Структури генераторів на основі зсувних регістрів з лінійною функцією зворотного зв'язку **LFSR** (Linear Feedback Shift Registers)

$$f(x) = x^{n} + c_{n-1} \cdot x^{n-1} + c_{n-2} \cdot x^{n-2} + \dots + c_{2} \cdot x^{2} + c_{1} \cdot x + 1$$

Схема з суміщеним зворотним зв'язком

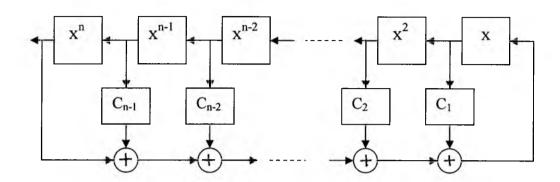
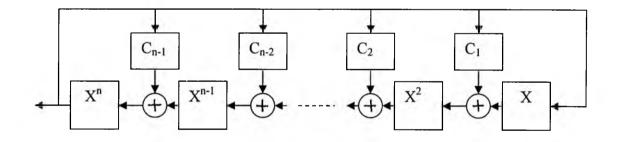


Схема з рознесеним зворотним зв'язком



Приклади простих поліномів

4: x^4+x^3+1	14: $x^{14}+x^{10}+x^6+x+1$	24: $x^{24}+x^7+x^2+x+1$
5: x^5+x^2+1	15: $x^{15}+x+1$	$25: x^{25}+x^3+1$
6: $x^6 + x + 1$	16: $x^{16}+x^{12}+x^3+x+1$	26: $x^{26}+x^6+x^2+x+1$
7: $x^7 + x^3 + 1$	17: $x^{17}+x^3+1$	27: $x^{27}+x^5+x^2+x+1$
8: $x^8 + x^4 + x^3 + x^2 + 1$	18: $x^{18}+x^7+1$	$28: x^{28} + x^3 + 1$
9: $x^9 + x^4 + 1$	19: $x^{19}+x^5+x^2+x+1$	29: $x^{29}+x^2+1$
$10: x^{10}+x^3+1$	20: $x^{20}+x^3+1$	$30: x^{30}+x^{23}+x^2+x+1$
$11: x^{11} + x^2 + 1$	21: $x^{21}+x^2+1$	$32: x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$
12: $x^{12}+x^6+x^4+x+1$	22: $x^{22}+x+1$	$33: x^{33} + x^{13} + 1$
13: $x^{13}+x^4+x^3+x+1$	23: $x^{23}+x^5+1$	64: $x^{64} + x^4 + x^3 + x + 1$

Конгруентні генератори $X_i = (X_{i-1} \cdot \mathbf{a} + \mathbf{b}) \bmod \mathbf{m}$

16: a=106 **b**=1283 **m**=6075 **32: a**=9301 **b**=49297 **m**=233280

Структури генераторів на основі зсувних регістрів з лінійною функцією зворотного зв'язку LFSR (Linear Feedback Shift Registers)

$$f(x) = x^{n} + c_{n-1} \cdot x^{n-1} + c_{n-2} \cdot x^{n-2} + \dots + c_{2} \cdot x^{2} + c_{1} \cdot x + 1$$

Схема з суміщеним зворотним зв'язком

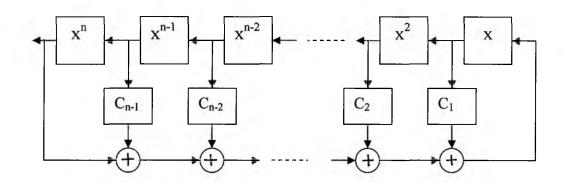
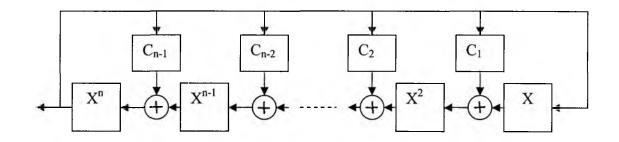


Схема з рознесеним зворотним зв'язком



Приклади простих поліномів

4: x^4+x^3+1 5: x^5+x^2+1 6: x^6+x+1 7: x^7+x^3+1 8: $x^8+x^4+x^3+x^2+1$ 9: x^9+x^4+1 10: $x^{10}+x^3+1$ 11: $x^{11}+x^2+1$ 12: $x^{12}+x^6+x^4+x+1$	14: $x^{14}+x^{10}+x^6+x+1$ 15: $x^{15}+x+1$ 16: $x^{16}+x^{12}+x^3+x+1$ 17: $x^{17}+x^3+1$ 18: $x^{18}+x^7+1$ 19: $x^{19}+x^5+x^2+x+1$ 20: $x^{20}+x^3+1$ 21: $x^{21}+x^2+1$	24: $x^{24}+x^7+x^2+x+1$ 25: $x^{25}+x^3+1$ 26: $x^{26}+x^6+x^2+x+1$ 27: $x^{27}+x^5+x^2+x+1$ 28: $x^{28}+x^3+1$ 29: $x^{29}+x^2+1$ 30: $x^{30}+x^{23}+x^2+x+1$ 32: $x^{32}+x^7+x^5+x^3+x^2+x+1$ 33: $x^{33}+x^{13}+1$
11. x + x + 1 12. x12 + x6 + x4 + x + 1 13. x13 + x4 + x3 + x + 1	21. x + x + 1 22. x22 + x + 1 23. x23 + x5 + 1	$33: x^{33} + x^{13} + 1$ $64: x^{64} + x^4 + x^3 + x + 1$

Конгруентні генератори $X_i = (X_{i-1} \cdot \mathbf{a} + \mathbf{b}) \bmod \mathbf{m}$

16: a=106 **b**=1283 **m**=6075 **32: a**=9301 **b**=49297 **m**=233280