УДК 681.32

**В. П. Семеренко**[1]

# АВТОМАТНІ ПРЕДСТАВЛЕННЯ ЦИКЛІЧНИХ КОДІВ

[1]Вінницький національний технічний університет

*Відомі способи представлення циклічних кодів (поліноміальний, матричний та алгебраїчний) придатні для всіх класів лінійних блокових завадостійких кодів, але вони не враховують особливостей конкретних класів кодів. Наприклад, властивість циклічності таких кодів містить в собі великі потенціальні можливості, яка майже не використовуються у зазначених способах представлення кодів.*

*Пропонуються автоматні представлення циклічних кодів з використанням скінченних автоматів в полях Галуа — лінійних послідовнісних схем (ЛПС). Цей тип скінченних автоматів належить до систем, процеси в яких розвиваються циклічно в часі, тобто до динамічних систем. Розглядаються дві автоматні моделі циклічних кодів: автоматно-аналітична і автоматно-графова. Наведено означення циклічних кодів на основі цих автоматних моделей. Показано взаємозв'язок автоматного представлення з відомими представленнями циклічних кодів.*

*Проведено класифікацію ЛПС з позицій автоматного представлення циклічних кодів. Вперше для класифікації враховується дві характеристичні матриці ЛПС, що дає можливість розрізняти чотири базових типи ЛПС: рекурсивні та нерекурсивні ЛПС типів Галуа та Фібоначчі. Для врахування напряму переміщення даних можна розрізняти лівосторонні та правосторонні ЛПС, тобто вісім типів ЛПС.*

*Проведено дослідження процедур систематичного кодування та декодування циклічних кодів на основі їх автоматно-аналітичних моделей. Показано, що всі типи ЛПС дають однаковий результат при кодуванні та декодуванні, але з різною трудомісткістю. Теоретично обґрунтовано апаратну реалізацію для кожного типу ЛПС. Наведені критерії вибору типу ЛПС відносно фізичного часу та програмно-апаратних витрат.*

*Основна перевага методів кодування та декодування циклічних кодів на основі запропонованих математичних моделей — лінійна складність обчислень і проста програмно-апаратна реалізація.*

**Ключові слова**: автомат, циклічні коди, лінійний автомат, лінійна послідовнісна схема, кодер, декодер.

## Вступ

Захист даних за допомогою завадостійких кодів широко застосовується в супутниковому та мобільному зв'язку, комп'ютерних мережах, магнітних і оптичних дисках. Серед завадостійких кодів найчастіше зустрічаються різні типи циклічних кодів: коди CRC, БЧХ, Ріда-Соломона [1]. По традиції згадують їх переваги, зокрема, просту апаратну і програмну реалізацію.

Одночасно варто зазначити, що математичні основи циклічних кодів закладені більше 50 років тому, і з тої пори мало що змінилось в теорії цих кодів. Вже з'явились нові коди (турбо-коди, коди з малою густиною перевірки на парність), а в циклічних кодах, як і раніше, основним методом пошуку помилок залишається громіздкий та незручний алгоритм Берлекемпа–Мессі [2]. Настав час провести повну ревізію циклічних кодів, і глибше дослідити їх властивості. Резерви цих чудових кодів ще далеко не вичерпані.

Перш, ніж розробляти нові сучасні методи кодування і декодування кодів, необхідно проаналізувати математичні основи їх представлення. Для циклічних кодів використовують три основних способи їх опису: поліноміальний, матричний та алгебраїчний.

В поліноміальному представленні до циклічного ($n$, $k$)-коду буде належати множина поліномів $z(x)$, які діляться без остачі на заданий породжувальний поліном

$$g(x) = g_0 + g_1 x + \cdots + g_{r-1} x^{r-1} + g_r x^r \qquad (1)$$

степеня $r$ ($r = n - k$) в полі Галуа $GF(q)$.

Циклічні коди можна описати також за допомогою породжувальної ($n \times k$)-матриці $G$ або перевіряльної ($(n-k) \times n$)-матриці $H$. Алгебраїчний спосіб представлення базується на використанні коренів породжувального поліному $g(x)$ в полі розширення $GF\left(q^m\right)$.

Всі ці способи представлення дістались циклічним кодам в спадок від лінійних кодів, підкласом яких вони є. Додаткова властивість циклічності містить в собі нові потенціальні можливості,

які майже не використовуються у відомих способах представлення циклічних кодів.

Таким чином, необхідна розробка нових методів представлення циклічних кодів і на їх основі нових сучасних методів кодування та декодування з максимальним врахуванням особливостей цих кодів. *Мета роботи* — розробити математичні основи представлення циклічних кодів на основі теорії лінійних послідовнісних схем (ЛПС).

**Автоматні моделі циклічних кодів**

Як теоретичну основу для завадостійких кодів можна використати математичний апарат цифрових фільтрів. Теорію фільтрації і теорію завадостійкого кодування поєднує спільна мета: обидві теорії вивчають відновлення корисних вхідних сигналів на фоні завад за спостереженнями за відповідними вихідними сигналами [3].

Однак, класичний цифровий фільтр є нелінійною системою внаслідок багатьох чинників. Оскільки циклічні коди належать до лінійних кодів, то застосувати теорію фільтрів до завадостійкого кодування можна тільки за усунення явища нелінійності. Ця проблема може бути вирішена з переходом до полів Галуа [4].

З іншого боку теорія фільтрів близька і до теорії автоматів, оскільки фільтр реалізує автоматне відображення: перетворює вхідні слова у вихідні [5]. А для лінійного фільтра можна вже дати автоматний опис його функціонування, на що вперше звернув увагу B. Friedland [6]:

$$s_{i+1} = s_i T + u_i B;$$
$$w_i = s_i R + u_i Q,$$

де $u_i, w_i, s_i$ — слова вхідний, вихідний і стану; $T, B, R, Q$ — матриці, які характеризують структуру фільтра.

Як відомо, для опису функціонування класичного скінченного автомата використовуються логічні числення, на основі яких розроблені різноманітні алгебри логіки.

Якщо за базовий математичний апарат взяти теорію скінченних полів, тоді отримаємо новий тип скінченного автомата, властивості якого будуть фактично збігатися з властивостями лінійних фільтрів. Такий тип скінченного автомата можна назвати лінійним автоматом. Лінійний автомат належить до систем, процеси в яких розвиваються в часі, тобто до динамічних систем.

Таким чином, маємо нову математичну модель, якій доцільно дати самостійний термін. На жаль, до цього часу використовуються різні терміни (лінійна послідовнісна машина [7], багататактний лінійний фільтр [2] тощо). Найточнішим терміном є «*лінійна послідовнісна схема*» (ЛПС), який в подальшому і буде використовуватись. Дамо формальне означення ЛПС в загальному вигляді.

**Означення 1**. ЛПС з $r$ елементами пам'яті, $l$ входами і $m$ виходами є скінченним автоматом лінійного типу (лінійним автоматом), який над полем Галуа $GF(q)$ описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(q) \tag{2}$$

і функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(q), \tag{3}$$

де $t$ — дискретний час; $A = \left[ a_{ij} \right]_{r \times r}$, $B = \left[ b_{ij} \right]_{r \times l}$, $C = \left[ c_{ij} \right]_{m \times r}$, $D = \left[ d_{ij} \right]_{m \times l}$ — характеристичні матриці; $S(t) = \left[ s_i \right]_r$, $U(t) = \left[ u_i \right]_l$, $Y(t) = \left[ y_i \right]_m$ — відповідно, слова стану, вхідне і вихідне.

Будемо розрізняти автоматно-аналітичну і автоматно-графову моделі циклічного коду [8].

Автоматно-аналітична модель базується на характеристичних матрицях ЛПС. На основі цієї моделі можна дати означення циклічного коду. Нехай ЛПС знаходиться в деякому початковому стані $S_{beg}(t)$, наприклад, нульовому стані. Подамо на її входи таку двійкову послідовність $L$ довжини $n$, щоб ЛПС через $n$ тактів часу знову повернулася в стан $S_{beg}(t)$.

**Означення 2.** Множина всіх двійкових послідовностей $L$ довжини $n$, які переводять ЛПС із будь-якого початкового стану $S_{beg}(t)$ знову в стан $S_{beg}(t)$, утворює циклічний ($n$, $k$)-код $\Omega$ над полем Галуа $GF(q)$. Кожна така послідовність $L$ є кодовим словом $Z$ циклічного ($n$, $k$)-коду.

Оскільки ЛПС є скінченним автоматом, тому ЛПС має також графове представлення (граф пе-

реходів-виходів), яке може бути основою автоматно-графової моделі циклічного коду. Автоматно-графова модель складається з системи поєднаних між собою нульових циклів.

**Означення 3**. Послідовність $L$ із $n$ однонаправлених дуг в графі $G_{FA}$, в якому $i$-та дуга відповідає розряду $z_i$ кодового слова $Z$ над полем $GF(q)$, називається кодовим шляхом $\eta$ графа $G_{FA}$ ($z_i \in Z,\ i = 1...n$).

**Означення 4**. Множина всіх кодових шляхів $\eta$ довжини $n$, які починаються і закінчуються в початковій вершині $v_0$ графа $G_{FA}$ утворює циклічний ($n$, $k$)-код $\Omega$ над полем Галуа $GF(q)$.

Важливо відмітити взаємозв'язок різних представлень циклічних кодів. Наприклад, структура матриць $A$ та $B$, як буде далі показано, визначається структурою породжувального полінома (1) циклічного коду, а його перевіряльна матриця $H$ може бути отримана $n$-кратним використанням функції станів (2).

## Класифікація і дослідження рекурсивних ЛПС

Можливі різні типи ЛПС, які визначають і вид характеристичних матриць. Вибір характеристичних матриць ЛПС визначається вимогою $r$-керованості ЛПС, тобто можливістю переходу з будь-якого стану $S(i)$ в стан $S(j)$ не більше, ніж за $r$ тактів роботи автомата [7].

Нас будуть цікавити лише ті одноканальні ЛПС (з одним входом і одним виходом), які можуть бути використані для задач кодування і декодування циклічних кодів. Далі розглянемо класифікацію таких ЛПС з позицій теорії фільтрів і теорії поліномів з метою дослідження їх властивостей. Будемо використовувати ЛПС над полем Галуа $GF(2)$, але всі міркування легко поширюються і на недвійкові поля Галуа. Необхідність вибору того чи іншого способу класифікації обгрунтовується лише практичними потребами, зокрема трудомісткістю процедур кодування і декодування, а також витратами на їх апаратну та програмну реалізацію.

По-перше, будемо розрізняти рекурсивні ЛПС та нерекурсивні ЛПС: перші використовуються у систематичному кодуванні, а другі — у несистематичному кодуванні циклічних кодів.

Порівнюючи між собою теорію ЛПС і теорію фільтрів можна сказати, що нерекурсивним ЛПС відповідає нерекурсивний фільтр і схема для множення поліномів, а рекурсивним ЛПС — рекурсивний (авторегресійний) фільтр і схема для ділення поліномів.

Розглянемо класифікацію рекурсивних ЛПС з позицій автоматного представлення циклічних ($n$, $k$)-кодів, тобто з позицій означення 1. Основні властивості циклічних кодів визначаються структурою характеристичних матриць $A$ та $B$.

В більшості публікацій розрізняють лише два типи ЛПС: типу Галуа і типу Фібоначчі [9], [10], які відрізняються лише структурою характеристичних матриць $A$. Однак, матриці $B$ також можуть бути різними. Будемо розглядати дві структури матриць $B$: одностовпцеву матрицю, в якій одиничний елемент знаходиться лише в першому або в $r$-му розряді, і одностовпцеву матрицю, елементи в якій відповідають коефіцієнтам породжувального полінома (1).

Для задач завадостійкого кодування матриці $A$ та $B$ мають бути такими, щоб ЛПС була $r$-керованою, тобто для будь-якої пари станів $S(i)$ і $S(j)$ існувала вхідна послідовність довжини $r$, яка переводить $r$-вимірну ЛПС із $S(i)$ в $S(j)$ [7]. А ЛПС буде $r$-керованою, якщо ранг $r \times r$-матриці

$$L_r = \left[ A^{r-1} \times B,\quad A^{r-2} \times B,\quad \ldots\quad ,\quad A \times B,\quad B \right] \tag{4}$$

буде дорівнювати $r$.

З урахуванням різних структур матриць $A$ та $B$ можна розрізнити чотири базових типів ЛПС, які будемо йменувати лівосторонніми:

1) лівостороння ЛПС типу 1 (типу Галуа) з матрицями

$$A = \begin{vmatrix} 0 & 0 & 0 & \ldots & g_0 \\ 1 & 0 & 0 & \ldots & g_1 \\ 0 & 1 & 0 & \ldots & g_2 \\ \ldots & \ldots & \ldots & \cdots & \ldots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix};\ B = \begin{vmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{vmatrix}; \tag{5}$$

2) лівостороння ЛПС типу 2 з матрицями

$$A=\begin{vmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ 0 & 1 & 0 & \dots & g_2 \\ \dots & \dots & \dots & \cdots & \dots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix};\ B=\begin{vmatrix} g_0 \\ g_1 \\ g_2 \\ \dots \\ g_{r-1} \end{vmatrix}; \tag{6}$$

3) лівостороння ЛПС типу 3 (типу Фібоначчі) з матрицями

$$A=\begin{vmatrix} g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix};\ B=\begin{vmatrix} 1 \\ 0 \\ \dots \\ 0 \\ 0 \end{vmatrix}; \tag{7}$$

4) лівостороння ЛПС типу 4 з матрицями

$$A=\begin{vmatrix} g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \cdots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix};\ B=\begin{vmatrix} g_0 \\ g_1 \\ g_2 \\ \dots \\ g_{r-1} \end{vmatrix}. \tag{8}$$

Елементи останнього стовпця матриці $A$ в (5) і (6), елементи першого рядка матриці $A$ в (7) і (8), а також елементи матриці $B$ в (6) і (8) відповідають коефіцієнтам породжувального полінома (1) циклічного коду $\Omega$.

Неважко помітити спільну властивість наведених матриць $A$: розташування одиничних елементів під головною діагоналлю. Оскільки коефіцієнт $g_0$ в поліномі (1) завжди дорівнює одиниці, тому в кожному рядку і в кожному стовпці матриці $A$ є хоча б одна одиниця. Саме це і забезпечує $r$-керованість матриці (4). Можна запропонувати ще четвірку матриць $A$ та $B$, які будемо йменувати правосторонніми, і структура яких також забезпечуватиме $r$-керованість матриці (4):

1) правостороння ЛПС типу 1 (типу Галуа) з матрицями

$$A=\begin{vmatrix} g_{r-1} & 1 & 0 & \dots & 0 \\ g_{r-2} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ g_1 & 0 & 0 & \cdots & 1 \\ g_0 & 0 & 0 & \dots & 0 \end{vmatrix};\ B=\begin{vmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{vmatrix}; \tag{9}$$

2) правостороння ЛПС типу 2 з матрицями

$$A=\begin{vmatrix} g_{r-1} & 1 & 0 & \dots & 0 \\ g_{r-2} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ g_1 & 0 & 0 & \cdots & 1 \\ g_0 & 0 & 0 & \dots & 0 \end{vmatrix};\ B=\begin{vmatrix} g_{r-1} \\ g_{r-2} \\ \dots \\ g_1 \\ g_0 \end{vmatrix}; \tag{10}$$

3) правостороння ЛПС типу 3 (типу Фібоначчі) з матрицями

$$A=\begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & 1 \\ g_0 & g_1 & g_2 & \cdots & g_{r-1} \end{vmatrix};\ B=\begin{vmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{vmatrix}; \tag{11}$$

4) правостороння ЛПС типу 4 з матрицями

$$A=\begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & 1 \\ g_0 & g_1 & g_2 & \cdots & g_{r-1} \end{vmatrix};\ B=\begin{vmatrix} g_{r-1} \\ g_{r-2} \\ \dots \\ g_1 \\ g_0 \end{vmatrix}. \tag{12}$$

**Систематичне кодування циклічних кодів на основі автоматних моделей**

Процес кодування циклічного ($n$, $k$)-коду полягає в тому, що $k$-розрядні інформаційні слова відображаються в $n$-розрядні кодові слова, які і передаються по каналу зв'язку [1]. При систематичному кодуванні інформаційне слово $I$ і контрольне слово $\Psi$ відокремлені один від другого і кодове слово $Z$ можна записати як $Z = I\,\Psi$.

З позицій автоматного представлення циклічних кодів процес систематичного кодування на стороні кодера складається з двох етапів. На першому етапі на вхід рекурсивної ЛПС подається інформаційне слово $I$, в результаті чого ЛПС перейде протягом $k$ тактів з початкового нульового стану $S(0)$ в стан $S(k)$ згідно з формулою, яка випливає з (2):

$$S(k) = A^k \times S(0) + L_k \times I, \quad GF(2),$$

де $L_k = \left[ A^{k-1} \times B, \quad A^{k-2} \times B, \quad \dots \quad , \quad A \times B, \quad B \right]$.

На другому етапі на вхід рекурсивної ЛПС необхідно подати таке контрольне слово $\Psi$, щоб ЛПС перейшла протягом $r$ тактів зі стану $S(k)$ в кінцевий стан $S(n)$:

$$S(n) = A^r \times S(k) + L_r \times \Psi, \quad GF(2). \tag{13}$$

Оскільки після завершення процедури кодування ЛПС повинна знову повернутись в початковий стан (тобто, $S(n) = S(0)$), тому рівність (13) можна записати як

$$L_r \times \Psi = A^r \times S(k), \quad GF(2). \tag{14}$$

Як вже зазначалось, для успішного завершення систематичного кодування необхідно, щоб ЛПС була $r$-керованою, тобто ранг $r \times r$ -матриці (4) повинен дорівнювати $r$. Тому розглянемо структуру цієї матриці для різних типів ЛПС.

Для лівосторонньої ЛПС типу 1 та правосторонньої ЛПС типу 1:

$$L_r^{(1,l)}=\begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix};\ L_r^{(1,r)}=\begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}.$$

Для лівосторонньої ЛПС типу 2 та правосторонньої ЛПС типу 2:

$$L_r^{(2,l)}=\begin{bmatrix} l_{1,1} & l_{1,2} & \dots & l_{1,r-1} & 1 \\ l_{2,1} & l_{2,2} & \dots & 1 & l_{2,r} \\ \dots & \dots & \dots & \dots & \dots \\ l_{r-1,1} & 1 & \dots & l_{r-1,r-1} & l_{r-1,r} \\ 1 & l_{r,2} & \dots & l_{r,r-1} & l_{r,r} \end{bmatrix};\ L_r^{(2,r)}=\begin{bmatrix} 1 & l_{1,2} & \dots & l_{1,r-1} & l_{1,r} \\ l_{2,1} & 1 & \dots & l_{2,r-1} & l_{2,r} \\ \dots & \dots & \dots & \dots & \dots \\ l_{r-1,1} & l_{r-1,2} & \dots & 1 & l_{r-1},r \\ l_{r,1} & l_{r,2} & \dots & l_{r,r-1} & 1 \end{bmatrix}.$$

Для лівосторонньої ЛПС типу 3 та правосторонньої ЛПС типу 3:

$$L_r^{(3,l)} = \begin{bmatrix} l_{1,1} & l_{1,2} & \dots & l_{1,r-1} & 1 \\ l_{2,1} & l_{2,2} & \dots & 1 & 0 \\ l_{3,1} & l_{3,2} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix}; \quad L_r^{(3,r)} = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ l_{2,1} & 1 & \dots & 0 & 0 \\ l_{3,1} & l_{3,2} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ l_{r,1} & l_{r,2} & \dots & l_{r,r-1} & 1 \end{bmatrix}.$$

Для лівосторонньої ЛПС типу 4 та правосторонньої ЛПС типу 4:

$$L_r^{(4,l)} = \begin{bmatrix} l_{1,1} & l_{1,2} & \dots & l_{1,r-1} & 1 \\ l_{2,1} & l_{2,2} & \dots & 1 & l_{2,r} \\ \dots & \dots & \dots & \dots & \dots \\ l_{r-1,1} & 1 & \dots & l_{r-1,r-1} & l_{r-1,r} \\ 1 & l_{r,2} & \dots & l_{r,r-1} & l_{r,r} \end{bmatrix}; \; L_r^{(4,r)} = \begin{bmatrix} 1 & l_{1,2} & \dots & l_{1,r-1} & l_{1,r} \\ l_{2,1} & 1 & \dots & l_{2,r-1} & l_{2,r} \\ \dots & \dots & \dots & \dots & \dots \\ l_{r-1,1} & l_{r-1,2} & \dots & 1 & l_{r-1},r \\ l_{r,1} & l_{r,2} & \dots & l_{r,r-1} & 1 \end{bmatrix},$$

де $l_{i,j} = \{0,1\}, i \neq j$.

Всі наведені типи ЛПС мають різну структуру матриці $L_r$, відповідно складність систематичного кодування буде різною.

Оскільки матриці $L_r^{(1,r)}$ та $L_r^{(1,l)}$ є одиничними діагональними матрицями, то рівність (14) можна записати як

$$\Psi = -(A^r \times S(k)), \quad GF(2) \text{ для лівосторонньої ЛПС типу 1;} \tag{15}$$

$$\Psi = A^r \times S(k), \quad GF(2) \text{ для правосторонньої ЛПС типу 1.} \tag{16}$$

Знак «–» в (15) означає операцію інверсії слова, тобто взаємної перестановки між молодшими і старшими компонентами слова.

З (15) та (16) випливає, що для отримання на *n*-му такті кодування контрольного слова $\Psi$ необхідно лише *r*-кратне множення слова стану $S(k)$ на матрицю $A$.

Для ЛПС типу 2 існує цікава закономірність (детально описана в [11]):

$$L_r^{(2,r)} = A^r; \quad L_r^{(2,l)} = -A^r.$$

В результаті рівність (14) можна записати як $\Psi = S(k)$, або $\Psi = -S(k)$. Це означає, що контрольне слово $\Psi$ буде отримано вже на *k*-му такті кодування.

Матриці $L_r^{(3,r)}$, $L_r^{(3,l)}$, $L_r^{(4,r)}$ і $L_r^{(4,r)}$ мають складнішу структуру, тому для ЛПС типу 3 та ЛПС типу 4 знайти з рівності (14) невідоме значення слова $\Psi$ можна лише в результаті розв'язання системи *r* лінійних рівнянь над полем $GF(2)$. Оптимальним методом розв'язання системи лінійних рівнянь є метод Гауса [12], який передбачає послідовне використання двох процедур: перетворення довільної матриці до трикутного вигляду і подальшого знаходження невідомих елементів. Неважко помітити, що матриці $L_r^{(3,r)}$ і $L_r^{(3,l)}$ вже представляють собою трикутні матриці, що дозволяє відразу перейти до другої процедури метода Гауса. Різниця між контрольними словами $\Psi$ для правосторонніх та лівосторонніх ЛПС одного типу полягає лише у їх інверсії. Таким чином, за зростанням складності реалізації та часом виконання систематичного кодування різні типи ЛПС можна розташувати в такому порядку: ЛПС типу 2, ЛПС типу 1, ЛПС типу 3, ЛПС типу 4 (табл.).

**Складність систематичного кодування циклічного (*n*, *k*)-коду для різних типів ЛПС**

| Тип ЛПС | Кількість тактів для отримання контрольного слова | Математичні процедури на другому етапі кодування |
|---|---|---|
| лівостороння ЛПС типу 1 | *n* | за формулою (15) |
| правостороння ЛПС типу 1 | *n* | за формулою (16) |
| лівостороння ЛПС типу 2 | *k* | — |
| правостороння ЛПС типу 2 | *k* | — |
| лівостороння ЛПС типу 3 | *n* | метод Гауса (друга процедура) |
| лівостороння ЛПС типу 3 | *n* | метод Гауса (друга процедура), |
| лівостороння ЛПС типу 4 | *n* | метод Гауса (перша і друга процедури) |
| правостороння ЛПС типу 4 | *n* | метод Гауса (перша і друга процедури) |

### Декодування циклічних кодів на основі автоматних моделей

Процес декодування циклічних кодів також можна розділити на два етапи:
– встановлення факту відсутності чи наявності помилки;
– визначення параметрів помилки при її наявності.

З позицій автоматного представлення циклічних кодів перший етап полягає в обчисленні стану $S(n)$, в який перейде ЛПС після подачі на її вхід *n*-розрядного кодового слова $Z$ за рекурсивною формулою, яка випливає з (2):

$$S(j+1) = A \times S(j) + B \times z_j, \quad GF(2), \quad z_j \in Z, \quad j = 1...n.$$

Стан $S(n)$ прийнято називати синдромом помилки: нульове значення цього стану свідчить про відсутність помилок в переданому кодовому слові в межах виявляючої здатності циклічного коду. За наявності помилки кратності $\tau$ в кодовому слові, яке позначимо як $Z_{err}^{(\tau)}$, буде отримано ненульовий синдром помилки $S_{err}^{(\tau)}$.

Суть процедури пошуку помилок найкраще пояснити за допомогою автоматно-графової моделі циклічного коду (графу $G_{FA}$) [13]. Кодовому слову *Z* відповідає шлях довжиною *n* в графі $G_{FA}$, який починається і закінчується в тій самій вершині, наприклад, у вершині $v_0$. Під впливом випадкової помилки кратності $\tau$ кодовий шлях в графі $G_{FA}$ починається з вершини $v_0$ і закінчується в деякій вершині помилки, яку позначимо як $v_{err}$. Такий шлях в графі $G_{FA}$ відповідає кодовому слову $Z_{err}^{(\tau)}$.Для виявлення та виправлення помилки необхідно знайти найкоротший шлях від вершини $v_{err}$ до вершини $v_0$. При цьому шлях буде проходити через різні нульові цикли графу $G_{FA}$. В [8] наведені методи виявлення помилок різних видів.

Тут зазначимо, що саме при декодуванні циклічного коду за його автоматно-графовою моделлю повною мірою використовується основна властивість цього коду — властивість циклічності. Тому розроблені методи декодування циклічних кодів мають невисоку складність і просту програмно-апаратну реалізацію.

### Апаратна реалізація циклічного кодування і декодування

В попередніх підрозділах розглядалась швидкість виконання операцій кодування і декодування з математичних позицій. Однак, фактичні витрати часу будуть залежати від схемотехнічної реалізації ЛПС, тобто функцій переходів (2) і функцій виходів (3).

Почнемо з лівосторонньої ЛПС типу 1, яка задається характеристичними матрицями (5).

**Теорема 1**. Для ЛПС типу 1 операції множення і додавання *r*-розрядних слів в полі $GF(2)$ при реалізації функцій (2) і (3) можна замінити операцією зсуву і однією операцією додавання *r*-розрядних слів в полі $GF(2)$.

*Доведення*. За правилами матричної алгебри процедура множення ($r \times r$)-розрядної матриці (5) на *r*-розрядне слово стану $S(t)$ складається з операцій додавання в полі $GF(2)$ тих стовпців матриці *A*, чиї номери збігаються з номерами ненульових компонент слова $S(t)$:

$$S(t+1) = \begin{vmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ 0 & 1 & 0 & \dots & g_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix} \times \begin{vmatrix} s_0 \\ s_1 \\ s_2 \\ \dots \\ s_{r-1} \end{vmatrix} = \begin{bmatrix} 0 \\ s_0 \\ 0 \\ \dots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ s_1 \\ \dots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \dots \\ s_{r-2} \end{bmatrix} + \dots + \begin{bmatrix} s_{r-1} \times g_0 \\ s_{r-1} \times g_1 \\ s_{r-1} \times g_2 \\ \dots \\ s_{r-1} \times g_{r-1} \end{bmatrix}.$$

Результатом множення матриці $B$ на компоненту *u* вхідного слова $U(t)$ буде слово $\begin{bmatrix} u \\ 0 \\ \dots \\ 0 \end{bmatrix}$.

Об'єднаємо отримані результати в два стовпці:

$$S(t+1)=\begin{bmatrix} u \\ s_0 \\ s_1 \\ \dots \\ s_{r-2} \end{bmatrix}+\begin{bmatrix} s_{r-1}\times g_0 \\ s_{r-1}\times g_1 \\ s_{r-1}\times g_2 \\ \dots \\ s_{r-1}\times g_{r-1} \end{bmatrix}. \qquad (17)$$

Як видно з (17), перший стовпець слова стану $S(t+1)$ є зсунутою в бік старших розрядів слова стану $S(t)$, причому в молодший розряд, що звільняється, заноситься компонента *u*. Другий стовпець слова стану $S(t+1)$ перетворюється в нуль при $s_{r-1}=0$, або в останній стовпець матриці $A$ при $s_{r-1}=1$. Для правосторонньої ЛПС типу 1 на основі матриць (9) слово стану $S(t+1)$ є таким:

$$S(t+1)=\begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_{r-1} \\ u \end{bmatrix}+\begin{bmatrix} s_0\times g_{r-1} \\ s_0\times g_{r-2} \\ \dots \\ s_0\times g_1 \\ s_0\times g_0 \end{bmatrix}.$$

Таким чином, для отримання слова стану $S(t+1)$ для лівосторонньої ЛПС необхідно лише одна операція зсуву в бік старших розрядів слова стану $S(t)$ при $s_{r-1}=0$, або операції зсуву і операції додавання *r*-розрядних слів при $s_{r-1}=1$. Для правосторонньої ЛПС змінюється лише напрям зсуву і компонента *u* заноситься в старший розряд, що звільняється.

В обох випадках апаратно операція зсуву реалізується регістром зсуву з лінійним оберненим зв'язком, а операції додавання — суматорами за модулем два.

Тепер розглянемо ЛПС типу 2, яка задається характеристичними матрицями (6).

**Теорема 2.** Для ЛПС типу 2 операції множення і додавання *r*-розрядних слів в полі $GF(2)$ за реалізації функцій (2) і (3) можна замінити операцією зсуву і однією або двома операціями додавання *r*-розрядних слів в полі $GF(2)$.

*Доведення*. По аналогії з доведенням Теореми 1 отримаємо структуру слова стану $S(t+1)$ для лівосторонньої ЛПС з матрицями (6)

$$S(t+1)=\begin{bmatrix} 0 \\ s_0 \\ s_1 \\ \dots \\ s_{r-2} \end{bmatrix}+\begin{bmatrix} s_{r-1}\times g_0 \\ s_{r-1}\times g_1 \\ s_{r-1}\times g_2 \\ \dots \\ s_{r-1}\times g_{r-1} \end{bmatrix}+\begin{bmatrix} u\times g_0 \\ u\times g_1 \\ u\times g_2 \\ \dots \\ u\times g_{r-1} \end{bmatrix}.$$

Для правосторонньої ЛПС з матрицями (10) структура слова стану $S(t+1)$ буде такою:

$$S(t+1)=\begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_{r-1} \\ 0 \end{bmatrix}+\begin{bmatrix} s_0\times g_{r-1} \\ s_0\times g_{r-2} \\ \dots \\ s_0\times g_1 \\ s_0\times g_0 \end{bmatrix}+\begin{bmatrix} u\times g_{r-1} \\ u\times g_{r-2} \\ \dots \\ u\times g_1 \\ u\times g_0 \end{bmatrix}.$$

В обох випадках ми отримаємо одну або дві операції додавання *r*-розрядних слів в полі $GF(2)$ в залежності від значень компонент $s_{r-1}$ і *u*. Найскладніший варіант буде у випадку $s_{r-1}=1$ і $u=1$.

**Теорема 3.** Для ЛПС типу 3 операції множення і додавання *r*-розрядних слів в полі $GF(2)$ за реалізації функцій (2) і (3) можна замінити операцією зсуву і декількома (не більше *r*) операціями додавання *r*-розрядних слів в полі $GF(2)$.

*Доведення*. За аналогією з доведенням теореми 1 отримаємо структуру слова стану $S(t+1)$ для лівосторонньої ЛПС типу 3 з матрицями (7)

$$S(t+1)=\begin{bmatrix} u \\ s_0 \\ s_1 \\ \dots \\ s_{r-2} \end{bmatrix}+\begin{bmatrix} s_0 \times g_{r-1} \\ 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}+\begin{bmatrix} s_1 \times g_{r-2} \\ 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}+\dots+\begin{bmatrix} s_{r-1} \times g_0 \\ 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}.$$

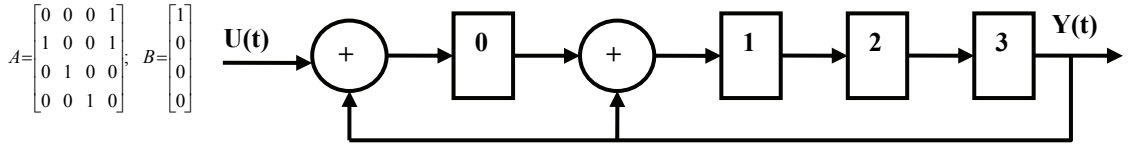
Для правосторонньої ЛПС типу 3 з матрицями (11) структура слова стану $S(t+1)$ буде такою:

$$S(t+1)=\begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_{r-1} \\ u \end{bmatrix}+\begin{bmatrix} 0 \\ 0 \\ \dots \\ \dots \\ s_0 \times g_0 \end{bmatrix}+\begin{bmatrix} 0 \\ 0 \\ \dots \\ \dots \\ s_1 \times g_1 \end{bmatrix}+\dots+\begin{bmatrix} 0 \\ 0 \\ \dots \\ \dots \\ s_{r-1} \times g_{r-1} \end{bmatrix}.$$

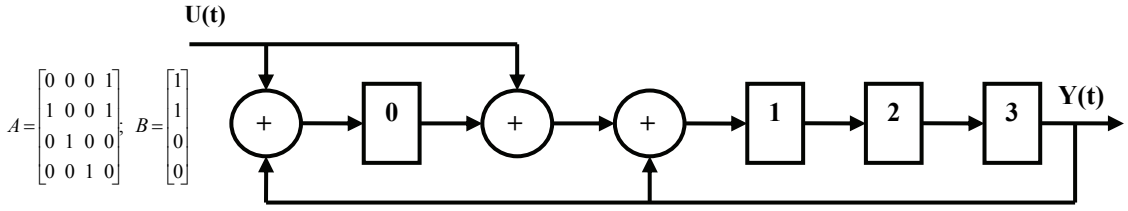
Апаратною реалізацією ЛПС типу 3 буде регістр зсуву з лінійним оберненим зв'язком і багатовходовим (не більше $r+1$ входів) суматором за модулем 2. Аналогічну апаратну реалізацію мають також ЛПС типу 4.

Найпростішу апаратну реалізацію мають ЛПС типу 1, а найскладнішу — ЛПС типу 3 і типу 4.

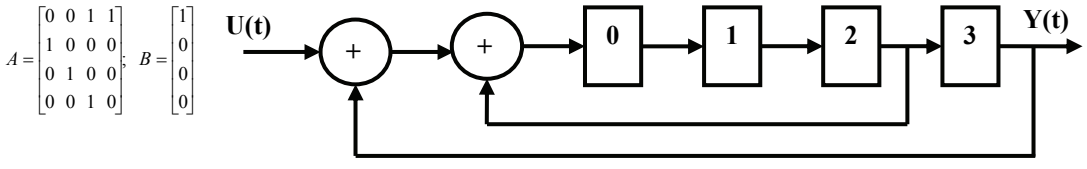
**Приклад**. Розглянемо апаратну реалізацію ЛПС. На рис. 1 показані схеми лівосторонніх ЛПС для матриць (5)—(8), а на рис. 2 — схеми правосторонніх ЛПС для матриць (9)—(12).



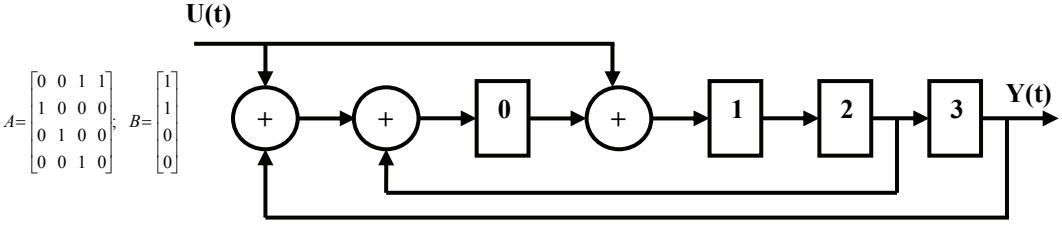

а)




б)




в)




г)

Рис. 1. Характеристичні матриці та схеми лівосторонніх ЛПС для циклічного (15,11)-коду з породжувальним поліномом $g(x)=1+x+x^4$: а — типу 1; б — типу 2; в — типу 3; г — типу 4

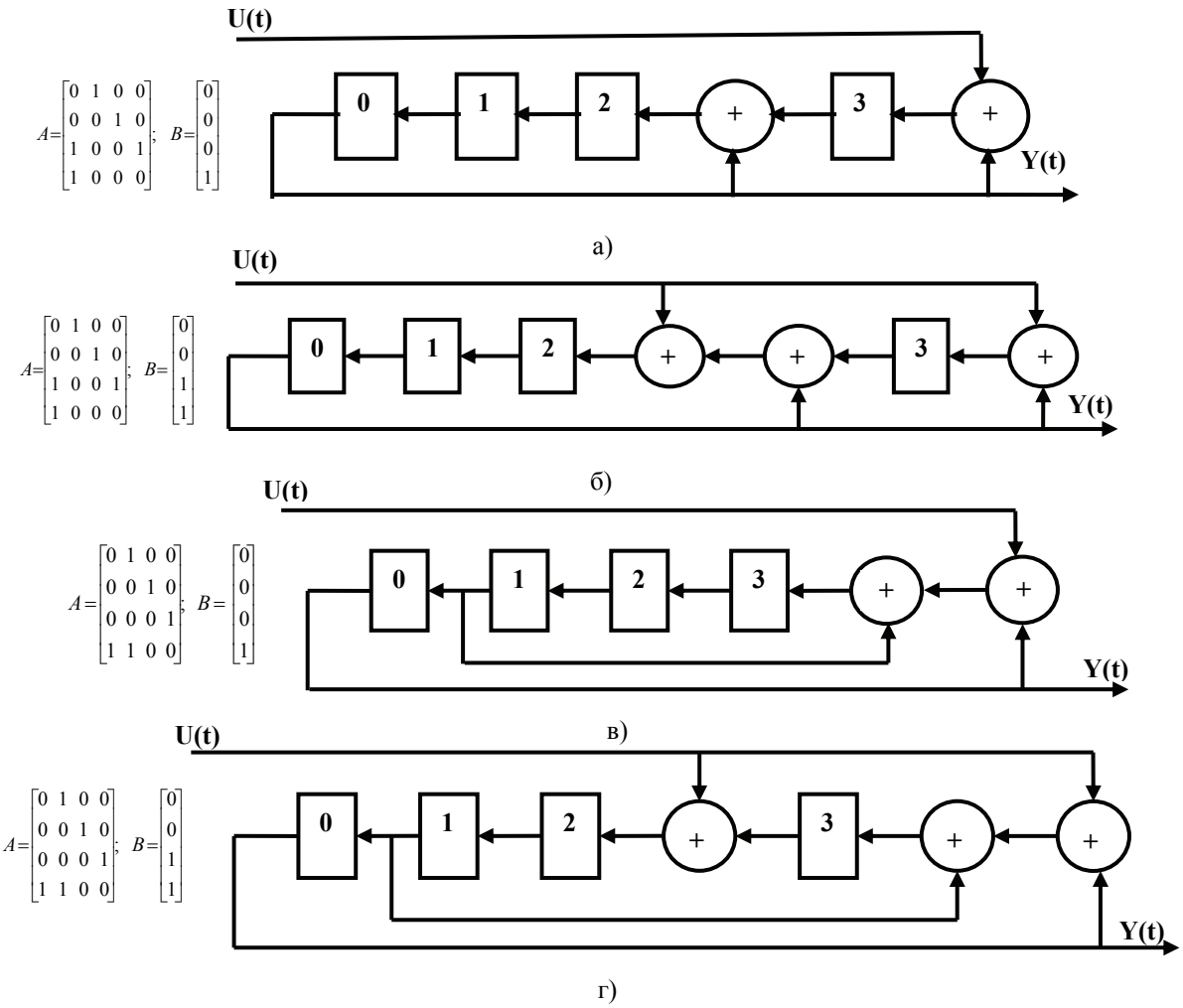



Рис. 2. Характеристичні матриці та схеми правосторонніх ЛПС для циклічного (15,11)-коду з породжувальним поліномом $g(x) = 1 + x + x^4$: а — типу 1; б — типу 2; в — типу 3; г — типу 4

Як випливає з рис. 1 та рис. 2 матриця $A$ визначає спосіб з'єднання між собою елементів затримки (тригерів) регістра зсуву. Якщо елемент $a_{ij}$ матриці $A$ дорівнює одиниці, тоді повинен існувати зв'язок між виходом $j$-го елемента затримки і входом $i$-го елемента затримки, а якщо $a_{ij} = 0$, тоді зв'язок між вказаними елементами затримки відсутній. Матриця $B$ визначає структуру входів ЛПС: якщо елемент $b_{ij}$ матриці $B$ дорівнює одиниці, тоді має існувати зв'язок між $j$-м входом ЛПС і входом $i$-го елемента затримки, а якщо $b_{ij} = 0$, тоді такий зв'язок відсутній.

В лівосторонніх ЛПС вхідні дані та дані з найстаршого розряду ЛПС завжди надходять в наймолодший розряд. Відповідно у правосторонніх ЛПС вхідні дані та дані з наймолодшого розряду ЛПС завжди надходять в найстарший розряд.

В процесі реалізації операцій кодування і декодування в недвійкових полях Галуа (наприклад, для кодів Ріда–Соломона [14]) в схемах кодерів та декодерів з'являється третій базовий елемент — помножувач в полях Галуа.

## Висновки

Автоматне представлення циклічних кодів є найпридатнішим для циклічних кодів, оскільки максимально враховує властивість циклічності та інші особливості цих кодів.

Існує тісний зв'язок між автоматним та іншими способами опису циклічних кодів, що дозволяє легко перейти від одного способу до іншого. Для автоматного задання циклічного коду необхідно вибрати породжувальний поліном з необхідною завадостійкістю, тип ЛПС та її параметри (лівостороння чи правостороння).

Вперше запропоновано вісім типів ЛПС і проаналізовано їх математичні властивості з позицій завадостійкого кодування. Всі типи ЛПС дають однаковий результат при кодуванні та декодуванні, але з різною трудомісткістю. Якщо критерієм ефективності вважати кількість математичних тактів, тоді найшвидшою є ЛПС типу 2. З позицій фізичного часу та програмно-апаратних витрат оптимальним вибором буде ЛПС типу 1. В кодері та декодері можна використовувати ЛПС з одним породжувальним поліномом, але різного типу в залежності від наявності різних вимог.

На основі математичного апарату ЛПС можна створити алгоритми кодування та декодування лінійної складності.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Р. Морелос-Сарагоса, *Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение*. Москва, Россия: Техносфера, 2006.

[2] В. Д. Колесник, *Кодирование при передаче и хранении информации (Алгебраическая теория блоковых кодов).* Москва, Россия: Высш. школа, 2009.

[3] Э. С. Айчифер, и Б. У. Джервис, *Цифровая обработка сигналов: практический подход*, 2-е изд. испр. Москва, Россия: Издательский дом «Вильямс», 1992.

[4] Р. Лидл, и Г. Нидеррайтер, *Конечные поля*. В 2 т., Т. 1. Москва, Россия: Мир, 1988.

[5] О. П. Кузнецов, и Г. М. Адельсон-Вельский. *Дискретная математика для инженера*, 2-е изд. Москва, Россия: Энергоатомиздат, 1988.

[6] B. Friedland, "Linear Modular Sequential Circuits," *IRE Trans*, vol. 6, pp. 61-68, 1959.

[7] А. Гилл, *Линейные последовательностные машины*. Москва, Россия : Наука, 1974.

[8] В. П. Семеренко, *Теорія циклічних кодів на основі автоматних моделей*. Вінниця, Україна : ВНТУ, 2015.

[9] F. Arnault, T. Berger, and M. Minier, "Revisiting LFSRs for Cryptographic Applications," *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 8095-8113, 2011.

[10] E. Milovanovic, M. Stojcev, I. Milovanovic, and T. Nikolic, "Concurrent Generation of Pseudo Random Numbers with LFSR of Fibonacci and Galois Type," *Computing and Informatics*, vol. 34, pp. 941-958, 2015.

[11] V. P. Semerenko, "The Theory of Parallel CRC Codes Based on Automaton Models," *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 9 (84), pp. 45-55. 2016. doi: 10.15587/1729-4061.2016.85603.

[12] Т. Х. Кормен, Ч. Е. Лейзерсон, Р. Л. Ривест, и К. Штайн, *Алгоритмы: построение и анализ*, 3-е изд. Москва, Россия: ООО Издательский дом «Вильямс», 2014.

[13] В. П. Семеренко, «Высокопроизводительные алгоритмы для исправления независимых ошибок в циклических кодах,» в *Системи обробки інформації: зб. наук. пр.* Харків, Україна: ХУПС, вип. 3(84), с. 80-89, 2010.

[14] В. П. Семеренко, «Декодирование кодов Рида-Соломона на основе графовой и автоматной моделей,» *Электронное моделирование*, № 1, с. 57-72, 2011.

Рекомендована кафедрою захисту інформації ВНТУ

Стаття надійшла до редакції 26.12.2017

***Семеренко Василь Петрович*** — канд. техн. наук, доцент, доцент кафедри обчислювальної техніки, e-mail: vpsemerenko@ukr.net .

Вінницький національний технічний університет, Вінниця

**V. P. Semerenko**[1]

# Automaton Presentations of Cyclic Codes

[1]Vinnytsia National Technical University

*Known methods for representing cyclic codes (polynomial, matrix, and algebraic) are suitable for all classes of linear block error-correcting codes, but they do not take into account the particularities of specific classes of the codes. For example, the cycle property of the cyclic codes contains large potential features that are not nearly used in the specified methods of code representation.*

*The automaton representations of cyclic codes using finite automaton in Galois fields – linear finite-state machine (LFSM) – are proposed. This type of finite automaton belongs to the systems the processes of which are developing in time cyclically, i.e. to dynamic systems. The automaton-analytic and automaton-graphical models are considered. Accordingly, the definition of cyclic codes based on these automaton models is given. The relationship between the automaton representation and the known representations of cyclic codes is shown.*

*The classification of LFSM from the positions of the automaton representation of cyclic codes is done. For the first time, two characteristic LFSM matrices are taken into account for classification, which makes it possible to distinguish four basic LFSM types: recursive LFSM and non-recursive LFSM of Galois and Fibonacci. When taking into account the direction of*

*data movement, it is possible to distinguish between left-hand and right-hand LFSM, i.e. eight types of LFSM.*

*A study of the procedures of systematic encoding and decoding of cyclic codes based on their automaton-analytical models is carried out. It is shown that all types of LFSM give an identical result at encoding and decoding, but with different labor intensiveness. The hardware implementation for each type of LFSM is theoretically substantiated. Criteria over type selection LFSM of relatively physical time and hardware-software expenses are brought.*

*Basic advantage of methods of encoding and decoding of cyclic codes based on offered mathematical models is the linear complexity of computations and simple hardware-software implementation.*

**Keywords:** automaton, cyclic codes, linear finite-state machines, encoder, decoder.

***Semerenko Vasyl P.*** — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Computer Technique, e-mail: vpsemerenko@ukr.net

**В. П. Семеренко**[1]

# Автоматные представления циклических кодов

[1]Винницкий национальный технический университет

*Известны способы представления циклических кодов (полиномиальный, матричный и алгебраический) пригодны для всех классов линейных блоковых помехоустойчивых кодов, но они не учитывают особенностей конкретных классов кодов. Например, свойство цикличности этих кодов содержит в себе большие потенциальные возможности, которые почти не используются в указанных способах представления кодов.*

*Предлагаются автоматные представления циклических кодов с использованием конечных автоматов в полях Галуа — линейных последовательностных схемах (ЛПС). Этот тип конечных автоматов принадлежит к системам, процессы в которых развиваются циклически во времени, т.е. к динамическим системам. Рассматриваются две автоматные модели циклических кодов: автоматно-аналитическая і автоматно-графовая. Соответственно приведено определение циклических кодов на основе этих автоматных моделей. Показана взаимосвязь автоматного представления с известными представлениями циклических кодов.*

*Приведена классификация ЛПС с позиций автоматного представления циклических кодов. Впервые для классификации учитываются две характеристические матрицы ЛПС, что позволяет различать четыре базовых типа ЛПС: рекурсивные и нерекурсивные ЛПС типов Галуа и Фибоначчи. При учете направления перемещения данных можно различать левосторонние и правосторонние ЛПС, т.е. восемь типов ЛПС.*

*Проведено исследование процедур систематичного кодирования и декодирования циклических кодов на основе их автоматно-аналитических моделей. Показано, что все типы ЛПС дают одинаковый результат при кодировании и декодировании, но с разной трудоемкостью. Теоретически обоснована аппаратная реализация для каждого типа ЛПС. Приведены критерии выбора типа ЛПС относительно физического времени и программно-аппаратных затрат.*

*Основное преимущество методов кодирования и декодирования циклических кодов на основе предложенных математических моделей — линейная сложность вычислений и простая программно-аппаратная реализация.*

**Ключевые слова**: автомат, циклические коды, линейная последовательностная схема, кодер, декодер.

***Семеренко Василий Петрович*** — канд. техн. наук, доцент, доцент кафедры вычислительной техники, e-mail: vpsemerenko@ukr.net