}} \hat{B}_2 = [\hat{b}_{2,1}, \hat{b}_{2,2}, \hat{b}_{2,3}, \hat{b}_{2,4}] = [0, 2, 1, 2]$, проверка $0 + 2 \cdot 3 + 1 \cdot 15 + 2 \cdot 105 = 231$,

$B_3 \xleftarrow{\text{ОПСС}} \hat{B}_3 = [\hat{b}_{3,1}, \hat{b}_{3,2}, \hat{b}_{3,3}, \hat{b}_{3,4}] = [0, 0, 1, 3]$, проверка $0 + 0 \cdot 3 + 1 \cdot 15 + 3 \cdot 105 = 330$,

$B_4 \xleftarrow{\text{ОПСС}} \hat{B}_4 = [\hat{b}_{4,1}, \hat{b}_{4,2}, \hat{b}_{4,3}, \hat{b}_{4,4}] = [0, 0, 0, 2]$, проверка $0 + 0 \cdot 3 + 0 \cdot 15 + 2 \cdot 105 = 210$.

Пусть задано число числа $X \xleftarrow{\text{СОК}} (1, 2, 3, 4)$, тогда вычислим $U_i = \sum_{j=1}^{i} x_j \hat{b}_{j,i}$:

$U_1 = x_1 \cdot \hat{b}_{1,1} = 1 \cdot 1 = 1$,

$U_2 = x_1 \cdot \hat{b}_{1,2} + x_2 \cdot \hat{b}_{2,2} = 1 \cdot 3 + 2 \cdot 2 = 7$,

$U_3 = x_1 \cdot \hat{b}_{1,3} + x_2 \cdot \hat{b}_{2,3} + x_3 \cdot \hat{b}_{3,3} = 1 \cdot 4 + 2 \cdot 1 + 3 \cdot 1 = 9$,

$U_4 = x_1 \cdot \hat{b}_{1,4} + x_2 \cdot \hat{b}_{2,4} + x_3 \cdot \hat{b}_{3,4} + x_4 \cdot \hat{b}_{4,4} = 1 \cdot 3 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 2 = 24$.

Вычислим $\hat{x}_i = |\sigma_{i-1} + U_i|_{p_i}$ и $\sigma_i = \left\lfloor \frac{\sigma_{i-1} + U_i}{p_i} \right\rfloor$:

$\hat{x}_1 = |U_1|_{p_1} = |1|_3 = 1$, $\sigma_1 = \left\lfloor \frac{U_1}{p_1} \right\rfloor = \left\lfloor \frac{1}{3} \right\rfloor = 0$,

$\hat{x}_2 = |\sigma_1 + U_2|_{p_2} = |0 + 7|_5 = 2$, $\sigma_2 = \left\lfloor \frac{\sigma_1 + U_2}{p_2} \right\rfloor = \left\lfloor \frac{7}{5} \right\rfloor = 1$,

$\hat{x}_3 = |\sigma_2 + U_3|_{p_3} = |1 + 9|_7 = 3$, $\sigma_3 = \left\lfloor \frac{\sigma_2 + U_3}{p_3} \right\rfloor = \left\lfloor \frac{1 + 9}{7} \right\rfloor = 1$,

$\hat{x}_4 = |\sigma_3 + U_4|_{p_4} = |1 + 24|_{11} = 3$.

Отсюда получим:

$$X = \sum_{i=1}^{n} \hat{x}_i \cdot \hat{w}_i = 1 \cdot 1 + 2 \cdot 3 + 3 \cdot 15 + 3 \cdot 105 = 367.$$

Проверим полученное значение, $|367|_3 = 1$, $|367|_5 = 2$, $|367|_7 = 3$ и $|367|_{11} = 4$.

Пусть необходимо расширить основания на $p_5 = 13$. Тогда

$$|X|_{p_{n+1}} = \left|\sum_{i=1}^{n} \hat{x}_i \cdot \hat{w}_i\right|_{p_{n+1}} = |1 \cdot 1 + 2 \cdot 3 + 3 \cdot 15 + 3 \cdot 105|_{13} = |367|_{13} = 3.$$

Изобретение поясняется фигурой 1, на которой изображена структурная схема устройства для перевода чисел из системы остаточных классов и расширения оснований. На входы остатков 1.1-1.n, где $n$ - количество оснований системы остаточных классов подается число $(x_1, x_2, \ldots, x_n)$, представленное в СОК. Остатки с соответствующих входов остатков 1.1-1.n записываются в регистры хранения остатков 2.1-2.n, которые в прототипе обозначены как нейроны входного слоя. С выходов регистров хранения остатков 2.1-2.n остатки по соответствующим модулям подаются на умножители 3, которые образуют треугольную матрицу и вычисляют значения произведений остатка на коэффициенты базиса в ОПСС $x_j \hat{b}_{j,i}$. В прототипе функцию умножителей выполняют нейронные сети конечного кольца, однако помимо умножения остатка на коэффициент ОПСС, в прототипе дополнительно вычисляется остаток от деления по модулю и перенос, обозначающий во сколько раз произведение $x_j \hat{b}_{j,i}$ превосходит модуль $p_j$. Выход первого регистра хранения остатка 2.1 по модулю $p_1$ подключен ко входам n умножителей 3.1.1-3.1.n, которые вычисляют значения $x_1 \hat{b}_{1,i}$, $i = \overline{1,n}$, выход второго регистра хранения остатка 2.2 по модулю $p_2$ подключен ко входам $(n-1)$ умножителя 3.2.2-3.2.n, которые вычисляют значения $x_2 \hat{b}_{2,i}$, $i = \overline{2,n}$, и так далее, выход n-го регистра хранения остатка 2.n по модулю $p_n$ подключен ко входу умножителя 3.n.n, который вычисляет значение $x_n \hat{b}_{n,n}$. Выходы умножителей 3 подключены ко входам n модулярных сумматоров 4 по модулям $p_i$, $i = \overline{1,n}$, при этом выход умножителя 3.1.1 подключен ко входу первого модулярного сумматора 4.1 по модулю $p_1$ и выполняет вычисления $\hat{x}_1 = |U_1|_{p_1} = \left|x_1 \hat{b}_{1,1}\right|_{p_1}$, $\sigma_1 = \left\lfloor \frac{x_1 \hat{b}_{1,1}}{p_1} \right\rfloor$, значение $\hat{x}_1$ поступает на выход первого модулярного сумматора 4.1 по модулю $p_1$, значение $\sigma_1$ поступает на выход переноса первого модулярного сумматора 4.1 по модулю $p_1$, выходы умножителей 3.1.2 и 3.2.2 подключены ко входам второго модулярного сумматора 4.2 по модулю $p_2$, вход переноса которого подключен к выходу переноса первого модулярного сумматора 4.1 по модулю $p_1$, и выполняет вычисления $\hat{x}_2 = |\sigma_1 + U_2|_{p_2} = \left|\sigma_1 + x_1 \hat{b}_{1,2} + x_2 \hat{b}_{2,2}\right|_{p_2}$, $\sigma_2 = \left\lfloor \frac{\sigma_1 + x_1 \hat{b}_{1,2} + x_2 \hat{b}_{2,2}}{p_2} \right\rfloor$, значение $\hat{x}_2$ поступает на выход второго модулярного сумматора 4.2 по модулю $p_2$, значение $\sigma_2$ поступает на выход переноса второго модулярного сумматора 4.2 по модулю $p_2$, и так далее, выходы умножителей 3.i.n, $i = \overline{1,n}$, подключены ко входам n-го модулярного сумматора 4.n по модулю $p_n$, вход переноса которого подключен к выходу переноса (n-1)-го модулярного сумматора

4.n-1 по модулю $p_{n-1}$, и выполняет вычисления $\hat{x}_n = |\sigma_{n-1} + U_i|_{p_n} = \left|\sigma_{n-1} + \sum_{i=1}^{n} x_i \hat{b}_{i,n}\right|_{p_n}$, $\sigma_n = \left\lfloor \frac{\sigma_{n-1} + \sum_{i=1}^{n} x_i \hat{b}_{i,n}}{p_2} \right\rfloor$, значение $\hat{x}_n$ поступает на выход n-го модулярного сумматора 4.n по модулю $p_n$, значение $\sigma_n$ поступает на выход переноса n-го модулярного сумматора 4.n по модулю $p_n$, который не подключен к другим элементам. Значения $\hat{x}_i$ с выходов i-х модулярных сумматоров 4.i по модулю $p_i$ подаются на входы i-х умножителей 5.i на основания ОПСС, $i = \overline{1,n}$, в которых происходит умножение $\hat{x}_i$ на $\hat{w}_i = \prod_{j=1}^{i-1} p_j$. Выход i-го умножителя 5.i на основания ОПСС подключен к i-м входам сумматора 6 и модулярного сумматора 7, $i = \overline{1,n}$, на вход расширенного основания 8 модулярного сумматора 7 подается значение модуля $p_{n+1}$, на выход восстановленного числа 9 сумматора 6 подается восстановленное число X в позиционной системе счисления, а на выход остатка по расширенному основанию 10 модулярного сумматора 7 значение числа по расширенному основанию, т.е. $|X|_{p_{n+1}}$.

На основе предыдущего примера рассмотрим работу устройства. n=4, $p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11$. На входы остатков 1.1-1.4 подаются значения (1,2,3,4), которые затем записываются в регистры хранения остатка 2.1-2.4 по соответствующим модулям. Значение 1 с выхода регистра хранения остатка 2.1 по модулю $p_1$ одновременно поступает на входы умножителя 3.1.1, где происходит умножение остатка $x_1 = 1$, на первый коэффициент базиса $B_1$ в ОПСС $\hat{b}_{1,1} = 1$, результат умножения $x_1 \cdot \hat{b}_{1,1} = 1$, умножителя 3.1.2, где происходит умножение на $\hat{b}_{1,2} = 3$, результат умножения $x_1 \cdot \hat{b}_{1,2} = 3$, умножителя 3.1.3, где происходит умножение на $\hat{b}_{1,3} = 4$, результат умножения $x_1 \cdot \hat{b}_{1,3} = 4$, умножителя 3.1.4, где происходит умножение на $\hat{b}_{1,4} = 3$, результат умножения $x_1 \cdot \hat{b}_{1,4} = 3$. Значение 2 с выхода регистра хранения остатка 2.2 по модулю $p_2$ одновременно поступает на входы умножителя 3.2.2, где происходит умножение остатка $x_2 = 2$, на второй коэффициент базиса $B_2$ в ОПСС $\hat{b}_{2,2} = 2$, результат умножения $x_2 \cdot \hat{b}_{2,2} = 4$, умножителя 3.2.3, где происходит умножение на $\hat{b}_{2,3} = 1$, результат умножения $x_2 \cdot \hat{b}_{2,3} = 2$, умножителя 3.2.4, где происходит умножение на $\hat{b}_{2,4} = 2$, результат умножения $x_2 \cdot \hat{b}_{2,4} = 4$. Значение 3 с выхода регистра хранения остатка 2.3 по модулю $p_3$ одновременно поступает на входы умножителя 3.3.3, где происходит умножение остатка $x_3 = 3$, на третий коэффициент базиса $B_3$ в ОПСС $\hat{b}_{3,3} = 1$, результат умножения $x_3 \cdot \hat{b}_{3,3} = 2$, умножителя 3.3.4, где происходит умножение на $\hat{b}_{3,4} = 3$, результат умножения $x_3 \cdot \hat{b}_{3,4} = 9$. Значение 4 с выхода регистра хранения остатка 2.4 по модулю $p_4$ поступает на вход умножителя 3.4.4, где происходит умножение остатка $x_4 = 4$, на четвертый коэффициент базиса $B_4$ в ОПСС $\hat{b}_{4,4} = 2$, результат умножения $x_4 \cdot \hat{b}_{4,4} = 8$. Значения коэффициентов ОПСС $b_{i,j}$ зависят только от заданной СОК и могут быть записаны в память.

Далее значение 1 с умножителя 3.1.1 поступает на первый модулярный сумматор 4.1 по модулю $p_1 = 3$. Поскольку $\hat{x}_1 = |1|_3 = 1$ и $\sigma_1 = \left\lfloor \frac{1}{3} \right\rfloor = 0$, на выход модулярного сумматора 4.1 подается 1, а на выход переноса 0.

Значение 3 с умножителя 3.1.2, значение 4 с умножителя 3.2.2 и значение 0 с выхода переноса модулярного сумматора 4.1 поступают на второй модулярный сумматор 4.2 по модулю $p_2 = 5$ . Поскольку $\hat{x}_2 = |3 + 4 + 0|_5 = 2$ и $\sigma_2 = \left\lfloor \frac{7}{5} \right\rfloor = 1$ , на выход модулярного сумматора 4.2 подается 2, а на выход переноса 1.

Значение 4 с умножителя 3.1.3, значение 2 с умножителя 3.2.3, значение 3 с умножителя 3.3.3 и значение 1 с выхода переноса модулярного сумматора 4.2 поступают на третий модулярный сумматор 4.3 по модулю $p_3 = 7$ . Поскольку $\hat{x}_3 = |4 + 2 + 3 + 1|_7 = 3$ и $\sigma_3 = \left\lfloor \frac{10}{7} \right\rfloor = 1$ , на выход модулярного сумматора 4.3 подается 3, а на выход переноса 1.

Значение 3 с умножителя 3.1.4, значение 4 с умножителя 3.2.4, значение 9 с умножителя 3.3.4, значение 8 с умножителя 3.4.4 и значение 1 с выхода переноса модулярного сумматора 4.3 поступают на четвертый модулярный сумматор 4.4 по модулю $p_4 = 11$ . Поскольку $\hat{x}_4 = |3 + 4 + 9 + 8|_{11} = 3$ , на выход модулярного сумматора 4.4 подается 3.

Значение 1 с выхода модулярного сумматора 4.1 поступает на вход умножителя 5.1 на основания ОПСС, где умножается на $\hat{w}_1 = 1,$ на выход умножителя 5.1 подается 1. Значение 2 с выхода модулярного сумматора 4.2 поступает на вход умножителя 5.2 на основания ОПСС, где умножается на $\hat{w}_2 = 3,$ на выход умножителя 5.2 подается 6. Значение 3 с выхода модулярного сумматора 4.3 поступает на вход умножителя 5.3 на основания ОПСС, где умножается на $\hat{w}_3 = 15,$ на выход умножителя 5.3 подается 45. Значение 3 с выхода модулярного сумматора 4.4 поступает на вход умножителя 5.4 на основания ОПСС, где умножается на $\hat{w}_4 = 105,$ на выход умножителя 5.4 подается 315. При этом основания ОПСС $\hat{w}_i$ зависят только от модулей СОК и могут быть записаны в память.

Значения с выходов умножителей 5.1-5.4 на основания ОПСС поступают на входы сумматора 6, где происходит сложение 1+6+45+315=367, результат которого подается на выход 9 восстановленного числа. Одновременно значения с выходов умножителей 5.1-5.4 на основания ОПСС поступают на входы модулярного сумматора 7, на вход 8 расширенного модуля которого поступает значение $p_{n+1} = 13$ . В модулярном сумматоре вычисляется сложение по модулю $|1 + 6 + 45 + 315|_{13} = 3$, результат которого подается на выход 10 остатка по расширенному основанию.

Можно заметить, что при реализации устройства отсутствует ресурсоемкая операция нахождения остатка по большому модулю $P = 1155$ . Также в отличие от прототипа сокращено количество умножителей 3 и упрощены реализуемые ими функции. За счет введения входа 8 расширенного основания устройство позволяет вычислить остаток по произвольному расширенному основанию, а введение сумматора 6 позволяет получить позиционное представление числа.

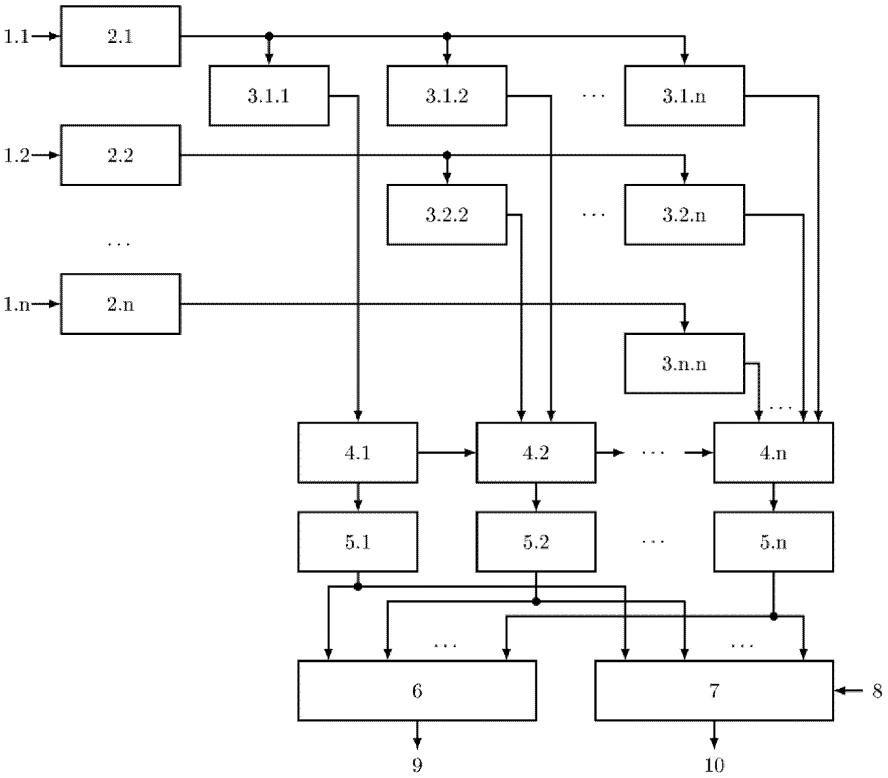
Реализация всего устройства возможна с использованием программируемых логических интегральных схем (ПЛИС) и может использоваться как отдельное устройство, так и как сопроцессор для выполнения немодульных операций.

## (57) Формула изобретения

Устройство для перевода чисел из системы остаточных классов и расширения оснований с модулями $p_1, p_2, \ldots, p_n$, содержащее n входов остатков, выход остатка по расширенному основанию, n регистров хранения остатков, (n-1) модулярный сумматор

по модулю, треугольную матрицу из $\frac{n\cdot(n+1)}{2}$ умножителей, где умножители производят умножение на коэффициенты $\hat{b}_{j,i}$ ортогональных базисов $B_i$ системы остаточных классов (СОК), где $B_i = P_i \cdot \left|P_i^{-1}\right|_{p_i}$, $P_i = P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ – мультипликативная инверсия, $i = \overline{1,n}$, $P = \prod_{i=1}^{n} p_i$ - рабочий диапазон СОК, представленных в обобщенной позиционной системе счисления (ОПСС) с основаниями $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, причем входы остатков соединены с соответствующими регистрами хранения остатков, выход первого регистра хранения остатка одновременно подключен к n умножителям, в которых происходит умножение на коэффициенты $\hat{b}_{1,i}, i = \overline{1,n}$, выход второго регистра хранения остатка одновременно подключен к (n-1) умножителю, в которых происходит умножение на коэффициенты $\hat{b}_{2,i}, i = \overline{2,n}$ и так далее, наконец, выход n-го регистра хранения остатка подключен к умножителю, в котором происходит умножение на коэффициенты $\hat{b}_{n,n}$, выходы умножителей, в которых происходит умножение на $\hat{b}_{i,2}$, $i = \overline{1,2}$, подключены к входам модулярного сумматора по модулю $p_2$, выход переноса которого подключен к входу переноса модулярного сумматора по модулю $p_3$, на входы которого поступают значения с выходов умножителей, в которых происходит умножение на $\hat{b}_{i,3}$, $i = \overline{1,3}$, а выход переноса соединен с входом переноса следующего модулярного сумматора и так далее, наконец, выходы умножителей, в которых происходит умножение на $\hat{b}_{i,n}$, $i = \overline{1,n}$, подключены к входам модулярного сумматора по модулю $p_n$, отличающееся тем, что в него введены модулярный сумматор по модулю $p_1$, n умножителей на основания ОПСС $\hat{w}_j = \prod_{i=1}^{j-1} p_i$, $j = \overline{1,n}$, сумматор с выходом восстановленного числа и модулярный сумматор с входом расширенного основания, причем выход умножителя, в котором происходит умножение на $\hat{b}_{1,1}$, подключен к входу модулярного сумматора по модулю $p_1$, выход переноса которого подключен к входу переноса модулярного сумматора по модулю $p_2$, выходы n модулярных сумматоров по модулю подключены к n соответствующим умножителям на основания ОПСС, выходы которых подключены одновременно к входам сумматора и модулярного сумматора, выход которого является выходом остатка по расширенному основанию.

1




Фиг. 1 Структурная схема устройства