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

Simplify notation: put $c_n = 1$

Proof.

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

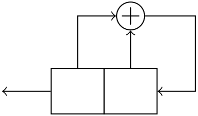
□

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 $k + n = i$

Example of proof

Using
$P(x) = x^2 + x + 1.$



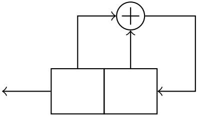
This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2).$
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Example of proof

Using
$P(x) = x^2 + x + 1.$



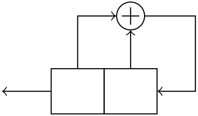
This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0$

Example of proof



Using
$P(x) = x^2 + x + 1$.

This LFSR produces output $\overline{011}$.

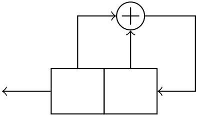
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x$

Example of proof

Using
$P(x) = x^2 + x + 1.$



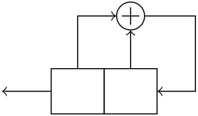
This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2).$
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2$

Example of proof



Using
$P(x) = x^2 + x + 1$.

This LFSR produces output $\overline{011}$.

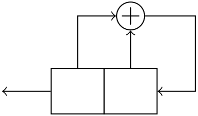
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2 + (1 + 1 + 0) \cdot x^3$

Example of proof

Using
$P(x) = x^2 + x + 1$.



This LFSR produces output $\overline{011}$.

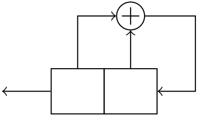
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2 + (1 + 1 + 0) \cdot x^3 + (1 + 0 + 1) \cdot x^4$

Example of proof

Using
$P(x) = x^2 + x + 1$.



This LFSR produces output $\overline{011}$.

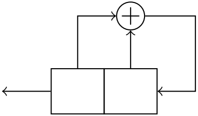
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2 + (1 + 1 + 0) \cdot x^3 + (1 + 0 + 1) \cdot x^4 + (0 + 1 + 1) \cdot x^5$

Example of proof

Using
$P(x) = x^2 + x + 1$.



This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2 + (1 + 1 + 0) \cdot x^3 + (1 + 0 + 1) \cdot x^4 + (0 + 1 + 1) \cdot x^5 + (1 + 1 + 0) \cdot x^6 \cdots$.

The coefficients of $x^2, x^3, \ldots$ match shifts of 011 because the coefficient vector of $P^*(x)$ is 111.
The coefficients of x^0 and x^1 have fewer terms because their degree is lower than $\deg(P)$.
That's why we need to treat them separately in

$$\sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i.$$