Напрям конкурсу: Інформаційна безпека

Тема: "Система формування факторіальних чисел"

Девіз: "Девіація"

2011 рік

ЗМІСТ

1 ПОСТАНОВКА ЗАДАЧІ

На практиці при вирішенні завдання захисту даних від несанкціонованого доступу широко використовуються перестановки. Так, наприклад, блоки керованих і фіксованих перестановок використовуються в різних блокових шифрах для виконання бітових перестановок, що залежать від перетворюваних даних [1]. При цьому забезпечується висока швидкість шифрування за рахунок досить високої швидкодії операцій з перестановками. Також перестановка рядків є одним з найбільш прийнятних способів захисту відеозображень. Далі, статичні і змінні перестановки смуг і відрізків мовного сигналу можуть ефективно використовуватися для захисту мовної інформації в каналах зв'язку [1 – 3]. Завдання зворотного перетворення актуальне при необхідності нумерації перестановок і відновлення початкових даних після передачі [1, 3]. Перетворення степеневих чисел у факторіальни є проміжним кроком при генерації перестановок. Перестановки на основі факторіальних чисел отримують відповідно до алгоритму, розглянутого в [1]:

Цифра старшого розряду факторіального числа залишається без змін і вважається за перший елемент перестановки, що будується. Наступну цифру порівнюють з першим елементом перестановки, якщо вона більше його, то необхідно збільшити дану цифру на 1, інакше вона без змін записується як другий елемент перестановки. Цифри наступних розрядів порівнюють спочатку з найменшим елементом перестановки, що будується. Якщо значення цифри при цьому більше значення даного елементу, то необхідно збільшити її на 1 і порівнювати з найменшим з елементів перестановки, що залишилися, і якщо значення цифри більше його, то вона збільшується на 1. Порівняння проводиться до тих пір, поки значення цифри не стане менше того значення елементу перестановки, що будується, з яким дана цифра порівнюється, або ж поки не буде проведено порівняння зі всіма елементами. Таким чином,

виходить черговий елемент перестановки.

Для зворотного переходу від перестановки до факторіального числа необхідно кожен елемент перестановки зменшити на число одиниць, рівне кількості попередніх елементів перестановки, менших за даний елемент. В результаті всі елементи перестановки будуть перетворені в цифри факторіального числа.

Як випливає з наведеного вище алгоритму, для отримання перестановок потрібні факторіальні числа, які, у свою чергу, отримують шляхом перетворення степеневих чисел.

Під факторіальною системою числення розуміється вираз вигляду:

$$F_{<\phi>} = X_n \cdot n! + X_{n-1} \cdot (n-1)! + ... + X_i \cdot i! + ... + X_1 \cdot 1! + X_0 \cdot 0!, \qquad (1.1)$$

де i = 0, 1, …, $0 \geq X_l \geq l$

Факторіальна система числення відноситься до систем числення із змішаною основою. Максимальне число Fmax у факторіальній системі має вигляд n (n–1) … l … 2 1 0 Мінімальне число 00…0…00 Fmin = 0. Діапазон факторіальних чисел враховує нуль, тому визначається як:

$$P = Fmax + 1. \qquad (1.2)$$

Для вирішення завдання перетворення двійкових чисел у факторіальних використовується алгоритм, розроблений в [1]. Проте даний алгоритм має недолік – складність його технічної реалізації. Тому в даній роботі ставляться наступні завдання:

1) знайти простий алгоритм формування факторіальних чисел;

2) розробити структуру пристрою, що реалізує запропонований алгоритм.

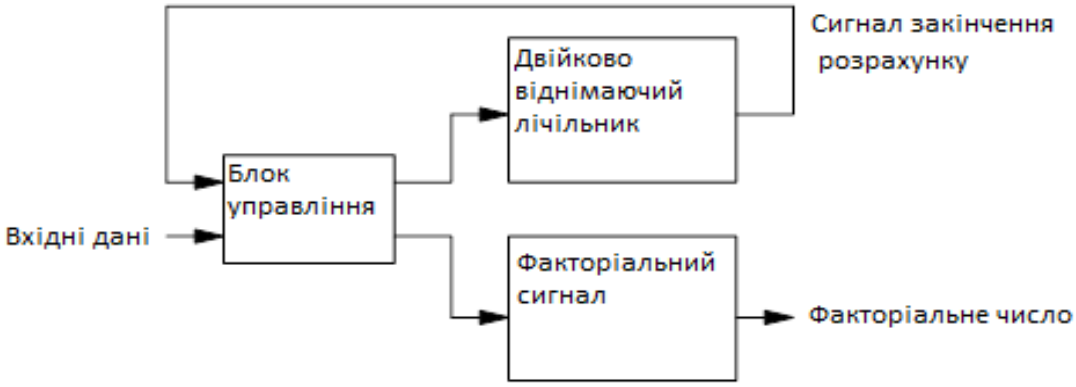
2 РОЗРОБКА СИСТЕМИ ФОРМУВАННЯ ФАКТОРІАЛЬНИХ ЧИСЕЛ

Запропонований в роботі метод перетворення двійкових і факторіальних чисел полягає в організації одночасного розрахунку у напрямі зменшення чисел, починаючи з початкового, і зростання чисел, до числа, яке необхідно отримати. Найбільш простим і ефективним способом реалізації цього алгоритму є використання лічильників – підсумовуючого і віднімаючого.

При перетворенні двійкового числа у факторіальне на віднімаючий двійковий лічильник подається початкова двійкова комбінація. Особливістю лічильника, що підсумовує, є те, що перерахунок ведеться у факторіальній системі числення. Таким чином, одночасно подаючи розрахунковий сигнал на обидва лічильники, ми збільшуємо на одиницю значення числа у факторіальному лічильнику і зменшуємо в двійковому. Для повного перетворення числа буде потрібна кількість розрахункових імпульсів, рівна величині перетворюваного числа. Перевагою даного методу є простота його реалізації, що компенсує зниження його швидкодії.

Схема, що реалізовує даний алгоритм, зображена на (мал. 2.1). У її склад входять: блок управління, двійковий віднімаючий лічильник, факторіальний підсумовуючий лічильник. Вхідні дані є початковим двійковим числом, а також різними керуючими сигналами. За допомогою блоку управління здійснюється контроль за процесом перетворення. На початку циклу перетворення початкове двійкове число подається з блоку управління на двійковий віднімаючий лічильник. Факторіальний лічильник при цьому встановлюється в нуль. Тактові імпульси, що подаються одночасно на входи двійкового і факторіального лічильників, зменшують двійкове число, записане в двійковому віднімаючому лічильнику і збільшують число у факторіальному лічильнику. При досягненні нульової комбінації в двійковому віднімаючому лічильнику формується сигнал закінчення рахунку, що забороняє через блок управління подачу тактових

імпульсів до початку наступного циклу. Далі факторіальне число, записане у факторіальному лічильнику, передається на вихід пристрою.

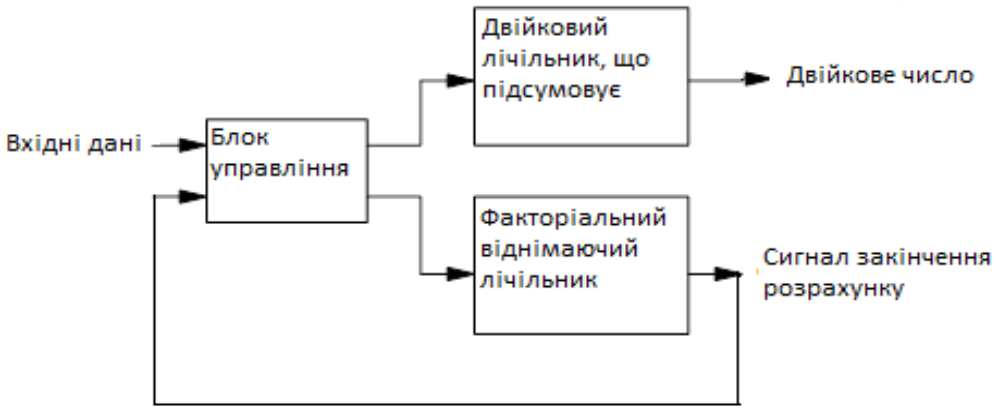


Малюнок 2.1 – Система перетворення двійкових чисел у факторіальні числа

Зворотне перетворення здійснюється по схожій схемі, але в цьому випадку використовується двійковий лічильник, що підсумовує, і факторіальний віднімаючий лічильник (мал. 2.2). Початкові дані, що є факторіальним числом, записуються у факторіальний віднімаючий лічильник. Розряди двійкового лічильника в початковому стані містять нулі. Розрахунковими імпульсами зменшується число у факторіальному лічильнику і збільшується в двійковому. Нульова комбінація у факторіальному лічильнику свідчить про закінчення розрахунку, далі відбувається прочитування двійкової комбінації з виходу двійкового лічильника.

При необхідності здійснювати, як пряме перетворення двійкових чисел у факторіальних, так і зворотне – факторіальних чисел в двійкові, може використовуватися схема з двома реверсивними лічильниками (мал. 2.3). Двійковий і факторіальний лічильники в цьому випадку можуть вести перерахунок, як в режимі, що підсумовує, так і в тому, що віднімає. За вибір

режиму роботи схеми і коректну її роботу у вибраному режимі відповідає блок управління на підставі отримуваних вхідних даних.



Малюнок 2.2 – Система перетворення факторіальних чисел в двійкові числа

Малюнок 2.3 – Система, що здійснює перехід між двійковими і факторіальними числами

Структурна схема блоку управління даної системи представлена на (мал. 2.4). У неї входять: блок зчитування вхідних даних, блок, що відповідає за зберігання факторіальних і двійкових чисел, блок управління напрямом рахунку, блок виведення даних. Блок зчитування вхідних даних призначений для прийому і подальшої передачі в інші блоки пристрою даних про напрям

перетворення чисел (двійкові числа перетворюються у факторіальних або навпаки), перетворювані числа (початкова комбінація двійкового або факторіального числа залежно від напряму рахунку), сигнали синхронізації з передавальним і приймаючим пристроями. Блок зберігання здійснює прийом початкової комбінації від блоку зчитування і зберігає її до початку циклу перетворення. Після зчитування всіх вхідних даних початкова комбінація передається з блоку зберігання в лічильник, що працює у віднімаючому режимі. Блок управління напрямом розрахунку на основі інформації, що отримується від блоку зчитування, встановлює двійковий і факторіальний лічильники в необхідний режим рахунку. Блок виведення даних отримує сигнал про закінчення рахунку від лічильника, що працює у віднімаючому режимі, після чого забезпечує виведення вихідної комбінації з лічильника, що працює в режимі, що підсумовує.

Малюнок 2.4 - Структура блоку управління системи переходу між двійковими і факторіальними числами

Дана схема може використовуватися і в системах, що здійснюють тільки один вид перетворення двійкових і факторіальних чисел. Проте в цьому випадку відпадає необхідність в блоці управління напрямом рахунку.

3 СТРУКТУРА І РОБОТА ФАКТОРІАЛЬНОГО ЛІЧІЛЬНИКА

Для вирішення завдання генерації факторіальних чисел необхідно на основі двійкових лічильників спроектувати факторіальний лічильник, що працює відповідно до наступного алгоритму.

1. У всі двійкові лічильники, що відповідають за розряди факторіального лічильника, записуються нулі.

2. Оскільки нульовий розряд факторіального числа завжди приймає нульове значення, він не бере участь в перерахунку. У двійковий лічильник, що відповідає за перший розряд факторіального лічильника, записується одиниця.

3. Додавання одиниці в лічильник першого розряду, що працює в двійковому коді, скидає його в нуль, одиниця переноситься в лічильник, що відповідає за другий розряд факторіального лічильника, що працює в трійковому коді.

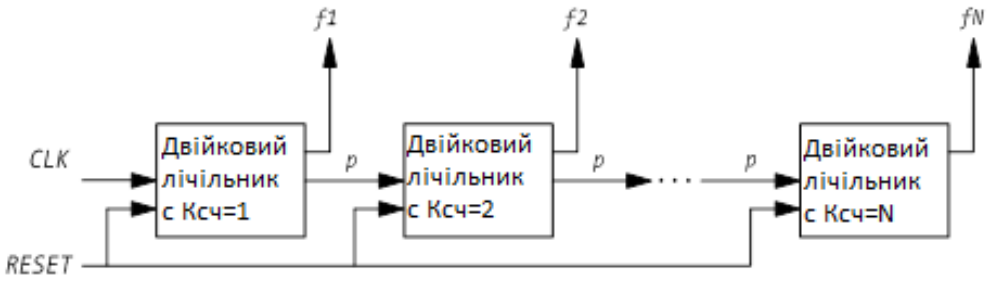
4. Пункти 2 і 3 повторюються до тих пір, поки не відбудеться переповнювання двійкового лічильника другого розряду. Далі одиниця переноситься в лічильник третього розряду, максимальне значення цифри в якому рівне трьом.

5. Збільшення числа на одиницю проводиться до тих пір, поки всі двійкові лічильники розрядів факторіального лічильника не заповняться максимально можливими значеннями. При цьому кожен наступний двійковий лічильник працює з коефіцієнтом перерахунку на одиницю більшим, ніж попередній.

Згідно [4], факторіальним лічильником є послідовність сполучених між собою двійкових лічильників, коефіцієнт перерахунку яких зростає на одиницю для кожного подальшого лічильника від 1 до N, де N – величина максимального розряду факторіального числа. Для побудови факторіального лічильника, що підсумовує, можуть використовуватися методи, що розглядаються у наступному розділі. Відмінність віднімаючого факторіального лічильника від

того, що підсумовує полягає в інвертуванні сигналів між елементами лічильників розрядів. В даному випадку для побудови лічильників розрядів факторіального лічильника переважно використовувати метод передустановки, оскільки лічильники розряду при переході з нульового стану в перше необхідно встановлювати в максимальне значення даного розряду факторіального числа. При використанні реверсивних лічильників розрядів, що дозволяють вести як прямій, так і зворотний рахунок, необхідно комбінувати методи управління скиданням лічильника, модифікації міжрозрядних зв'язків лічильника і передустановки.

Приклад побудови факторіального лічильника показаний на (мал. 3.1). Сигнали f1, f2, fN позначають значення цифр розрядів факторіального числа, p – сигнал перенесення. Нульовий розряд факторіального числа завжди приймає значення «0», тому не бере участь в перерахунку.



Малюнок 3.1 – Структурна схема N-розрядного факторіального лічильника.

4 ЛІЧИЛЬНИКИ З ДОВІЛЬНИМ КОЕФІЦІЄНТОМ ПЕРЕРАХУНКУ

Лічильники з коефіцієнтом перерахунку, рівними $2m$ будуються за допомогою послідовного з'єднання Т-триггеров, що міняють свій стан на протилежний під час отримання імпульсів на вхід синхронізації. Для реалізації Т-триггера може бути використаний універсальний D-триггер із зворотним зв'язком або JK-триггер. Для побудови лічильників з коефіцієнтом перерахунку, відмінним від $2m$ може використовуватися один з наступних методів: метод управління скиданням лічильника, метод модифікації міжрозрядних зв'язків лічильника, метод передустановки, метод використання лічильників з Ксч = $2n + 1$.

4.1Метод управління скиданням лічильника [5, 6]

Один з принципів побудови лічильників з коефіцієнтом розрахунку, відмінним від $2m$, полягає у виключенні декількох станів звичайного двійкового лічильника, що є надмірними для лічильника, який треба побудувати. При цьому надмірні стани виключаються за допомогою зворотних зв'язків усередині лічильника. Число надмірних станів для будь-якого лічильника визначається з наступного виразу:

$$M = 2^m - K_{СЧ} \qquad (4.1.1)$$

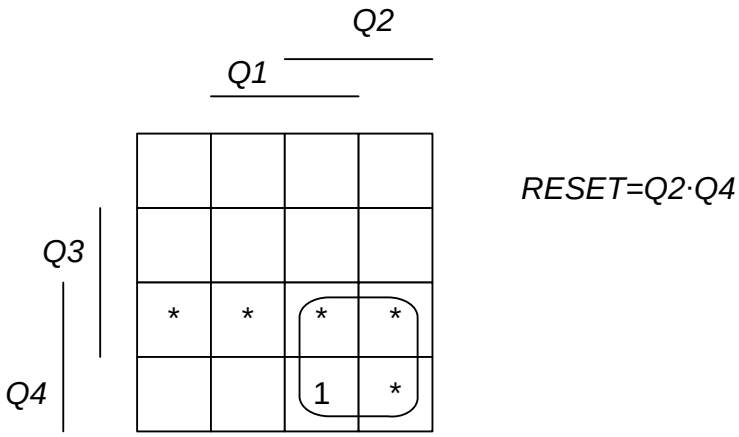
де M – число заборонених станів, Ксч – необхідний коефіцієнт рахунку, 2^m – число стійких станів двійкового лічильника.

Завдання синтезу такого лічильника полягає у визначенні необхідних зворотних зв'язків і мінімізації їх числа. Необхідна кількість трігерів

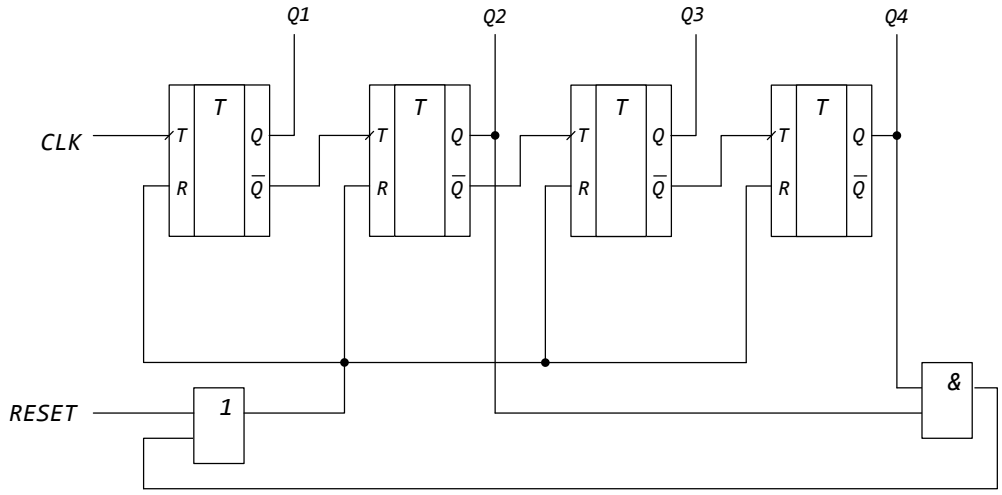
визначається з виразу:

$$n = \lceil \log_2 K_{СЧ} \rceil \qquad (4.1.2)$$

Розглянемо приклад реалізації лічильника з Ксч=10 даним методом. Очевидно, що скидаючи двійковий чотирирозрядний лічильник в нуль кожного разу, коли він прийматиме стан 1010, можна забезпечити повернення лічильника в початковий стан після кожних десяти імпульсів. Мінімізація зворотних зв'язків проводиться, враховуючи невживані стани лічильника (мал. 4.1.1). Схема лічильника зображена на (мал. 4.1.2). Подібний прийом зручно застосовувати при використанні лічильників в інтегрального виконання, що мають осередки кон'юнкції (І) на входах установки в нуль.



Малюнок 4.1.1 – Мінімізація зворотних зв'язків лічильника



Малюнок 4.1.2 – Приклад реалізації лічильника з Ксч = 10

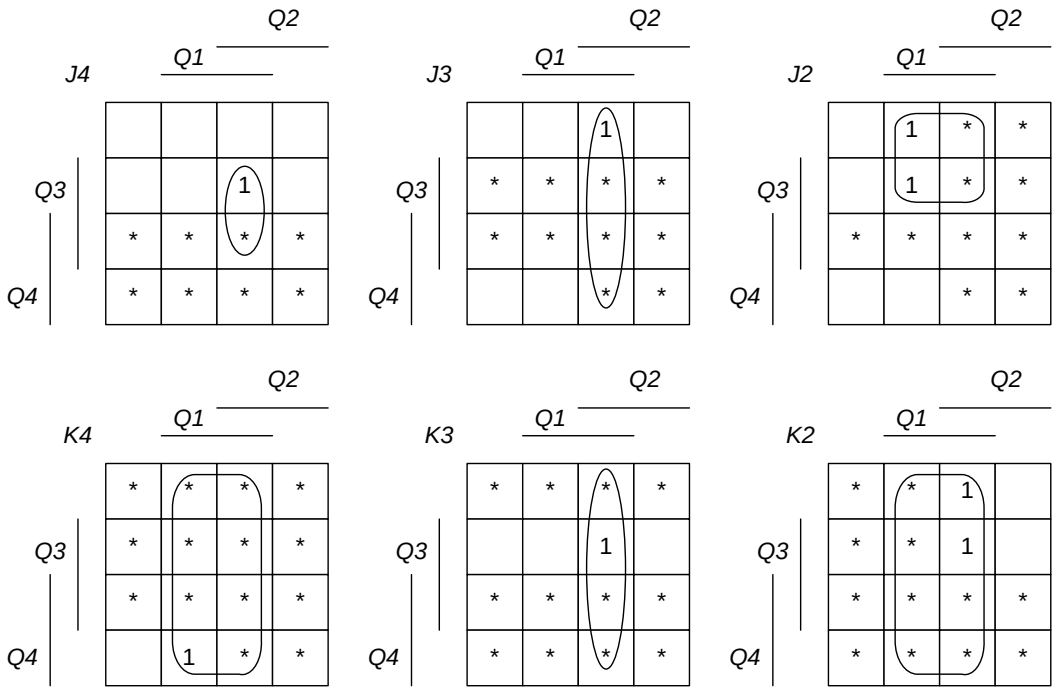
4.2 Метод модифікації міжрозрядних зв'язків лічильника [5, 6]

Один з методів проектування лічильників із заданим коефіцієнтом перерахунку полягає у виключенні невживаних станів лічильника з його таблиці переходів. У перших стовпцях даної таблиці відображенті поточні стани трігерів лічильника, а в подальших – наступні за ними стани. Аналіз таблиці дозволяє встановити ті переходи, які мають бути здійснені трігерами, що входять до складу лічильника. Потім за допомогою таблиці відповідного керуючого трігера, знаходяться значення логічних функцій на входах керуючих трігерів, що дозволяють здійснити ці переходи.

Таблиця 4.2.1 є прикладом таблиці переходів для побудови лічильника з коефіцієнтом перерахунку, рівним 10. На (мал. 4.2.1) приведені карти Карно для логічних функцій, яким повинні відповідати сигнали, присутні на входах керуючих трігерів (нульові значення функцій в клітки карти Карно не записані).

Таблиця 4.2.1 – таблиця переходів станів трігерів для лічильника з Ксч = 10

N	T				t+1				j4	k4	j3	k3	j2	k2	j1	k1
	Q4	Q3	Q2	Q1	Q4	Q3	Q2	Q1								
0	0	0	0	0	0	0	0	1	0	*	0	*	0	*	1	*
1	0	0	0	1	0	0	1	0	0	*	0	*	1	*	*	1
2	0	0	1	0	0	0	1	1	0	*	0	*	*	0	1	*
3	0	0	1	1	0	1	0	0	0	*	1	*	*	1	*	1
4	0	1	0	0	0	1	0	1	0	*	*	0	0	*	1	*
5	0	1	0	1	0	1	1	0	0	*	*	0	1	*	*	1
6	0	1	1	0	0	1	1	1	0	*	*	0	*	0	1	*
7	0	1	1	1	1	0	0	0	1	*	*	1	*	1	*	1
8	1	0	0	0	1	0	0	1	*	0	0	*	0	*	1	*
9	1	0	0	1	0	0	0	0	*	1	0	*	0	*	*	1



Малюнок 4.2.1– Карти Карно для логічних функцій лічильника з Ксч = 10

Після спрощення за допомогою карт Карно отримані логічні вирази, використовувані для управління входами “J” і “K”, виглядають

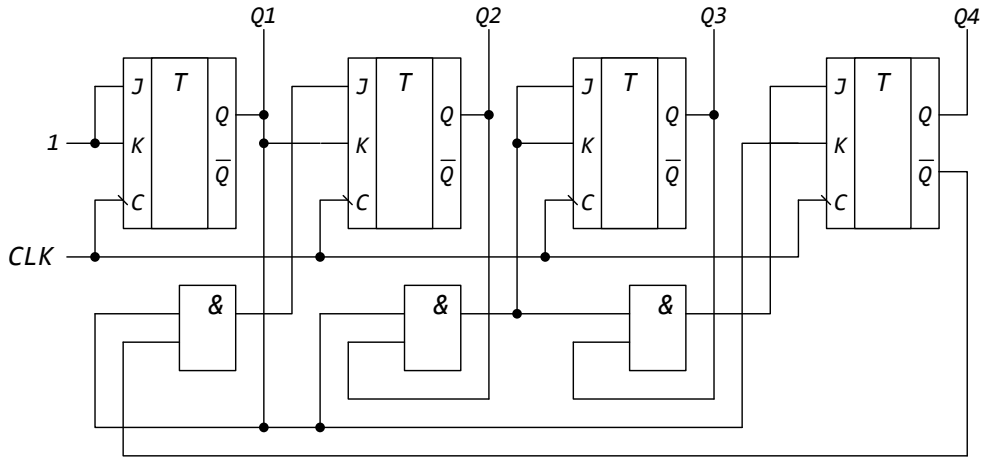
$$J_4 = Q_1 \cdot Q_2 \cdot Q_3; \qquad K_4 = Q_1;$$

$$J_3 = Q_1 \cdot Q_2; \qquad K_3 = Q_1 \cdot Q_2;$$

$$J_2 = Q_1 \cdot \overline{Q_4}; \qquad K_2 = Q_1.$$

Проглядання стовпців J1 і K1 в таблиці 1 показує, що всіх значень, що набувають, або «*», або «1». Оскільки стани, що не використовуються, можуть також брати участь в процесі спрощення, то всі клітки карти Карно для J1 і K1 виявляються заповненими символами «1» і «*». Отже J1 = K1 = 1.

На (мал. 4.2.2) показана схема синхронного лічильника з Ксч = 10.



Малюнок 4.2.2 – Схема реалізації синхронного лічильника з коефіцієнтом перерахунку Ксч = 10

Перевагою данного методу є можливість побудови лічильників з будь-якою розрахунковою послідовністю, недолік методу – ускладнення процессу мінімізації при збільшенні розрядності лічильника.

Якщо лічильник через яку-небудь несправність опиниться в одному з заборонених (невживаних) станів, то його робота може бути перервана

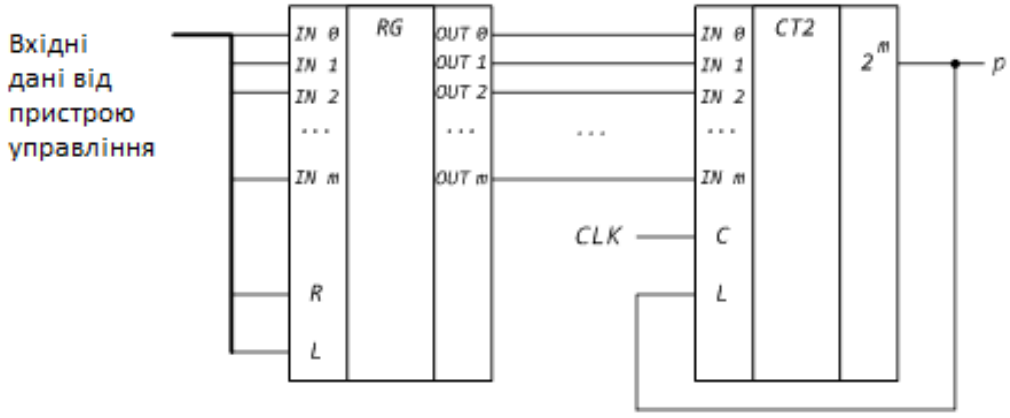
спеціальним сигналом і також може бути поданий сигнал про несправність в схемі лічильника. Виявити це дозволяє схема, що реалізовує вираз, що описує функцію невживаних станів.

4.3 Метод передустановки [6]

Даний метод побудови лічильників з коефіцієнтом рахунку, відмінним від 2m, полягає у використанні лічильників з передустановкою (малюнок 4.3.1). Суть методу полягає в тому, що двійковий лічильник заздалегідь встановлюється в початковий стан, відмінний від нульового. Номер початкової двійкової комбінації визначається з виразу:

$$N_0 = 2^m - K_{СЧ}, \qquad (4.3.1)$$

де N_0 – номер початкової комбінації, Ксч – необхідний коефіцієнт перерахунку, 2m – число станів двійкового лічильника.



Малюнок 4.3.1 – Схема реалізації лічильника з передустановкою

Установка лічильника здійснюється за допомогою запису даних з елементу

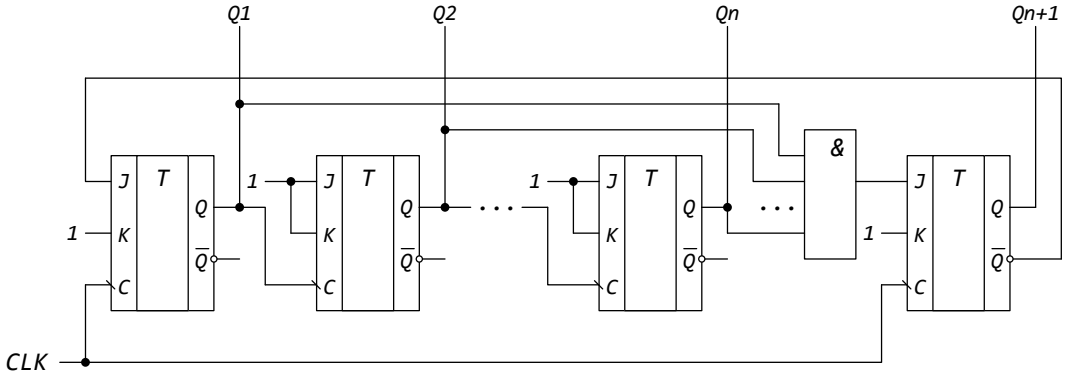
пам'яті, який отримує їх від пристрою управління лічильником. Спочатку кожного циклу перерахунку початкова комбінація прочитується з елементу пам'яті і записується в двійковий лічильник. Під час переходу лічильника в нульовий стан, сигнал переповнювання лічильника *p* подається на вхід дозволу запису *L* і забезпечує запис початкової комбінації в лічильник.

Для побудови двійкових лічильників з природним порядком рахунку (від 0 до Ксч) на основі даного методу, необхідно виходи лічильника завести на входи перетворювача коду, що здійснює визначення номера поточної комбінації в лічильнику.

Перевагою методу є можливість настроювати лічильник на різні коефіцієнти перерахунку за допомогою запису різних початкових двійкових комбінацій в елемент пам'яті. Недолік полягає в необхідності використання додаткових мікросхем для реалізації запам'ятовуючого пристрою.

4.4Метод використання лічильників з Ксч = 2n + 1 [7]

У основі даного методу лежить використання лічильників, з коефіцієнтом перерахунку на одиницю більшим за ступінь двійки (мал. 4.4.1). Збільшення коефіцієнта перерахунку на одиницю досягається використанням додаткового (одиничного) JK-тригера. Даний тригер на відміну від інших тригерів лічильника, що працюють в рахунковому режимі, об'єднує по своєму J-входу виходи попередніх тригерів. На вхід K одиничного тригера подається 1, на вхід C, як і на аналогічний вхід тригера молодшого розряду лічильника, подається тактуючий імпульс CLK. Виходи Q всіх двійкових розрядів лічильника підключаються через логічний елемент I до входу J одиничного тригера, інверсний вихід одиничного тригера підключається до входу триггера молодшого розряду лічильника.



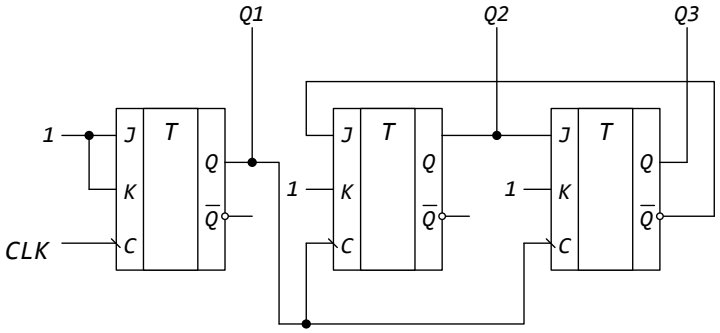
Малюнок 4.4.1 – Схема лічильника з коефіцієнтом перерахунку 2n + 1

Початковим станом для лічильника є нульовий. Інверсний сигнал з виходу одиничного тригера забезпечує рахунковий режим роботи тригера молодшого розряду. Після того, як всі рахункові тригери встановляться в одиничний стан, сигнали з їх виходів забезпечать перемикання одиничного тригера в 1 і лічильник перейде в 2n + 1 стан. При цьому запис 1 в тригер молодшого розряду забороняється сигналом з інверсного виходу одиничного тригера. Наступний тактуючий імпульс встановить лічильник в початковий стан.

При подачі на тактуючий вхід розглянутого вище лічильника сигналу з виходу звичайного двійкового лічильника з Ксч = 2n можна отримати лічильник, коефіцієнт перерахунку якого визначається як Ксч = 2n · (2n + 1).

Приклад лічильника для n = 1 представлений на (мал. 4.4.2). Для нього коефіцієнт перерахунку Ксч = 21 · (21 + 1) = 6.

Перевагою використання лічильників з Ксч = 2n + 1 є простіша у ряді випадків структура лічильників через відсутність логічних елементів, що забезпечують зворотні зв'язки. Недолік методу полягає в неможливості використання для побудови лічильників з Ксч Е 2n · (2n + 1).



Малюнок 4.4.2 – Схема лічильника з коефіцієнтом перерахунку 6, побудованого по схемі об'єднання лічильників з Ксч = 2n і Ксч = 2n + 1

5 ОЦІНКА ПАРАМЕТРІВ ПЕРЕТВОРЮВАЧА

Розглянемо вимоги, що висуваються до лічильників залежно від максимальної розрядності перетворюваного числа.

Для представлення k-того розряду факторіального числа потрібний двійкових розрядів, отже, для k-розрядного факторіального числа потрібна наступна кількість розрядів факторіального лічильника:

$$K_{Ф} = \sum_{i=1}^{k} \lceil \log_2 (k+1) \rceil \qquad (5.1)$$

Величина десяткового числа, відповідного k-розрядному факторіальному числу, визначатиметься відповідно формулі (1.1):

$$D = \sum_{i=1}^{k} (X_k \cdot k!) \qquad (5.2)$$

де Xk – значення k-того розряду факторіального числа.

Звідси, число розрядів двійкового числа (і, відповідно, необхідна розрядність двійкового лічильника) визначається таким чином:

$$K_{Д} = \lceil \log_2 D \rceil = \left\lceil \log_2 \left(\sum_{i=1}^{k} (X_k \cdot k!) \right) \right\rceil \qquad (5.3)$$

Приклад. Визначити розрядність двійкового і факторіального лічильників, потрібну для отримання п'ятирозрядних факторіальних чисел.

Рішення. Максимальне п'ятирозрядне факторіальне число в десятковій формі запису має наступний вигляд: F=43210. Для запису даного числа в

двійковому вигляді буде потрібно наступну кількість розрядів (5.1):

$$K_{\Phi} = \left|\log_2(4+1)\right| + \left|\log_2(3+1)\right| + \left|\log_2(2+1)\right| + \left|\log_2(1+1)\right| + \left|\log_2(0+1)\right| = 9.$$

Величина десяткового числа D, відповідного числу F (5.2):

$$D = 4 \cdot 4! + 3 \cdot 3! + 2 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 119.$$

Число розрядів двійкового лічильника (5.3) $K_{Д} = \lceil \log_2 119 \rceil = 5$.

Час перетворення числа не залежить від способу перетворення (двійкове у факторіальне або навпаки), а визначається виключно кількістю рахункових імпульсів, тобто величиной числа D, а також частотою роботи системи f:

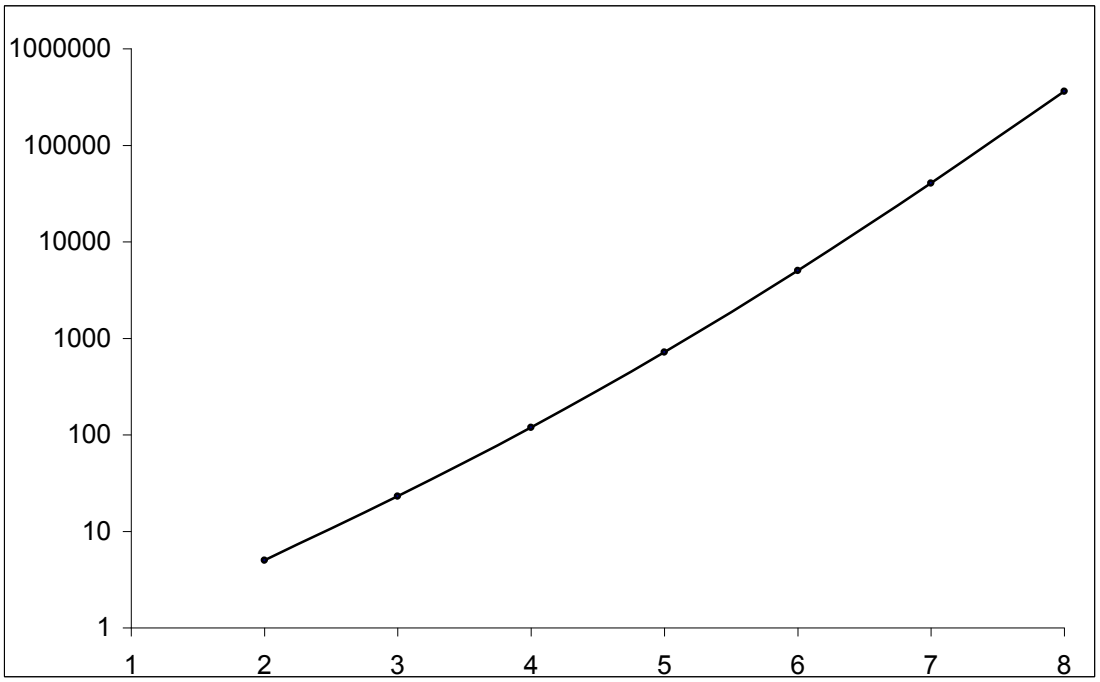
$$T_P = D / f = \sum_{i=1}^{k} (X_k \cdot k!) / f \qquad (5.4)$$

Розглянемо дану залежність при фіксованій частоті роботи системи, досліджуючи тільки число циклів її роботи. Визначимо максимальний час перетворення залежно від розрядності факторіального числа. У таблиці 5.1 показані максимальні значення параметра D для розрядності факторіального числа Чр.

Таблиця 5.1

Чр	2	3	4	5	6	7	8
D	5	23	119	719	5039	40319	362879

Графічно дана залежність показана на (мал. 5.1). Аналізуючи графік залежності можна зробити вивід, що при збільшенні розрядності факторіального числа залежність наближається до експоненціальної.



Малюнок 5.1 – Залежність максимального часу роботи системи від розрядності перетворюваного числа при фіксованій частоті роботи системи

Залежність середнього часу перетворення числа від розрядності факторіального числа представлена в таблиці 5.1 і на (мал. 5.2). Дану величину можна оцінити, провівши дослідження на деякому вибраному інтервалі, або скориставшись наступною формулою:

$$D_{k\,cp} = (D_k + 1)/2 \qquad (5.5)$$

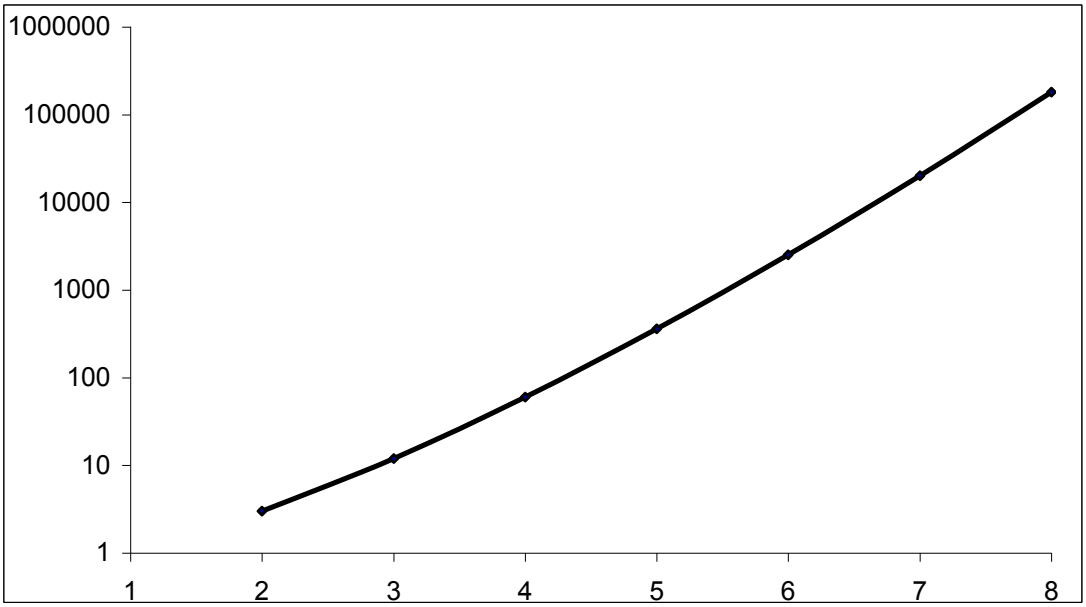
де k – розрядність факторіального числа;

Dk – максимальний час роботи системи для розрядності числа k.

Таблиця 5.2.

Чр	2	3	4	5	6	7	8
Dср п	3	12	60	360	2520	20160	181440
Dср т	3	14	57,3	349,5	2551,6	20119,7	181279,7

У таблиці 2 Dср т – середній час перетворення, отриманий по формулі (5.5), Dср п – середній час перетворення, отриманий на основі практичного дослідження. Збіг результатів практичного дослідження і розрахункових даних свідчить про відсутність помилок при визначенні величини.



Малюнок 5.2 – Залежність середнього часу роботи системи від розрядності перетворюваного числа при фіксованій частоті роботи системи

ВИСНОВКИ

Для вирішення поставленого завдання формування і перебору факторіальних чисел використовувався метод, що передбачає використання двох лічильників: підсумовуючого факторіального і віднімаючого двійкового. Основною перевагою цього методу є простота його реалізації, а також можливість збільшення діапазону перетворюваних чисел шляхом додавання додаткових структурних елементів факторіального лічильника і збільшення коефіцієнта перерахунку двійкового лічильника. Даний метод може ефективно використовуватися в пристроях, призначених для захисту даних від несанкціонованого доступу, що вимагають підвищену надійність і не пред'являють високих вимог до швидкодії.

СПИСОК ЛІТЕРАТУРИ

1. Борисенко а.А., Кулик і.А., Горячев а.Е. Електронна система генерації перестановок на базі факторіальних чисел. Вісник СумДУ. Технічні науки. – 2007. – №1. – с.183 – 188.

2. Рейнгольд Э., Нівергельт Ю., Део Н. Комбінаторниє алгоритми: теорія і практика. – М.: Вид-во "Мир", 1980. – 477 с.

3. Borisenko A.A., Kalashnikov V.V., Kulik I.A., Goryachev A.E. Generation of Permutations Based Upon Factorial Numbers. Eighth International Conference on Intelligent Systems Design and Applications. Kaohiung, Taiwan, 2008. – p. 57 – 61.

4. Горячев А.Е. Построение факториальных чисел на основе двоичных счётчиков. Вісник СумДУ. Технічні науки. – 2008. – №4.

5. Угрюмов Е.П. Цифровая схемотехника. – СПб.: БХВ-Петербург. 2004. – 528с.: ил.

6. Зубчук В.И., Сигорский В.П., Шкуро А.Н. Справочник по цифровой схемотехнике. – К.: Техника. 1990. – 448с.

7. Букреев И.Н., Горячев В.И., Мансуров Б.М. Микроэлектронные схемы цифровых устройств. – 3-е изд., перераб. и доп. – М.: Радио и связь. 1990. – 416с.: ил.