УКРАЇНА

(19) UA (11) 59628 (13) U

(51) МПК (2011.01)
G11B 20/10 (2006.01)
G06F 17/00

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) ПРИСТРІЙ ДЛЯ ПЕРЕБОРУ ПЕРЕСТАНОВОК

(21) u201012855
(22) 29.10.2010
(24) 25.05.2011
(46) 25.05.2011, Бюл.№ 10, 2011 р.
(72) БОРИСЕНКО ОЛЕКСІЙ АНДРІЙОВИЧ, ГОРЯЧЕВ ОЛЕКСІЙ ЄВГЕНІЙОВИЧ
(73) СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
(57) Пристрій для перебору перестановок, що містить блок керування, перший лічильник, перший дешифратор, перший комутатор і блок порівняння, який **відрізняється** тим, що додатково містить факторіальний лічильник, блок перетворення, другий лічильник, другий дешифратор, блок сортування та другий комутатор, причому перший вхід блока керування є входом запуску пристрою, а вихід з'єднаний з входом першого і другого лічильників, першим входом блока перетворення, першим входом блока сортування та входом факторіального лічильника, вихід якого з'єднаний з другим входом блока перетворення, перший вихід якого є інформаційним виходом пристрою, а другий вихід з'єднаний з інформаційним входом першого комутатора, вихід якого з'єднаний з першим входом блока порівняння і другим входом блока сортування, вихід якого з'єднаний з інформаційним входом другого комутатора, вихід другого комутатора з'єднаний з другим входом блока порівняння, вихід якого з'єднаний з другим входом блока керування, вхід першого дешифратора з'єднаний з виходом першого лічильника, а вихід з'єднаний із третім входом блока перетворення та керуючим входом першого комутатора, вхід другого дешифратора з'єднаний з виходом другого лічильника, а вихід з'єднаний із третім входом блока сортування та керуючим входом другого комутатора.

Корисна модель належить до галузі автоматики й обчислювальної техніки, призначена для перебору всіх перестановок порядку n і може бути використана при рішенні задач комбінаторної оптимізації, а також у системах захисту інформації від несанкціонованого доступу та перешкодостійкої передачі даних.

Відомий пристрій для перебору перестановок, що містить блок керування і блок декодування, причому блок керування містить групу регістрів, дешифратор, схему вибору мінімального числа, ключі і елемент затримки, а блок декодування містить групу регістрів, блоки ділення, суматори, елементи затримки, елементи АБО, ключі (див. ав.св. СРСР №1410056, М.кл., G06F 15/20, 1988 р.).

До недоліків даного пристрою відносяться значні апаратурні витрати завдяки використанню суматорів і додаткових регістрів і невисока швидкодія через використання блоків ділення для перетворення номера в перестановку.

Відомий також пристрій для перебору сполучень, розміщень і перестановок, що містить дві групи регістрів, дві групи елементів І, дві групи елементів АБО, групу елементів порівняння, лічильник, дешифратор, три елементи затримки, блок керування, генератор тактових імпульсів, перемикач, комутатор, вихідний регістр і елемент АБО (див. ав.св. СРСР №1124319, М.кл., G06F 15/20, 1984 р.). Даний пристрій є найбільш близьким до заявляємого технічного рішення, тому й обраний як прототип.

Недоліком прототипу є недостатньо висока швидкодія через фіксовану кількість тактів порівняння елементів перестановки.

В основу корисної моделі поставлена задача підвищення швидкодії пристрою перебору перестановок і зменшення апаратурних витрат на його реалізацію шляхом введення нових конструктивних ознак. Поставлена задача вирішується тим, що в пристрій для перебору перестановок, що містить блок керування, перший лічильник, перший дешифратор, перший комутатор і блок порівняння, відповідно до корисної моделі, додатково введено факторіальний лічильник, блок перетворення, другий лічильник, другий дешифратор, блок сортування та другий комутатор, причому перший вхід блока керування є входом запуску пристрою, а

(19) UA (11) 59628 (13) U

вихід з'єднаний з входом першого і другого лічильників, першим входом блока перетворення, першим входом блока сортування та входом факторіального лічильника, вихід якого з'єднаний з другим входом блока перетворення, перший вихід якого є інформаційним виходом пристрою, а другий вихід з'єднаний з інформаційним входом першого комутатора, вихід якого з'єднаний з першим входом блока порівняння і другим входом блока сортування, вихід якого з'єднаний з інформаційним входом другого комутатора, вихід другого комутатора з'єднаний з другим входом блока порівняння, вихід якого з'єднаний з другим входом блока керування, вхід першого дешифратора з'єднаний з виходом першого лічильника, а вихід з'єднаний із третім входом блока перетворення та керуючим входом першого комутатора, вхід другого дешифратора з'єднаний з виходом другого лічильника, а вихід з'єднаний із третім входом блока сортування та керуючим входом другого комутатора.

Причинно-наслідковий зв'язок між сукупністю ознак корисної моделі і технічним результатом полягає в наступному. Завдяки використанню факторіального лічильника знижуються апаратурні витрати на схеми ділення двійкового числа і підвищується швидкодія за рахунок більш швидкого у порівнянні з алгоритмом, що використовує ділення двійкового числа, перебору факторіальних чисел (Для перетворення двійкового числа в факторіальне число довжини n потрібно n операцій ділення). Для виконання перетворення факторіального числа в перестановку використовується швидкодіючий алгоритм генерації перестановок (Борисенко А.А., Кулик І.А., Горячев О.Є. Електронна система генерації перестановок на базі факторіальних чисел. Вісник СумДУ. Технічні науки. - 2007. - №1. - с 183-188). Для того щоб знайти відповідність між числом в факторіальній системі числення і перестановкою, необхідно цифру, яка стоїть в n-му розряді факторіального числа залишити без змін і вважати її першим елементом перестановки. Наступну цифру (n-1)-го розряду факторіального числа необхідно порівняти з першим елементом перестановки і, якщо вона буде дорівнювати йому чи буде більше, то необхідно збільшити цю цифру на 1, а якщо ні, то залишити її без змін. В обох випадках буде отриманий другий елемент перестановки. Далі в загальному випадку спочатку виконують порівняння цифри факторіального числа з найменшим елементом серед уже знайдених елементів перестановки. Якщо ця цифра дорівнює цьому найменшому елементу або більше за нього, то тоді вона збільшується на одиницю. В іншому випадку вона стає черговим елементом перестановки. Збільшена ж на одиницю цифра факторіального числа далі порівнюється з найменшим елементом сформованої частини перестановки без урахування елемента, щодо якого вже відбулося порівняння, і далі цикл повторюється до тих пір, поки не буде сформований елемент перестановки. Далі вибирають наступну цифру факторіального числа і за допомогою наведеного вище правила знаходять новий елемент перестановки, і так триває до останньої цифри факторіального числа. Завдяки використанню алгоритму генерації перестановок, реалізованого за допомогою блока перетворення, блока сортування і блока порівняння, знижуються витрати апаратури, необхідної для зберігання проміжних та кінцевих величин, а також схем вибірки мінімального значення.

На Фіг.1 наведена структурна схема пристрою для перебору перестановок.

Пристрій містить блок 1 керування, факторіальний лічильник 2, перший і другий лічильники 3, 4 відповідно, перший і другий дешифратори 5, 6 відповідно, блок 7 перетворення, блок 8 сортування, перший і другій комутатори 9, 10 відповідно та блок 11 порівняння.

Перший вхід блока 1 керування є входом запуску пристрою, на другий вхід подається сигнал з виходу блока 11 порівняння, а вихід з'єднаний з входом першого та другого лічильників 3, 4 відповідно, входом факторіального лічильника 2, першим входом блока 7 перетворення і першим входом блока 8 сортування. Вихід факторіального лічильника 2 з'єднаний з другим входом блока 7 перетворення. Вихід першого лічильника 3 з'єднаний зі входом першого дешифратора 5, вихід якого з'єднаний з третім входом блока 7 перетворення і керуючим входом першого комутатора 9. Перший вихід блока 7 перетворення є інформаційним виходом пристрою, а другий вихід з'єднаний з інформаційним входом першого комутатора 9, вихід якого з'єднаний з першим входом блока 11 порівняння і другим входом блока 8 сортування. Вихід другого лічильника 4 з'єднаний зі входом другого дешифратора 6, вихід якого з'єднаний з третім входом блока 8 сортування і керуючим входом другого комутатора 10. Вихід блока 8 сортування з'єднаний з інформаційним входом другого комутатора 10, вихід якого з'єднаний з другим входом блока 11 порівняння.

За допомогою факторіального лічильника 2 вирішується завдання швидкого перебору факторіальних чисел, що не потребує значних апаратурних витрат. Даний лічильник представляє собою пристрій, призначений для послідовного перебору всіх факторіальних чисел довжини n (Горячев О.Є. Побудова факторіальне чисел на основі двійкових лічильників. Вісник СумДУ. Технічні науки. - 2008. - № 4. - С. 16-23).

Блок 7 перетворення призначений для здійснення переходу від цифр факторіального числа, що одержується в факторіальному лічильнику 2, до перестановки. Структура блока 7 перетворення представлена на Фіг.2. Блок містить n елементів І 12 і n двійкових лічильників 13. На вхід блока подаються сигнали 14 факторіального лічильника 2, сигнали 15 першого дешифратора 5 і сигнали 16 блока 1 керування. На вхід кожного з лічильників 13_1 (i=1,2,...n) подається сигнал 14; з виходу факторіального лічильника 2, сигнал 16_2 дозволу запису, сигнал 16_3 обнулення, тактовий сигнал 16_4 і сигнал з виходу елемента І 12_i, на вхід якого подається рахунковий сигнал 16_1 і сигнал 15_i з першого дешифратора 5. Вихід 17 лічильників 13 є інформаційним виходом пристрою перебору перестановок, з виходу 18 сигнал подається на входи першого комутатора 9.

Блок 8 сортування виконує завдання сортування сформованих у процесі перетворення елементів перестановки в порядку зростання їх значень. Структурна схема блока 8 сортування зображена на Фіг.3. Вона містить n-2 елементів І 19, n-2 комутаторів 20 і n-1 регістрів 21. На вхід блока подаються сигнали 22 блока 1 керування, сигнали 23 другого дешифратора 6 і сигнали 24 першого комутатора 9. На вхід елементів І 19_j (j=1,2,...n-2) подається сигнал 22_3 дозволу запису і сигнал 23_{j+i} з другого дешифратора 6, а сигнал з їхнього виходу подається на вхід регістрів 21_j, крім того, на вхід елементів І 19_1-19_{n-3} подається сигнал с виходу наступного за номером елемента І. На вхід комутаторів 20_j подається сигнал з виходу регістрів 21_j і сигнал 24 з виходу першого комутатора 9, сигнал з їхнього виходу подається на вхід регістрів 21_{j+1}. На вхід регістрів 21_1-21_{n-1} також подається сигнал 22_1 обнулення і тактовий сигнал 22_2 від блока 1 керування, крім того на вхід регістра 21_{n-1} безпосередньо подається сигнал 22_3 дозволу запису.

Пристрій для перебору перестановок працює наступним чином:

При подачі сигналу "Пуск" на вхід блока 1 керування відбувається примусове обнулення елементів пам'яті пристрою. Далі в факторіальному лічильнику 2 відбувається генерація першого факторіального числа, цифри розрядів якого потім надходять на входи лічильників 13 блока 7 перетворення, відкриті для запису сигналом 16_2 блока керування 1. На вхід першого дешифратора 5 в цей час надходить перша комбінація (що містить всі нулі) з виходу першого лічильника 3, що забезпечує позитивний сигнал на першому виході першого дешифратора 5. Даний сигнал надходить на вхід першого комутатора 9 і відкриває для передачі сигнали з виходів лічильника 13_1 блока 7 перетворення, в якому записана цифра старшого розряду факторіального числа. Під впливом сигналу 22_3 дозволу запису, що надходить з виходу блока 1 керування, вона записується в перший регістр 21_1 блока 8 сортування. Потім відбувається збільшення числа на одиницю у першому лічильнику 3, що відкриває для зчитування з лічильника 13_2 блока 7 перетворення наступну цифру факторіального числа. В цей час перша комбінація з виходу другого лічильника 4 подається на вхід другого дешифратора 6, сигнал з виходу якого потім поступає на вхід другого комутатора 10 і відкриває для зчитування перший регістр 21_1 блока 8 сортування. Комбінації з виходів першого і другого комутаторів 9, 10 відповідно надходять на вхід блока 11 порівняння. На підставі результатів порівняння, отриманих з виходу блока 11 порівняння, блоком 1 керування здійснюються наступні дії. Якщо цифра факторіального числа, що міститься в лічильнику 13_2 блока 7 перетворення, менше елемента перестановки, що міститься в регістрі 21_1 блока 8 сортування, то вона без змін записується в перший регістр 21_1 блока 8 сортування, елемент з першого регістра 21_1 при цьому переписується в другій регістр 21_2. Якщо цифра факторіального числа більше або дорівнює елементу перестановки, то відбувається її збільшення на одиницю і запис у другій регістр 21_2 блока 8 сортування. Далі пристрій переходить до перетворення наступної цифри факторіального числа.

У загальному випадку процес перетворення k-тої цифри факторіального числа відбувається наступним чином. З виходу першого лічильника 3 k-та комбінація надходить на вхід першого дешифратора 5 і перетворюється в одиничний сигнал на його k-тому виході. Даний сигнал подається на вхід першого комутатора 9 і відкриває для передачі на вхід блока 11 порівняння комбінацію з виходів k-того лічильника 13_k блока 7 перетворення. На другий вхід блока 11 порівняння подаються отримані раніше елементи перестановки з блока 8 сортування, починаючи з першого регістра 21_1. Вибір регістру, комбінація з виходів якого буде передана на вхід блока 11 порівняння, здійснюється за допомогою другого лічильника 4 і другого дешифратора 6. Якщо цифра факторіального числа, що перетворюється, дорівнює елементу перестановки, з яким порівнюється, або більше його, то вона збільшується на одиницю і порівнюється з наступним елементом перестановки. Якщо ж цифра факторіального числа менше елемента перестановки, то вона без змін записується в регістр 21 блока 8 сортування, в якому був записаний елемент перестановки, з яким відбувалося порівняння. При цьому відбувається перезапис значень елементів перестановки в блоці 8 сортування в наступний за номером регістр, починаючи з порівнюваного елемента. У разі, коли цифра факторіального числа більше або дорівнює останньому елементу перестановки з раніше отриманих, вона збільшується на одиницю і записується в перший незаповнений регістр 21_k блока 8 сортування.

Приклад переходу від факторіальне числа до перестановки показано у таблиці.

Виведення елементів перестановки з виходу блока 7 перетворення може здійснюватися як безпосередньо після їх отримання, так і після завершення циклу генерації всіх елементів.

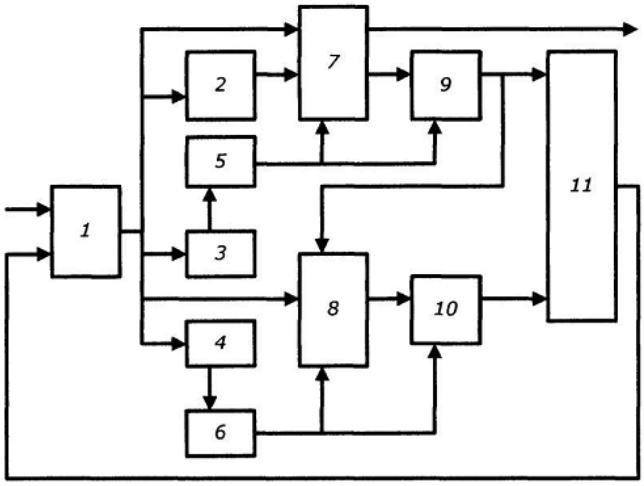
Після закінчення циклу генерації відбувається скидання в нульовий стан першого та другого лічильників 3, 4 відповідно, а також лічильників блока 7 перетворення і регістрів блока 8 сортування. Далі блоком 1 керування генерується сигнал, що збільшує число в факторіальному лічильнику 2 на одиницю, після чого починається наступний цикл отримання перестановки.

Таблиця

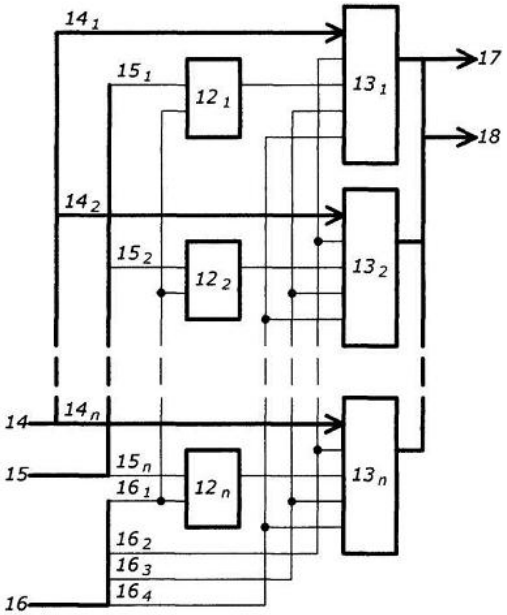
Перетворення факторіального числа 01441210 в перестановку

Такт	Перший дешифратор	Блок перетворення	Другий дешифратор	Блок сортування
1	10000000	01441210	1000000	0000000
2	01000000	01441210	1000000	0000000
3	00100000	02441210	1000000	0200000
4	00100000	02541210	0100000	0200000
5	00010000	02641210	1000000	0260000
6	00010000	02651210	0100000	0260000
7	00010000	02661210	0010000	0260000
8	00001000	02671210	1000000	0267000
9	00001000	02672210	0100000	0267000
10	00001000	02673210	0010000	0267000
11	00000100	02673210	1000000	0236700
12	00000100	02673310	0100000	0236700
13	00000100	02673410	0010000	0236700
14	00000100	02673510	0001000	0236700
15	00000010	02673510	1000000	0235670
16	00000010	02673520	0100000	0235670
17	00000010	02673530	0010000	0235670
18	00000010	02673540	0001000	0235670
19	00000001	02673540	1000000	0234567
20	00000001	02673541	0100000	0234567
21	10000000	02673541	1000000	0123456

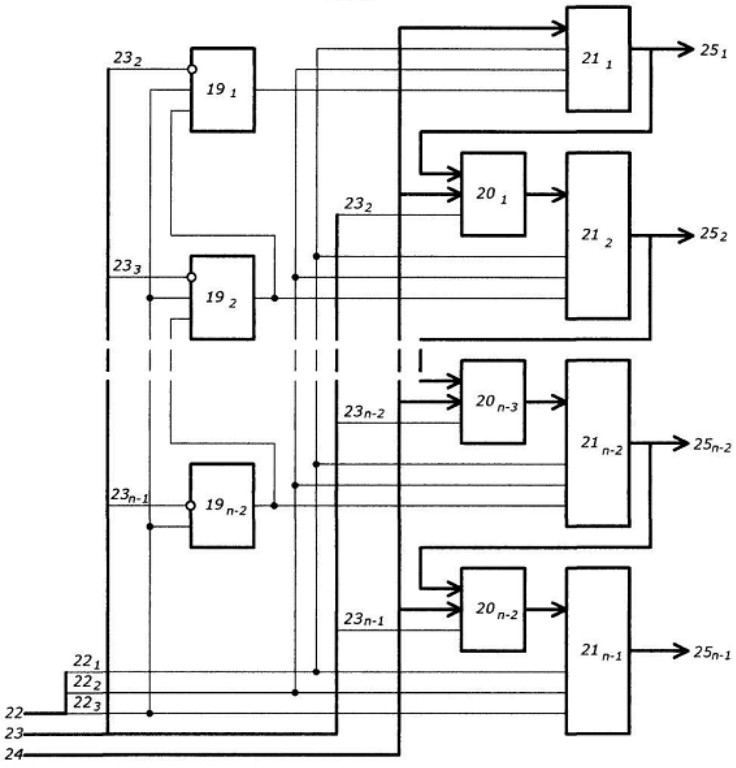
Таким чином, введення нових конструктивних ознак дозволяє підвищити швидкодію пристрою і знизити апаратурні витрати. Крім того, існує можливість зміни послідовності перебору перестановок шляхом побудови спеціалізованого факторіального лічильника.



Фіг. 1



Фіг. 2



Фіг. 3

Комп'ютерна верстка А. Рябко Підписне Тираж 24 прим.

Міністерство освіти і науки України
Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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