Algorytmy

LFSR (ang. *Linear Feedback Shift Register*)

1. Wypełnij rejestr pseudolosową sekwencją wartości binarnych.
2. Wykonaj operację sumy modulo 2 (*XOR*) na wybranych komórkach rejestru, przesuń rejestr w lewo i wpisz uzyskany bit do skrajnie prawej komórki. Bit ten stanowi wyjście generatora.
3. Powtarzaj punkt 2, aż do uzyskania ciągu wyjściowego o wymaganej długości.

Algorytm Berlekamp'a-Massey'a

0. Założenia początkowe: $c(D) = 1, L = 0, q = -1, b(D) = 1, N = 0$.
1. Wczytaj ciąg binarny S^n o długości n.
2. Dopóki $N < n$ wykonuj operacje w pętli.
   2.1. Wyznacz wartość rozbieżności *d:*
   $$d = \left(S_N + \sum_{i=1}^{L} c_i S_{N-i+1}\right) mod\ 2 \qquad (1.1)$$
   2.2. Jeśli wartość rozbieżności jest równa *1*, wtedy:
      2.2.1. Zachowaj stan wielomianu połączeń *c(D)*.
      2.2.2. Wyznacz nowy wielomian *c(D)* taki, że:
      $$c(D) = c(D) \oplus b(D) \times D^{N-q} \qquad (1.2)$$
      2.2.3. Jeżeli stopień rejestru *L* jest mniejszy lub równy od *N/2* to:
         2.2.3.1. Wyznacz nowy stopień jako $L = N - L + 1$.
         2.2.3.2. Do zmiennej *q* przypisz *N*.
         2.2.3.3. Do wielomianu pomocniczego *b(D)* przypisz zachowany stan wielomianu połączeń (pkt *2.2.1*).
   2.3. Zwiększ wartość licznika *N* o *1*.
3. Uzyskana wartość stanowi złożoność liniową ciągu S^n.

Zadania szczegółowe

1. Przygotuj implementację generatora ciągów pseudolosowych *LFSR*. Aplikacja powinna pozwalać na wybranie dowolnych sprzężeń zwrotnych. Ponadto, powinna umożliwiać określenie długości ciągu wyjściowego oraz oferować możliwość wyświetlenia danych i ich zapisu do pliku tekstowego (wariant: *„bity" oddzielone przecinkami*).
2. Korzystając z algorytmu *Berlekamp'a-Massey'a*, wyznacz wielomian opisujący dowolny, wygenerowany ciąg pseudolosowy. Przetestuj wybrane wyjście w ramach gotowej implementacji algorytmu (http://bma.bozhu.me/). Czy uzyskane wyniki są identyczne?
3. Napisz program, który pozwoli na znalezienie wielomianu opisującego sprzężenia zwrotne generatora *LFSR*, dla dowolnego ciągu wejściowego. Aplikacja powinna wizualizować kolejne etapy działania.
4.* Sporządź sprawozdanie z zajęć. Powinno ono obejmować:
   a. ogólną charakterystykę generatora *LFSR*,
   b. omówienie algorytmu *Berlekamp'a-Massey'a*, w tym przykład wyznaczenia wielomianu dla dowolnego wejścia,
   c. omówienie sposobu implementacji,
   d. odpowiedzi na postawione w instrukcji pytania,
   e. zestawienie przykładowych wyjść programów (*parametry generatora LFSR, wygenerowany ciąg, wyznaczona wartość wielomianu*) wraz ze stosownymi wnioskami,
   f. krótkie podsumowanie.