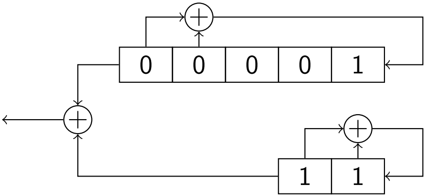
LFSRs: Math vs. mystery

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

A fourth example



These LFSRs produce $\overline{000010001100101011111}$ and $\overline{011}$ of periods 21 and 3.

Their sum gives

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
---------------------------------------------
  0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0
```

of period 21.

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
---------------------------------------------
  1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1
```

of period 7?

Our hypotheses would have predicted: 21, 21, 21, 21, 3, 1 and some more for the $2^5 - 21 - 1 = 10$ missing states in the first. But we do not get the fourth 21.

Some notation

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

Some notation

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

- Examples: $(x^n + 1)^* = x^n(x^{-n} + 1) = 1 + x^n$; $(f^*(x))^* = f(x)$.

Some notation

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

- Examples: $(x^n + 1)^* = x^n(x^{-n} + 1) = 1 + x^n$; $(f^*(x))^* = f(x)$.
- The generating function of a sequence $\{s_i\}_i$ is given by

$$S(x) = \sum_{i=0}^{\infty} s_i x^i.$$

Note: S depends on the starting state; there are 2^n different generating functions for an LFSR with state size n.

Some notation and helpful results

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

- Examples: $(x^n+1)^* = x^n(x^{-n}+1) = 1 + x^n$; $(f^*(x))^* = f(x)$.
- The generating function of a sequence $\{s_i\}_i$ is given by

$$S(x) = \sum_{i=0}^{\infty} s_i x^i.$$

  Note: S depends on the starting state; there are 2^n different generating functions for an LFSR with state size n.
- Claims: $\deg(P^*(x)S(x)) < n$.

Claim: $\deg(P^*(x)S(x)) < n$

Proof.

$$P^*(x)S(x) \quad = \quad \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right) \sum_{i=0}^{\infty} s_i x^i$$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right) \sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i$$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$
\begin{aligned}
P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i} x^i\right) \sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i} x^i \sum_{i=0}^{\infty} s_i x^i \\
&= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} c_{n-j} s_{i-j} \right) x^i + \sum_{i=n}^{\infty} \left(\sum_{j=0}^{n} c_{n-j} s_{i-j} \right) x^i
\end{aligned}
$$

□

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$
\begin{aligned}
P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i
\end{aligned}
$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j}$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$
\begin{aligned}
P^*(x)S(x) &= \left(1+\sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i
\end{aligned}
$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i$$

$$= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j} s_{k+n-j}$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i$$

$$= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j} s_{k+n-j}$
and rename $k + n = i$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$
\begin{aligned}
P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty} 0 \cdot x^i
\end{aligned}
$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j}s_{k+n-j}$
and rename $k + n = i$

Characterization of characteristic polynomial

This gives an alternative definition of the characteristic polynomial:

Lemma

Let $F(x)$ of $\deg(F) < n$ and $P(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ with $c_0 = 1$. Then the power series

$$S(x) = F(x)/P^*(x)$$

is the generating function of an LFSR with state size n satisfying $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j}$.

Proof computes $P^*(x)S(x)$.
Then observes that $\deg(F) < n$ forces cancellations as in previous proof.

A promised proof

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r.

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.
Remember from calculus: $\sum_{j=0}^{\infty} x^{jr} = 1/(x^r + 1)$.

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.
Remember from calculus: $\sum_{j=0}^{\infty} x^{jr} = 1/(x^r + 1)$.
Combine with previous lemma:

$$S(x) = F(x)/P^*(x) = \bar{S}(x)/(x^r + 1)$$

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.
Remember from calculus: $\sum_{j=0}^{\infty} x^{jr} = 1/(x^r + 1)$.
Combine with previous lemma:

$$S(x) = F(x)/P^*(x) = \bar{S}(x)/(x^r + 1)$$

rearrange, compute reciprocal, and remember $(x^r + 1)^* = x^r + 1$

$$F^*(x)(x^r + 1) = \bar{S}^*(x)P(x)$$

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.
Remember from calculus: $\sum_{j=0}^{\infty} x^{jr} = 1/(x^r + 1)$.
Combine with previous lemma:

$$S(x) = F(x)/P^*(x) = \bar{S}(x)/(x^r + 1)$$

rearrange, compute reciprocal, and remember $(x^r + 1)^* = x^r + 1$

degree $< n$ $\quad$ $F^*(x)(x^r + 1) = \bar{S}^*(x)P(x)$ $\quad$ irreducible of degree n

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.
Remember from calculus: $\sum_{j=0}^{\infty} x^{jr} = 1/(x^r + 1)$.
Combine with previous lemma:

$$S(x) = F(x)/P^*(x) = \bar{S}(x)/(x^r + 1)$$

rearrange, compute reciprocal, and remember $(x^r + 1)^* = x^r + 1$

degree $< n$ $\quad$ $F^*(x)(x^r + 1) = \bar{S}^*(x)P(x)$ $\quad$ irreducible of degree n

Thus $P(x)\big|(x^r + 1)$, i.e. $\mathrm{ord}(P) = \ell | r$.

A promised proof

Lemma

Let $P(x)$ with $\deg(P) = n$ be the characteristic polynomial of an LFSR. If $P(x)$ is irreducible and has order ℓ then all non-zero starting states give sequences of period ℓ.

Proof.

Let $\{s_i\}_i$ have period r. We know $r|\ell$.
Put $\bar{S}(x) = \sum_{i=0}^{r-1} s_i x^i$. Then $S(x) = \bar{S}(x)\left(1 + x^r + x^{2r} + \cdots\right)$.
Remember from calculus: $\sum_{j=0}^{\infty} x^{jr} = 1/(x^r + 1)$.
Combine with previous lemma:

$$S(x) = F(x)/P^*(x) = \bar{S}(x)/(x^r + 1)$$

rearrange, compute reciprocal, and remember $(x^r + 1)^* = x^r + 1$

degree $< n$ $\quad F^*(x)(x^r + 1) = \bar{S}^*(x)P(x)$ $\quad$ irreducible of degree n

Thus $P(x)\big|(x^r + 1)$, i.e. $\mathrm{ord}(P) = \ell|r$.

Together this gives $r = \ell$. □

Theorem

Let $\{s_i\}_i$ and $\{t_i\}_i$ be sequences from LFSRs with characteristic polynomials $P(x)$ and $Q(x)$.
There exists an LFSR with output matching $\{s_i + t_i\}_i$.
Its characteristic polynomial is $\mathrm{lcm}(P(x), Q(x))$.

Proof.

The generating function of the sum is

$$\sum (s_i + t_i)x^i = S(x) + T(x) = \frac{F(x)}{P^*(x)} + \frac{G(x)}{Q^*(x)} =$$

Theorem

Let $\{s_i\}_i$ and $\{t_i\}_i$ be sequences from LFSRs with characteristic polynomials $P(x)$ and $Q(x)$.
There exists an LFSR with output matching $\{s_i + t_i\}_i$.
Its characteristic polynomial is $\mathrm{lcm}(P(x), Q(x))$.

Proof.

The generating function of the sum is

$$\sum (s_i + t_i)x^i = S(x) + T(x) = \frac{F(x)}{P^*(x)} + \frac{G(x)}{Q^*(x)} =$$

$$\frac{a(x)F(x)}{\mathrm{lcm}(P^*(x), Q^*(x))} + \frac{b(x)G(x)}{\mathrm{lcm}(P^*(x), Q^*(x))} = \frac{a(x)F(x) + b(x)G(x)}{R^*(x)},$$

where $R(x) = \mathrm{lcm}(P(x), Q(x))$ (thus $R^*(x) = \mathrm{lcm}(P^*(x), Q^*(x))$),
$R^*(x) = a(x)P^*(x) = b(x)Q^*(x)$.

Theorem

Let $\{s_i\}_i$ and $\{t_i\}_i$ be sequences from LFSRs with characteristic polynomials $P(x)$ and $Q(x)$.
There exists an LFSR with output matching $\{s_i + t_i\}_i$.
Its characteristic polynomial is $\mathrm{lcm}(P(x), Q(x))$.

Proof.

The generating function of the sum is

$$\sum (s_i + t_i)x^i = S(x) + T(x) = \frac{F(x)}{P^*(x)} + \frac{G(x)}{Q^*(x)} =$$

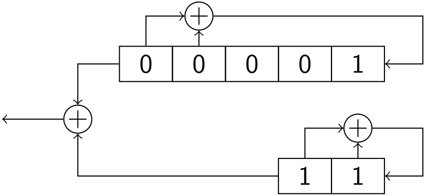
$$\frac{a(x)F(x)}{\mathrm{lcm}(P^*(x), Q^*(x))} + \frac{b(x)G(x)}{\mathrm{lcm}(P^*(x), Q^*(x))} = \frac{a(x)F(x) + b(x)G(x)}{R^*(x)},$$

where $R(x) = \mathrm{lcm}(P(x), Q(x))$ (thus $R^*(x) = \mathrm{lcm}(P^*(x), Q^*(x))$),
$R^*(x) = a(x)P^*(x) = b(x)Q^*(x)$.

$$\deg(a(x)F(x) + b(x)G(x)) < \deg(R)$$

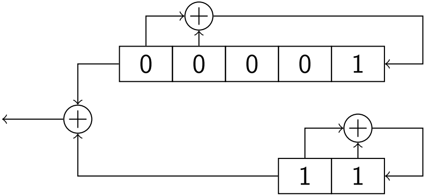
as $\deg(F) < \deg(P)$ and $\deg(G) < \deg(Q)$.
All this holds independent of the starting states. □

A mystery solved

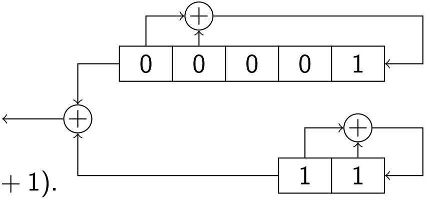


A mystery solved

The characteristic polynomials are $x^2 + x + 1$ and $x^5 + x + 1$.



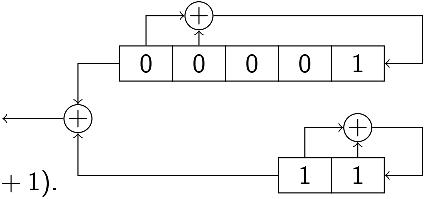
A mystery solved



The characteristic polynomials are $x^2 + x + 1$ and $x^5 + x + 1$.

The latter factors as
$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

A mystery solved

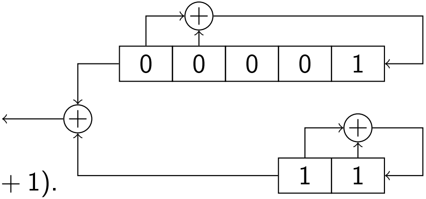


The characteristic polynomials are $x^2 + x + 1$ and $x^5 + x + 1$.

The latter factors as
$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

Thus their lcm is just $x^5 + x + 1$.

A mystery solved



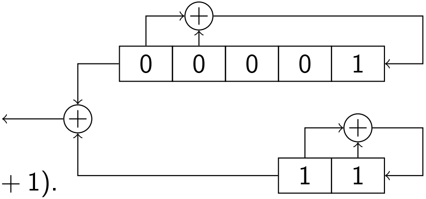
The characteristic polynomials are $x^2 + x + 1$ and $x^5 + x + 1$.

The latter factors as
$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

Thus their lcm is just $x^5 + x + 1$.

We're not missing a "fourth" 21 – there is only one!
All three sequences of period 21 would have turned out to be the same!

A mystery solved



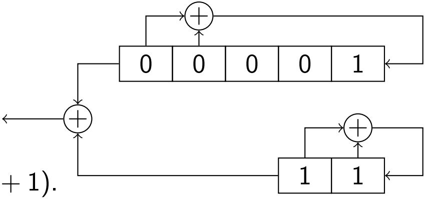
The characteristic polynomials are $x^2 + x + 1$ and $x^5 + x + 1$.

The latter factors as
$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

Thus their lcm is just $x^5 + x + 1$.

We're not missing a "fourth" 21 – there is only one!
All three sequences of period 21 would have turned out to be the same!
We also have sequences of periods 7,3, and 1, reaching 2^5.

A mystery solved



The characteristic polynomials are $x^2 + x + 1$ and $x^5 + x + 1$.

The latter factors as
$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

Thus their lcm is just $x^5 + x + 1$.

We're not missing a "fourth" 21 – there is only one!
All three sequences of period 21 would have turned out to be the same!
We also have sequences of periods 7,3, and 1, reaching 2^5.

Do the following to analyze LFSRs:

1. Factor the characteristic polynomial $P(x) = \prod f_i^{e_i}(x)$, for $f_i(x)$ irreducible, $f_i \neq f_j$, and $e_i > 0$.
2. Compute orders of $f_i^{e_i}(x)$.
3. Combine periods, taking care of offsets to get all periods. No cancellations because the f_i are co-prime.

Step 2 is different from what you did on sheet 2. Revisit LFSR (f).

Correct hypotheses

The following holds for LFSRs with co-prime characteristic polynomials.

- Adding LFSRs of max periods p and r gives period $\mathrm{lcm}(p, r)$.
- If the first LFSR has periods $p = 2^m - 1$ and 1 and the second LFSR has periods $r = 2^n - 1$ and 1, then
  - their sum has $\gcd(p, r)$ sequences of period $\mathrm{lcm}(p, r)$ (resulting from the $\gcd(p, r)$ different offsets)
  - and sequences of period p, r, and 1, from initializing one or both in the all-zero state.
  - These sum up to $\gcd(p, r) \cdot \mathrm{lcm}(p, r) + p + r + 1 = p \cdot r + p + r + 1$ $= (p + 1)(r + 1) = 2^m \cdot 2^n$, thus accounting for all 2^{m+n} states.
- If one or both do not have maximal periods we expect
  - $\gcd(p, r)$ sequences of period $\mathrm{lcm}(p, r)$
  - sequences of period p, r, and 1,
  - sequences from combinations of the other parts.