

# Quiz 7

The Berlekamp–Massey algorithm is an algorithm that will find the shortest linear feedback shift register (LFSR) for a given binary output sequence.

The algorithm will also find the minimal polynomial of a linearly recurrent sequence in an arbitrary field.

1. Please write a program based on Berlekamp–Massey algorithm to find the shortest linear feedback shift register (LFSR) for the given sequence down below.

- 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1

Please refer <http://bma.bozhu.me/>

# Quiz 7

2. Find the sequence generation rule of 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610.....

### 3. Extra credit

Use Berlekamp–Massey algorithm to find out the sequence rule of 0, 1, 1, 2, 3, 5, 8, 13, 21, 34

**HINT** 0, 1, 1, 2, 3, 5, 8, 13, 21, 34...

$$s(x) = x^8 + x^7 + 2x^6 + 3x^5 + 5x^4 + 8x^3 + 13x^2 + 21x + 34$$

$$r(x) = x^9$$

欲求次數小的 $c(x)$  使得  $f(x)r(x) + c(x)s(x) = b(x)$  ,  $\deg b < \deg c$

列表

算式

	$f(x)$	$c(x)$	$b(x)$
(1)	1	0	$x^9$
(2)	0	1	$x^8 + x^7 + 2x^6 + 3x^5 + 5x^4 + 8x^3 + 13x^2 + 21x + 34$