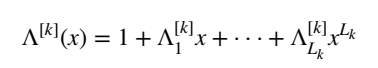
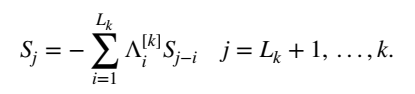
## BM Decoding algorithm

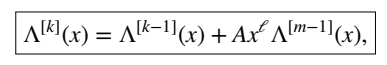
## Berlekamp-Massey algorithm basic

The BMA is based on the connection polynomial and LFSR which produces syndromes:





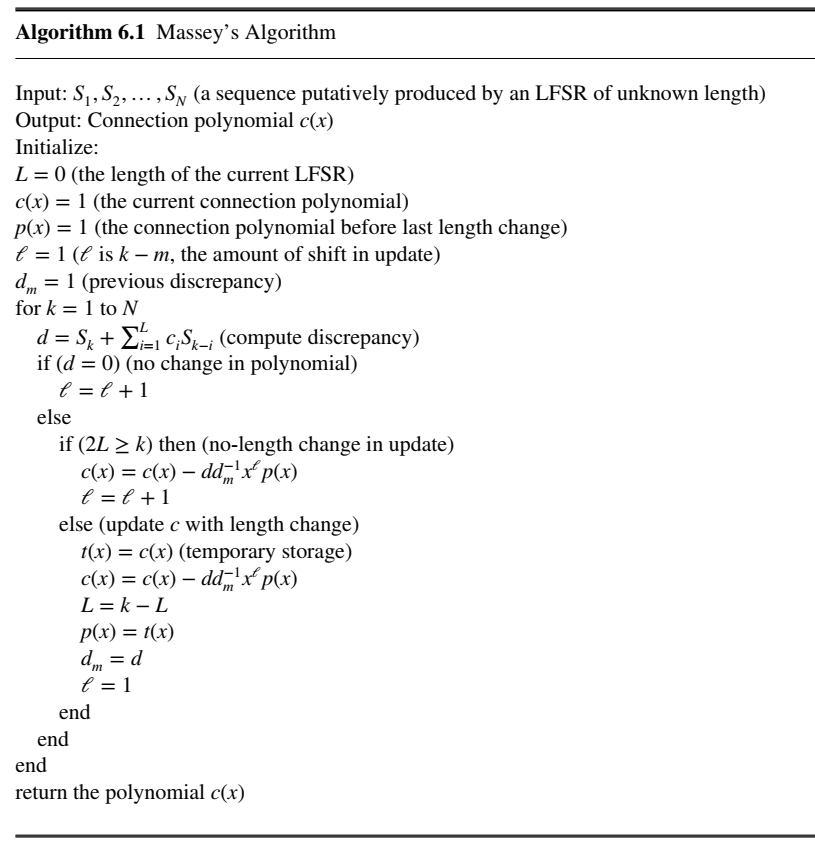
If the output of LFSR at stage k cannot be satisfied, the connection polynomial should be updated. The key of updating connection polynomial is:



The LFSR which produces the desired sequence has the shortest length because of the property of its recursiveness. That can be proved with inductive hypothesis (see Todd K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, Theorem 6.28 and Theorem 6.29).

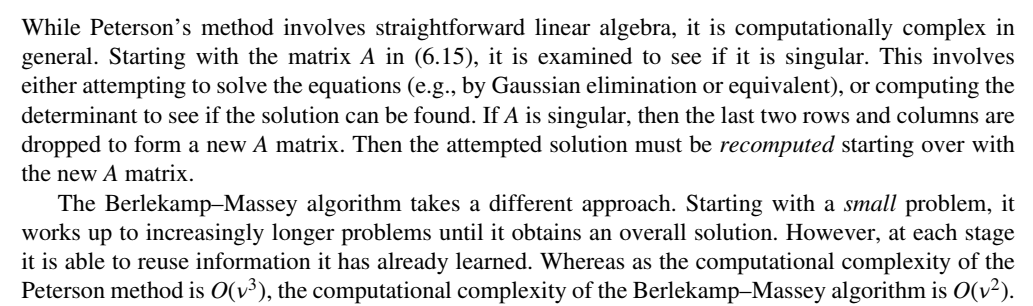
The updating method with length-change is different from that with no-length-change.

## Decoder Architectures



There is another BMA, called riBM which is described in: Zhang Xinmiao, *VLSI architectures for modern error-correcting codes*, section 4.4.3. It replaces the inverting calculation by another calculator.

## Complexity Analysis



(Notice the computational complexity of PGZ algorithm in that book is different from that in Xinmiao Zhang’s book. This should be checked later.)

## Example

