

# Extended windmill generators

Who? Cédric Lauradoux

When? ISIT 2009

# Primitive polynomials

Common practices for LFSRs

- **Trinomials:**

$$q(x) = x^m + x^i + 1.$$

- **Pentanomials:**

$$q(x) = x^m + x^i + x^j + x^k + 1.$$

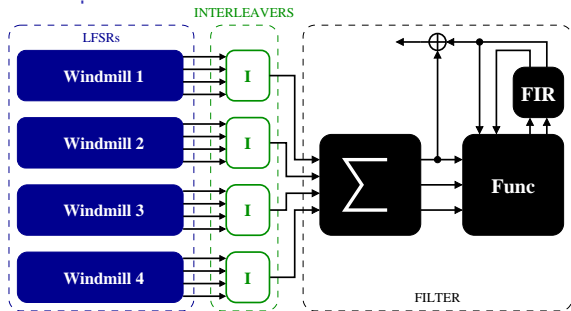
- **Windmill polynomials:**

$$q(x) = \alpha(x^v) + \beta(x^{-v})x^n.$$

Windmill generators were introduced by Smeets in 1988.

# Windmill polynomials

The E0 stream cipher



E0 polynomials:

$$q_1(x) = x^{25} + x^{20} + x^{12} + x^8 + 1$$

$$q_2(x) = x^{31} + x^{24} + x^{16} + x^{12} + 1$$

$$q_3(x) = x^{33} + x^{28} + x^{24} + x^4 + 1$$

$$q_4(x) = x^{39} + x^{36} + x^{28} + x^4 + 1$$

# Windmill polynomials

## Parallel generators

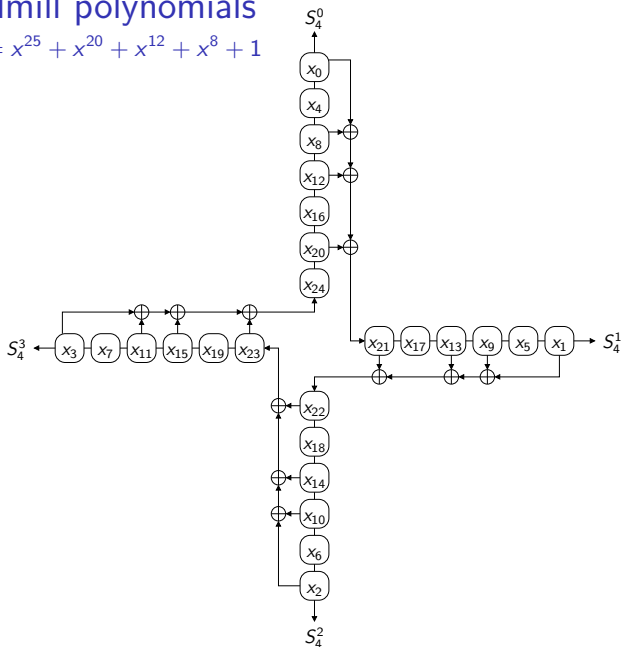
Example

*Linear congruential generator:*

$$X_{t+1} = aX_t + c \pmod n$$
$$X_{k(u+1)} = a^k X_{ku} + \left( \frac{a^k - 1}{a - 1} \right) \cdot c \pmod n.$$

# Windmill polynomials

$$q_1(x) = x^{25} + x^{20} + x^{12} + x^8 + 1$$



# Windmill polynomials

Numbers and limitations

Remark

*Estimation of the number of primitive windmill polynomials:*

$$\frac{2^{1+2\lfloor \frac{n}{v} \rfloor} \cdot \phi(2^n - 1)}{n \cdot 2^n}.$$

**[Smeets1989]**

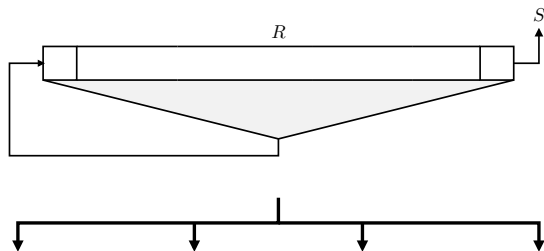
Theorem

*There is no irreducible windmill polynomials of degree  $n = 3 \bmod 8$  for  $v = 2^i$ .*

**[Chambers1989]**

# Extended windmill polynomials

Parallel FeedBack transform [Günther 1988]



# Extended windmill polynomials

PFB transform with  $q(x) = \alpha(x^v) + \beta(x^{-v})x^n$

- $\beta(x) = 1:$   $(n = 25, v = 4)$

- otherwise:

How is it working ?

# Extended windmill polynomials

How to choose the shift registers ?

Let consider the polynomial:

$$q(x) = \alpha(x^v) + \beta(x^{-v})x^n.$$

For the feedback function of  $R_j$ :

there is a contribution from  $R_i$  and from  $R_{\sigma(i)}$ .

$\sigma$  is a permutation of  $1, 2, \dots, v - 1$  :

$$\sigma(k) = nk + c \pmod{v}$$

Given  $n$  and  $v$ ,  $c$  is fixed and so  $\sigma$  is fixed too.

# Extended windmill polynomials

## New definition

Let consider the polynomial:

$$q(x) = \alpha(x^v) + \beta(x^{-v})x^{n-\phi} + x^n.$$

For the feedback function of  $R_j$ :

there is a contribution from  $R_{\sigma_1(i)}$  and from  $R_{\sigma_2(i)}$ .

$\sigma_1$  and  $\sigma_2$  are two permutations of  $1, 2, \dots, v-1$  :

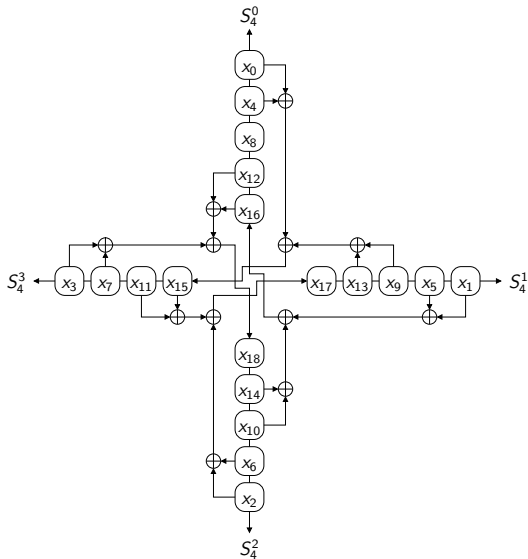
$$\begin{aligned}\sigma_1(k) &= nk + c \bmod v, \\ \sigma_2(k) &= n + k - \phi \bmod v,\end{aligned}$$

Given  $n$  and  $v$ ,  $\sigma_1$  is fixed.

Free choice for  $\sigma_2$ .

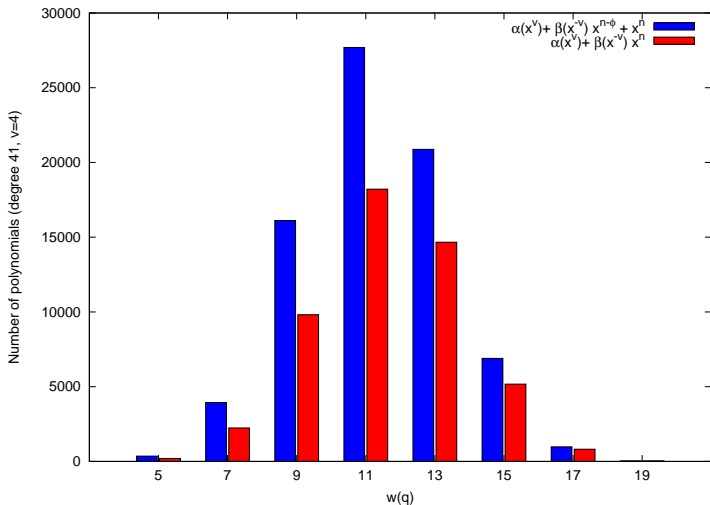
# Extended windmill polynomials

$$q(x) = x^{19} + x^{13} + x^9 + x^4 + 1$$



# Extended windmill polynomials

## Numbers and distribution I



# Extended windmill polynomials

## Numbers and distribution II

### Summary:

- for some degree  $n$ , up to  $\times 3$  on the number of polynomials;
- extended windmills for odd and even degree;
- extended windmills for  $n = 3 \pmod 8$ ;
- no estimation on the number of extended windmills;
- no extended windmills for  $n = 0 \pmod 8$ .

More informations, tables and polynomials on:

<http://www.info.ucl.ac.be/Bienvenue/PagesPersonnelles/lauradou/windmill.html>

# Conclusion

**Largest class of polynomials that defines a windmill**

**Generalization to non-linear feedback shift registers:**

- **Feedback with Carry Shift Registers (FCSR):**

$$q = \alpha + 2^{n-\phi}\beta + 2^n$$

with  $\alpha = \sum \alpha_i 2^{i\nu}$  and  $\beta = \sum \beta_j 2^{-j\nu}$ . (watermill)

- More generally, shift registers associated with **non-linear Boolean feedback functions**.

