Berlekamp-Massey algorithm

IN: A sequence $\mathbf{s} = (s_0, s_1, \ldots, s_{N-1})$ of length N.

OUT: The shortest LFSR $< C(D), L >$ generating $\mathbf{s}$.

1. *Initilization* $C(D) = 1$, $L = 0$, $C^*(D) = 1$, $d^* = 1$, $m = -1$, $n = 0$.
2. While $(n < N)$ do the following:
   - 2.1 Compute the discrepancy
   $$d = s_n - \sum_{i=1}^{L} -c_i s_{n-i}.$$
   - 2.2 If $d \neq 0$ do the following:
     - $T(D) = C(D)$, $C(D) = C(D) - d \cdot (d^*)^{-1} \cdot C^*(D) D^{n-m}$.
     - If $L \leq n/2$ then $L = n + 1 - L$, $C^*(D) = T(D)$, $d^* = d$, $m = n$.
   - 2.3 $n = n + 1$.
3. Return $< C(D), L >$