

МЕТОД ФОРМУВАННЯ ТА ОПРАЦЮВАННЯ СИГНАЛЬНИХ КОРЕКТУЮЧИХ КОДІВ У КОМП'ЮТЕРНИХ СИСТЕМАХ

© Воронич А.Р., 2012

Викладено метод формування та багатоканального передавання інформації з використанням сигнальних коректуючих кодів у базисі Галуа. Показано перспективу використання таких кодів для збільшення пропускної здатності каналу передачі в комп'ютерних системах. Крім цього, застосування спіральних властивостей сигнальних коректуючих кодів у базисі Галуа дає змогу підвищити коректуючі властивості сигнальних кодів у разі виникнення пакетів помилок.

Ключові слова: коректуючі сигнальні коди, базис Галуа.

Technology of multichannel information transmission is described with using corrective signal codes in Galois basis. It is shown perspective of use these codes to increase bandwidth transmission in computer systems. Besides using of spiral properties corrective signal codes in the Galois basis we can increase the corrective properties of signal codes when packet errors emergence

Key words: corrective signal codes, Galois basis.

Вступ

З розвитком сучасних технологій актуальною проблемою стала організація комп'ютерних мереж з удосконаленням багатоканальних способів передавання інформації. Застосування сигнальних коректуючих кодів (СКК) поля Галуа [1,2], які володіють рекурентними властивостями, дає змогу забезпечити високу завадостійкість методу формування і опрацювання маніпульованих сигналів. Можливість значного покращення характеристик систем передавання даних у сучасних комп'ютерних мережах потребує глибоких теоретичних та експериментальних досліджень СКК.

Аналіз публікацій і окреслення наукової задачі

Аналіз наукової літератури показує, що більшість сучасних досягнень в області завадозахищеності передавання даних із застосуванням коректуючих кодів ґрунтується на використанні кодів Хемінга [3–5].

Код Хемінга – це код з виправленням помилок, який забезпечує виявлення і виправлення всіх однорозрядних помилок у символі. Він найефективніший для символів з невеликою кількістю розрядів – наприклад, від 4 до 8 розрядів. У разі збільшення кількості розрядів у символі зростає імовірність пропустити багаторозрядну помилку, виявити яку код Хемінга неспроможний [4].

Коректуючу здатність коду Хемінга збільшують введенням перевірки на парність

У комп'ютерних системах використовують метод передавання, та приймання інформації на основі модифікованої частотної модуляції (Modified Frequency Modulation – MFM) [6], на основі чотирьох сигнальних ознак: фронт наростання(\otimes), фронт спаду(\oplus), які відповідають символу “1”, і потенціал “+”, потенціал “–”, які відповідають символу “0”. Якщо повторяється символ “0”, для бітової синхронізації також використовують фронт наростання(\otimes) чи спаду(\oplus). Проте цей метод не дає змоги виявляти та виправляти помилки в сигналах на фізичному рівні, а також ефективно використовувати сигнальний простір каналів зв'язку, який містить чотири сигнальних ознаки: фронт наростання та спаду, потенціали “+” та “–”.

У сучасних комп'ютерних мережах широко використовується код Боуза–Чоудхурі–Хоквінгема (БЧХ), в якому, з метою захисту від помилок, на передавальній стороні каналу зв'язку процесор обчислює контрольну суму коректуючого коду (KK_i) [6].

Прикладом застосування контрольної суми є контрольна послідовність, необхідна для виявлення помилок передачі в структурі фрейма стандартного протоколу HDLC (рис. 1).

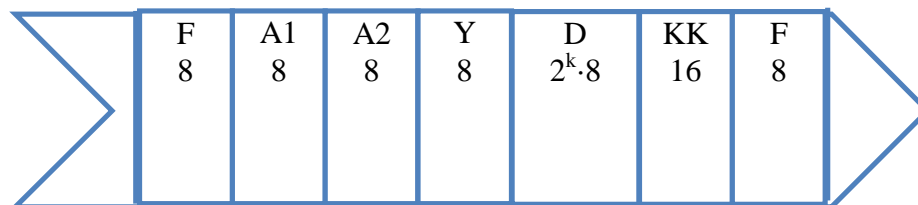


Рис. 1. Структура фрейма протоколу HDLC:

F – прапорець (байт 01111110); $A1$ – адреса передавальної станції;

$A2$ – адреса приймальної станції; Y – тип кадру; D – дані ($D=2^k \cdot 8$);

KK – коректуючий код БЧХ

БЧХ-код є циклічним кодом, який можна задати породжуючим незвідним поліномом. Щоб знайти його, в разі БЧХ-коду треба заздалегідь визначити довжину коду n (вона не може бути довільною) і необхідну мінімальну відстань $d \leq n$.

Алгоритм знаходження породжуючого полінома наведено в [5,7]. Як показано в [7], a – примітивний елемент поля $GF(q^m)$ (тобто $a^{q^m-1} = 1, a^i \neq 1, i < q^m - 1$). $b = a^s$ – елемент поля $GF(q^m)$ порядку $n, s = (q^m - 1) / n$

Тоді нормований поліном $g(x)$ мінімального степеня над полем $GF(q^m)$, коренями якого є $(d-1)$ степені $b^{l_0}, b^{l_0+1}, \dots, b^{l_0+d-2}$ елемента b , для деякого цілого l_0 , які йдуть підряд (зокрема 0 і 1), є породжуючим поліномом БЧХ-коду над полем $GF(q^m)$ з довжиною n і мінімальною відстанню $d_0 \geq d$.

У процесі виявлення та виправлення помилок знаходять контрольну суму (KK_i) інформаційного масиву даних (D_i), які передаються по лінії зв'язку. На приймальній стороні обчислюється контрольна сума бітів переданого масиву даних (KK'_i) і порівнюється з переданим кодом контрольної суми. Якщо контрольні суми, сформовані на передавальній та приймальній стороні лінії зв'язку ($KK_i = KK'_i$), збігаються, то по зворотній лінії зв'язку передається код квитанції KB^+ , що інформація передана правильно, і починається передача наступного інформаційного масиву даних (D_{i+1}). Якщо названі контрольні суми не збігаються ($KK_i \neq KK'_i$) на передавальну сторону лінії зв'язку по зворотному каналу передається код квитанції KB^- про наявність помилок в інформаційному масиві або в коді контрольної суми, що його супроводжувала, і повторно по лінії зв'язку передаються інформаційні дані (рис. 2).

Недоліком цього методу є можлива велика кількість повторних передавань інформаційних пакетів у разі зростання інтенсивності помилок внаслідок завад у лініях зв'язку, що знижує швидкодію передавання даних у комп'ютерних мережах і можливість виникнення помилок у самих контрольних сумах.

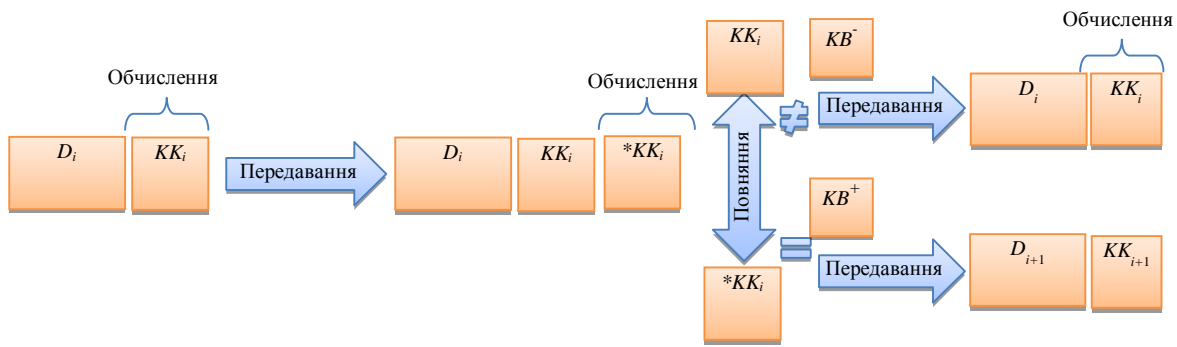


Рис. 2. Метод передавання даних з використанням контрольної суми (D_i – масив даних i -го потоку, KK_i , $*KK_i$ – контрольна сума, обчислена на передавальній і приймальній стороні i -го потоку відповідно, KB^+ , KB^- – код квитанції про відсутність чи наявність помилок у повідомленні, відповідно)

Мета роботи

Метою роботи є розроблення методу формування та опрацювання сигнальних коректуючих кодів у базисі Галуа та реалізація ефективних методів підвищення завадозахищеності та швидкості передавання інформаційних даних розподілених комп'ютеризованих систем та мереж.

Дослідження багатоканальної системи передавання даних з виправленням помилок на основі сигнальних коректуючих кодів у базисі Галуа. В основу дослідження покладено задачу підвищення швидкості передавання пакетів даних та захисту і корекції від помилок сигналів за допомогою мультिकанальної маніпуляції біт-орієнтованих потоків даних на фізичному рівні на основі рекурентних властивостей кодів поля Галуа [2].

Спочатку процесор обчислює контрольну суму коректуючого коду БЧХ (рис. 3), яка передається разом з інформаційним масивом по лінії зв'язку у вигляді пакета даних. Далі на передавальній стороні на фізичному рівні інформаційні біти “одиниць” пакета даних модулюються бітами послідовності коду поля Галуа з використанням першої і другої сигнальних ознак, а інформаційні біти “нулів” пакета даних використовуються для передавання наступного потоку даних шляхом модуляції його інформаційних бітів “одиниць” третьою і четвертою сигнальними ознаками, причому для нулів наступного потоку даних використовується п'ята сигнальна ознака. На приймальній стороні на фізичному рівні відбувається виявлення та виправлення помилок у сигналах, маніпульованих кодами поля Галуа. В результаті на приймальній стороні лінії у пакеті даних зменшується кількість можливих помилок і тим самим зменшується кількість повторних передач, а також підвищується швидкість передавання інформації більше ніж в півтора раза за рахунок багатоканальності.

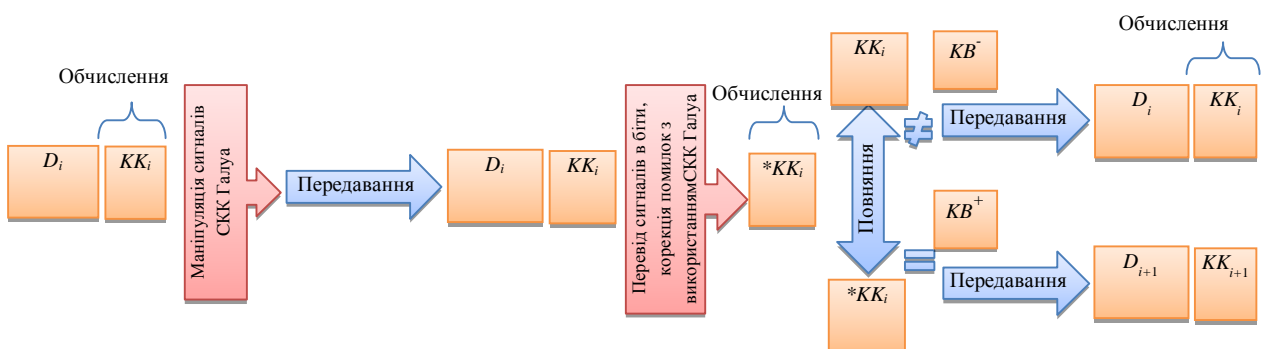


Рис. 3. Метод передавання даних з використанням СКК у базисі Галуа

Біти одиниць першого потоку в пакеті даних $D_1 + KK_1$ на передавальній стороні модулюються рекурентним кодом Галуа $G_2^{(k)}$. Причому для одиниць в пакеті даних біт Галуа “1”

передається фронтом наростання(\otimes), а біт Галуа “0” передається фронтом спаду(\oplus). На місці нулів першого потоку в пакеті даних вставляється другий потік у пакеті даних $D_2 + KK_2$, одиниці якого також нумеруються рекурентним кодом Галуа G_2^k . Причому в другому потоці пакета даних біт Галуа “1” передається потенціалом “+”, а біт Галуа “0” передається потенціалом “-”. Нулі другого пакета даних маніпулюються 5-ю ознакою – паузою сигналу: “0”

Методи формування та завадозахищеного передавання інформації у багатоканальній комп’ютерній мережі на основі СКК у базисі Галуа. Спочатку в пам’ять процесора передавальної сторони вноситься масив даних D_i . Далі відбувається обчислення контрольної суми коду БЧХ – KK_i . На передавальній стороні відбувається модуляція одиниць першого пакета даних $D_1 + KK_1$ за допомогою бітів сигнального коректуючого коду Галуа, причому біт Галуа “1” передається фронтом наростання(\otimes), а біт Галуа “0” передається фронтом спаду(\oplus), на місці нулів вставляються інформаційні сигнали другого пакета даних $D_2 + KK_2$, одиниці якого модулюються за допомогою бітів сигнального коректуючого коду Галуа, причому біт Галуа “1” передається потенціалом “+”, а біт Галуа “0” – потенціалом “-”. Нулі пакета даних $D_2 + KK_2$ модулюються іншою ознакою – паузою сигналу. Приклад промодульованого повідомлення зображено на рис. 3.

Приклад сигналу, маніпульованого за допомогою запропонованих сигнальних коректуючих кодів, за якого об’єм коду Галуа відповідає об’єму даних, наведено на рис. 4.

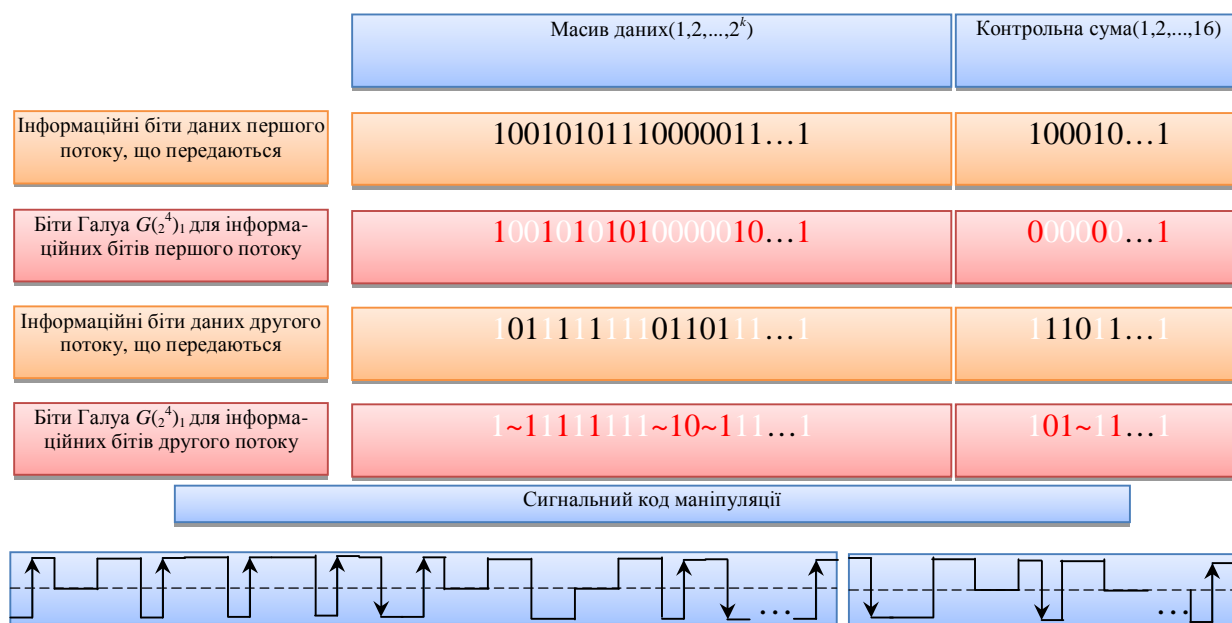


Рис. 4. Приклад промодульованого повідомлення для масиву даних і контрольної суми (~ – ознака паузи сигналу “0”)

Так забезпечується ефективно симетричне кодування потоку даних у вигляді кодів Галуа.

На приймальній стороні відбувається демодуляція біт-орієнтованого потоку даних з корекцією помилок завдяки рекурентним властивостям кодів поля Галуа.

На рис. 6 показано випадки, коли в першому потоці даних є тільки одиниці, тоді відбувається модуляція рекурентним кодом Галуа (де сигнальною ознакою є фронт наростання або фронт спаду). Або тільки нулі в першому і одиниці в другому, тоді відбувається модуляція рекурентним кодом Галуа (де сигнальною ознакою є рівень потенціалу “+” або “-”), причому в цьому випадку другий потік даних передається з максимальною швидкістю лінії зв’язку, тобто наявний ефект адаптивного завантаження лінії зв’язку.

Для СКК в базисі Галуа, які володіють рекурентними властивостями, можливе виправлення помилок на фізичному рівні. Реалізація потоку даних, маніпульованих за допомогою сигнальних коректуючих кодів, з виявленням та виправленням помилок зображена на рис. 5.

На рис. 6 наведено приклад виникнення помилок на сигнальному рівні в 7-й та 21-й позиції нулів, а також 10-й та 19-й позиції одиниць.

У запропонованому методі використано по дві ознаки маніпуляції для кодування двох різних потоків даних. При використанні 2^k+1 ознак маніпуляції на сигнальному рівні, наприклад, набори з різних фаз, частот, шумоподібних сигналів та їх комбінацій тощо, по лінії зв'язку може одночасно передаватися k інформаційних потоків даних з пропускнуою здатністю $1+0.5+0.25+0.125+\dots \text{ bit/c}$, відповідно (рис. 7).

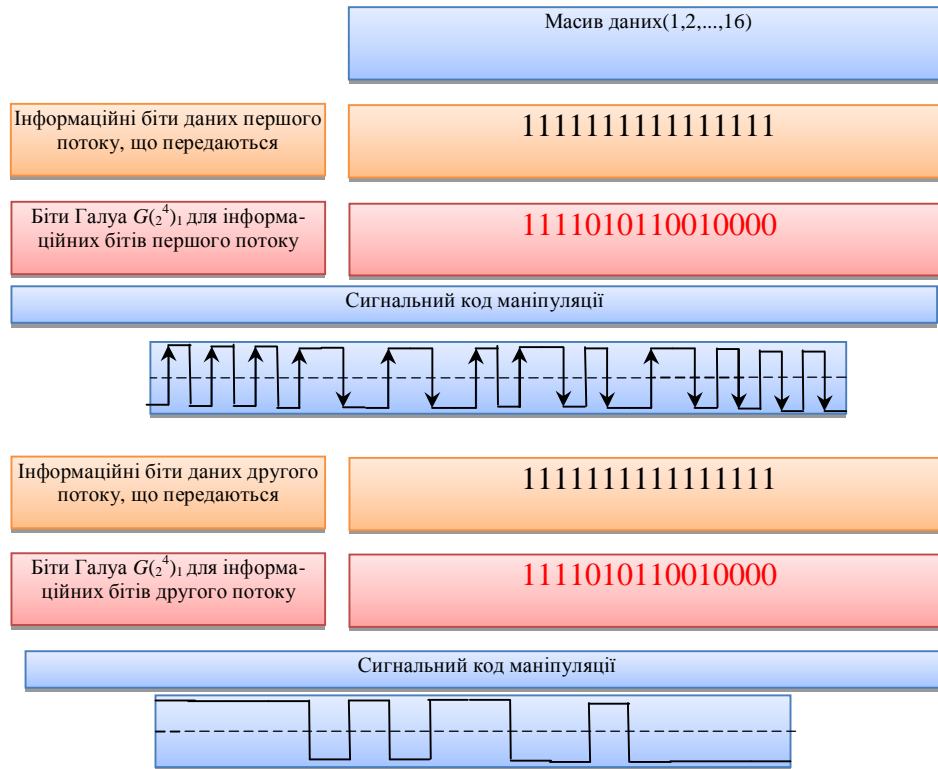


Рис. 5. Приклад повідомлення для масиву даних, коли в першому або другому потоці даних одні одиниці

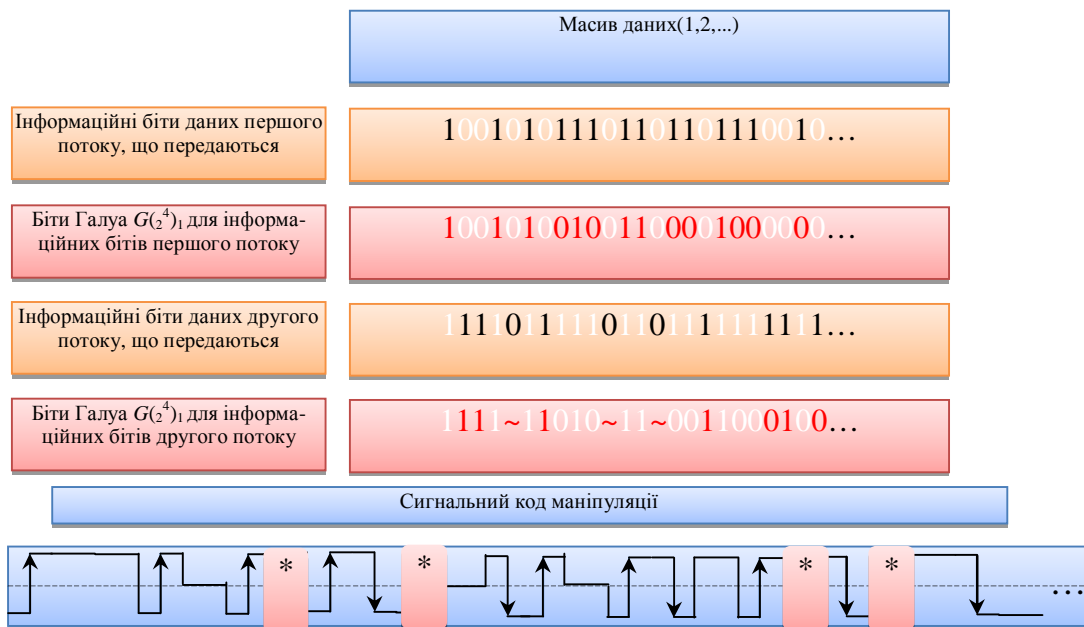


Рис. 6. Приклад потоку даних, маніпульованих за допомогою сигнальних коректуючих кодів, з виявленням помилок на сигнальному рівні, (* – помилка, яка вводиться)

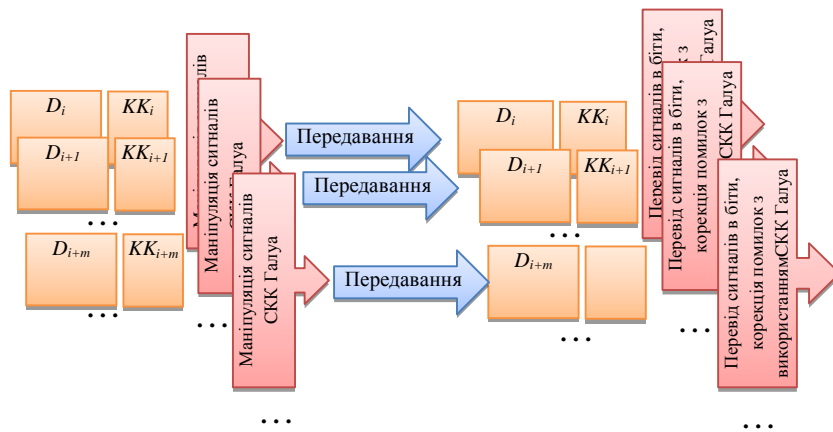


Рис. 7. Послідовність виконання операцій під час передавання k потоків даних

Водночас коректуючі коди в базисі Галуа, зокрема запропоновані нами сигнальні коректуючі коди, характеризуються функціональними обмеженнями, оскільки у разі виявлення помилок, довжина яких більша за розрядність кордону поля Галуа, можуть виникати неправильні корекції помилок. Внаслідок цього знижуються коректуючі властивості сигнальних кодів, особливо на низових рівнях комп'ютерних систем, де спостерігається значний вплив та зростання рівня промислових завод. Тому актуальним науково-технічним завданням є вдосконалення методів захисту інформації від помилок на основі сигнальних коректуючих кодів з метою підвищення рівня захисту під час виявлення пакетів помилок, які можуть виникати при завмираннях в каналах зв'язку та тиражуванні біт-орієнтованих помилок при їх коректуванні.

Виправлення помилок у сигнальних кодах з урахуванням спіральних властивостей кодів Галуа. Нехай маємо код Галуа G_2^4 , який формується рекурентним кодом [8]

$$G_{i+1} = G_i \oplus G_{i-4}, \quad (1)$$

тобто

$$G_2^4 = 1111\ 01011\ 0010\ 0011\ 1101\ 0110\ 0100\ 0111\ 1010\ 1100\ 1000\ 1111\ 0101\ \dots \quad (2)$$

Можна показати, що код, генерований на основі виразу (2), можна упакувати в спіраль (рис. 8), причому по кожній з чотирьох твірних формується рекурентна послідовність, яка має відповідні рекурентні властивості коду в базисі Галуа $G_{i+1} = G_i \oplus G_{i-4}$.

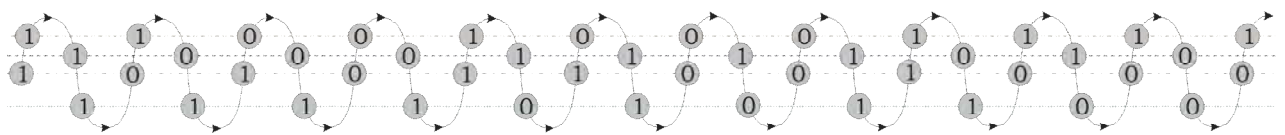


Рис. 8. СКК, упакований у вигляді спіралі

Але коли цю спіраль, закодовану рекурентним кодом, розкрутимо, то рекурентність збережеться через 12 символів і можливо виправляти помилки по твірних спіралі згідно з виразом:

$$G_{i+1,j} = G_{i,j} \oplus G_{i-12,j}, \quad j \in \overline{1,4} \quad (3)$$

З урахуванням спіральних властивостей сигнальний рекурентний код можна використати у разі виявлення пакетів помилок, оскільки спочатку перевіряються і виправляються помилки згідно з виразом (1) а потім згідно з виразом (3) по твірних спіралі [8].

На рис. 9 показано виявлення помилок з використанням спіральних властивостей сигнальних коректуючих кодів поля Галуа. Як видно з рис. 10, у разі виникнення помилок у п'яти підряд позиціях виявити помилки завдяки рекурсивному виразу (2) неможливо, оскільки можлива неправильна корекція, тому потрібно виявляти ці помилки завдяки спіральним властивостям, тобто виразу (3).

Біти Галуа G_2^4	1111010*****00011110...
Лінійні коди $G_{i,4}$	11110101100*00011110...
Спіральні коди $G_{i,12,j}$	11110101100100011110...

Рис. 9. Виявлення помилок з використанням спіральних властивостей СКК поля Галуа

Дослідження ефективності застосування лінійних та спіральних СКК в базисі Галуа дало змогу встановити можливість 100 % виправлення однократних помилок в інформаційних потоках за рахунок лінійних СКК у базисі Галуа, а також пакетів помилок у разі одночасного застосування лінійних та спіральних СКК у базисі.

Висновки

Проведені дослідження доводять можливість організації багатоканальних комп'ютерних мереж із застосуванням СКК в базисі Галуа, причому інформаційні біти "1" кожного потоку даних кодується відповідними сигнальними ознаками, поставленими у відповідність коду Галуа, а замість "0" йде наступний потік даних. Цей спосіб дає змогу в одній лінії передавати дані з різних потоків, забезпечуючи кращу заводозахищеність і корекцію помилок на сигнальному рівні. Застосування спіральних властивостей сигнальних коректуючих кодів у базисі Галуа дає змогу покращити ефективність формування та передавання інформації, створює перспективу їх широкого застосування в комп'ютерних системах для підвищення заводостійкості, коректувальних властивостей цих кодів і захисту від несанкціонованого доступу.

1. Николайчук Я.М. Теория джерел інформації. – Видання друге, виправлене. – Тернопіль: ТзОВ "Терно-граф", 2010. – 536 с. 2. Пат. на корисну модель 63648 Україна МПК(2011.01) H04J13/00. Багатоканальний спосіб передавання та приймання інформації / Николайчук Я.М., Воронич А.Р., 3. US Pat. 2552629 Error-detecting and Correcting/ Richard W. Hamming, Morristown, and Bernard D. Holbrook, Madison, N. J (New York, US)/ Bell Telephone Laboratories (New York, US). Serial No. 138,016 20 Field: May 15, 1951. 4. Харкевич А.А. Борьба с помехами. – М.: Наука, 1965. – 275 с. 5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: пер. с англ. – М.: Мир, 1976. – 600 с. 6. US Pat. 4376958 G11B5/09. Modified Frequency Modulation/ Archibald M. Pettigrew(Glenrothes, GB6)/Elcomatic Limited (Glasgow, GB6). Appl. No.:06/166,777. Filed: Jul 8, 1980. 7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с. 8. Воронич А.Р. Спіральні коди поля Галуа та їх коректуючі властивості // Збірник матеріалів проблемно-наукової міжгалузевої конференції "Юриспруденція та проблеми інформаційного суспільства". – Івано-Франківськ. – 2011. – С.76–78.