# ЛІНІЙНА СКЛАДНІСТЬ

Лінійною складністю $L(S)$ двійкової послідовності $S=s_0, s_1,\ldots,s_{n-1}, s_j\in\{0,1\}$ називається найменша довжина зсувного регістру з лінійною функцією зворотного зв'язку (Linear Feedback Shift Register – LFSR), що здатний відтворити цю послідовність. Доведено, що якщо значення лінійної складності послідовності дорівнює половині її довжини, тобто якщо $L(S)=n/2$, то таку послідовність теоретично не можливо екстраполювати. Для визначення лінійної складності використовується ітераційний алгоритм Berlecamp-Massey.

Алгоритм дозволяє не тільки визначити значення лінійної складності послідовності, але й отримати поліном зворотного зв'язку LFSR, що відтворює задану послідовність.

Вхідними даними для роботи алгоритму Berlecamp-Massey є двійкова послідовність $s_0,s_1,\ldots,s_{n-1}$. В алгоритмі використовуються наступні компоненти: $L$ - поточне значення лінійної складності, $C(D) = c_L\cdot D^L + c_{L-1}\cdot D^{L-1} + \ldots + c_1\cdot D + 1$ - поліном лінійної функції зворотного зв'язку для $L$-розрядного зсувного регістру, $B(D)$-допоміжний поліном, $N$ - номер поточного біту заданої двійкової послідовності. В наведеному нижче описі алгоритму операції додавання відповідають операціям додавання по модулю 2. Итераційний алгоритм Berlecamp-Massey полягає в виконанні наступної послідовності кроків:

1. Присвоєння початкових значень: $C(D) = B(D) = 1$, $x=1$, $L=0$, $N=0$.

2. Обчислення для поточного $N$–го біту $s_N$ заданої послідовності біту $d$ неузгодженості з поточним поліномом $C(D)$ по $L$ попереднім бітам послідовності:

$$d = s_N + \sum_{j=1}^{L} c_j \cdot s_{N-j} . \qquad (1)$$

3. Якщо $d=0$, то біт $s_N$ правильно відтворюється LFSR з регістром довжиною $L$ зі структурою зворотного зв'язку, що задається $C(D)$ , відповідно, виконується інкремент значення $x=x+1$ і перехід на п.6.

4. Якщо $d=1$ і при цьому $2\cdot L > N$ , то біт $s_N$ невірно відтворюється LFSR з регістром довжиною $L$ зі структурою зворотного зв'язку, що задається $C(D)$ і

правильне відтворення біту $s_N$ може бути досягнуте корекцією поліному $C(D)$ без збільшення довжини L зсувного регістру. Корекція поліному виконується у відповідності з формулою: $C(D) = C(D)+D^x \cdot B(D)$, $x = x+1$.

5. Якщо $d = 1$, але $2 \cdot L \leq N$, то адекватне відтворення біту $s_N$ може бути досягнуте збільшення довжини зсувного регістру $L=N+1-L$ і корекцією поліному, що задає функцію зворотного зв'язку: $C(D) =C(D)+D^x \cdot B(D)$, при цьому в в $B(D)$ зберігається попереднє значення поліному $C(D)$: $B(D) = C(D)$, а значення $x$ встановлюється в одиницю $x = 1$.

6. Виконується перехід до обробки наступного символу послідовності: $N = N+1$. Якщо при цьому N=n , то кінець, інакше - повернення на п.2 алгоритму.

Робота описаного алгоритму Berlecamp-Massey ілюструється наступним прикладом. Нехай задана двійкова послідовність:

$S = s_0, s_1, \ldots, s_{14}$ =1 0 1 0 1 1 0 0 1 0 0 0 1 1 1

Згідно з п.1 алгоритму: $C(D)=1$; $B(D)=1$; $x=1$, $N=0$, $L=0$.

**N=0**. Так як $L=0$, то сума в формулі (1) не обчислюється і тому $d = x_0 = 1$ Оскільки $2 \cdot L=N$, то виконується п.5 алгоритму, а саме: $C(D) = C(D)+D^1 \cdot B(D) = 1+D$, $x = 1$, $B(D)=1$; $L=0+1- 0=1$.

**N=1.** Так як $C(D)=1+D^1$, то $d = x_1+x_0 \cdot 1 = 1$. Оскільки $2 \cdot L>N$, корекція $C(D)$ виконується по п.4 описаного вище алгоритму: $C(D)=C(D)+D^1 \cdot B(D)=1+D+D =1$, $x = 2$.

**N=2** Оскільки в формулі для $C(D)$ нема ні одного $D$, то $d = x_2 + 0 = 1 + 0=1$. Так як $2 \cdot L=N$, то корекція поліному $C(D)$ виконується згідно п.5 алгоритму: $C(D)=C(D)+D^2 \cdot B(D) = 1+D^2$. $B(D)=1$, $x=1$; $L=2+1-1=2$; це означає, що при відтворенні наступного біту послідовності враховуються два попередніх. Оскільки в вираз для $C(D)$ входить $D^2$, то відтворення відбувається лише з урахуванням першого біта зазначеної пари попередніх бітів.

**N=3** При відтворенні біту $s_3$ - попередні біти $s_1$ $s_2$ = 0 1, першому з яких відповідає компонента $D^2$ поліному $C(D)$, а другому – компонента $D^1$, яка

відсутня в поточному значенні поліному $C(D)$. Згідно п.2 обчислюється значення $d$: $d=s_3 + s_1 = 0$. Оскільки $d=0$, то виконується п.3: $x=x+1=2$.

**N=4** Для біту $s_4$ - попередні : $s_2$ $s_3$ =1 0. Згідно п.2 значення $d$ обчислюється у вигляді: $d=s_4 + s_2 = 0$. Оскільки $d=0$, то виконується п.3: $x=x+1=3$.

**N=5** Для біту $s_5$ - попередні біти $s_3$ $s_4$ = 0 1. Згідно п.2 значення $d$ обчислюється як: $d=s_5 + s_3 = 1$. Оскільки при $d=1$ виконується умова $2 \cdot L<N$, то корекція поліному $C(D)$ реалізується згідно п. 5 описаного алгоритму: $C(D)=C(D)+D^3 \cdot B(D) = 1+D^2+D^3$. $B(D) = 1+D^2$, $L=5+1-2=4$. $x=1$.

**N=6** Так як L=4 то відтворення біту $s_6$ виконується по чотирьом попереднім бітам: $s_2$ $s_3$ $s_4$ $s_5$ = 1 0 1 1. Оскільки $C(D)$ містить тільки $D^2$ і $D^3$ ( $s_2$ відповідає компоненті $D^4$, $s_3$ відповідає $D^3$, біт $s_4$ - компоненті $D^2$, а $s_5$ - $D$ ), то відновлення значення біту $s_6$ згідно (1) виконується у наступному вигляді: $d=s_6+ (s_3+s_4) = 0+(0+1)=1$. Так як $2 \cdot L = 8 > N$, то виконується п.4 алгоритму, за яким $C(D) = C(D)+D^1 \cdot B(D) = 1+D^2+D + D \cdot (1+D^2) = 1+D+D^2$, $x=x+1=2$.

**N=7.** Обчислення біту $s_7$ знов виконується по чотирьом ($L=4$) попереднім бітам послідовності $s_3$ $s_4$ $s_5$ $s_6$. За п.2 обчислюється $d=s_7 + (s_5 + s_6) =1$. В силу того, що $2 \cdot L =8 > N$ то корекція поліному виконується по п.4 алгоритму $C(D) = C(D)+D^2 \cdot B(D) = 1+D+D^2 + D^2 \cdot (1+D^2) = 1+D+D^4$. $x=x+1=3$

**N=8.** Обчислення біту $s_8$ знов виконується по чотирьом ($L=4$) попереднім бітам послідовності $s_4$ $s_5$ $s_6$ $s_7$. В виразі поліному $C(D)$ лише дві ненульові компоненти $D^4$ и $D^1$, які співвідносяться з парою крайніх бітів $s_4$ та $s_7$. Відповідно, в п.2 обчислюється $d=s_8 + (s_4+s_7)=0$. За п.3 $x=x+1=4$.

Легко перевірити, що в подальшому, для всіх наступних бітів послідовності $s_9$, $s_{10}$, …,$s_{14}$ обчислене в п.2 значення $d$ завжди дорівнюватиме нулю, тобто значення лінійної складності $L=4$ не зміниться. Таким чином, задана двійкова послідовність відтворюється 4-розрядним LFSR з функцією зворотного зв’язку, що описується поліномом $C(D)= D^4 +D+1$.