

n	e	p_1	p_2	N
100	0.001	0.501	0.499	400.0
	0.01	0.510	0.490	400.2
	0.1	0.600	0.400	416.7
	0.2	0.700	0.300	476.2
1 000	0.001	0.501	0.499	4000.0
	0.01	0.510	0.490	4 001.6
	0.1	0.600	0.400	4 166.7
	0.2	0.700	0.300	4 761.9
10 000	0.001	0.501 ⁿ	0.499	40 000.2
	0.01	0.510	0.490	40 016.0
	0.1	0.600	0.400	41 666.7
	0.2	0.700	0.300	47 619.0

n Number of random numbers required.

e A zero bit occurs with probability $0.5 + e$

p_1 Probability of a 1-bit

p_0 Probability of a 0-bit

N Expected number of samples required.

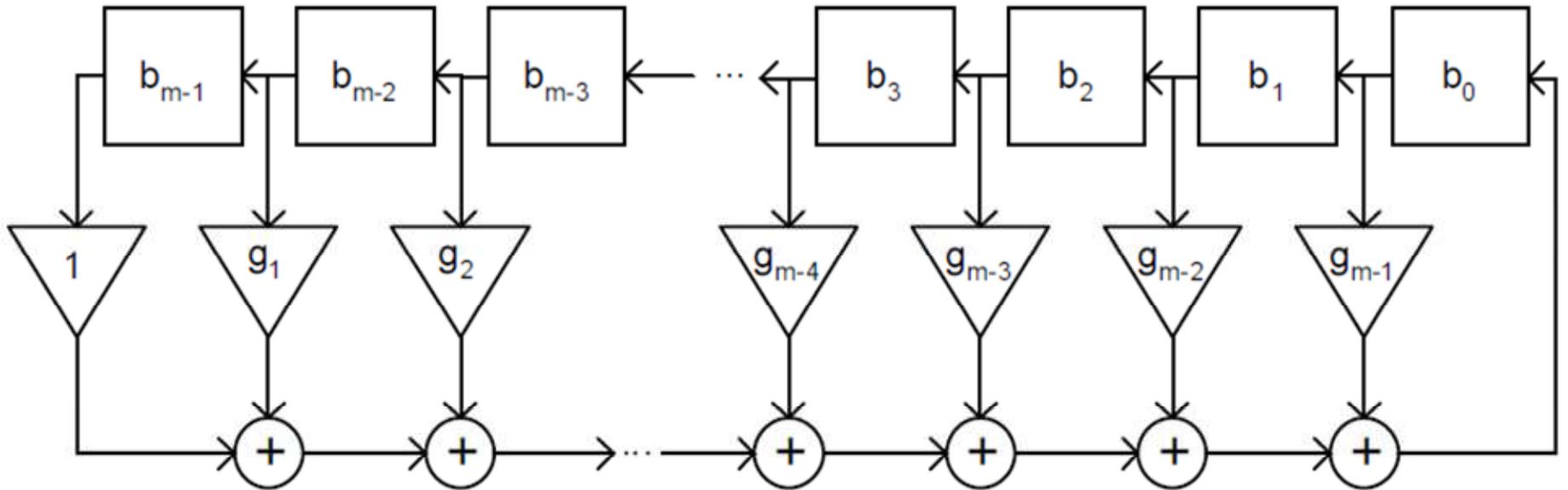


Figure 1: A generalized Fibonacci implementation of the linear feedback shift register.

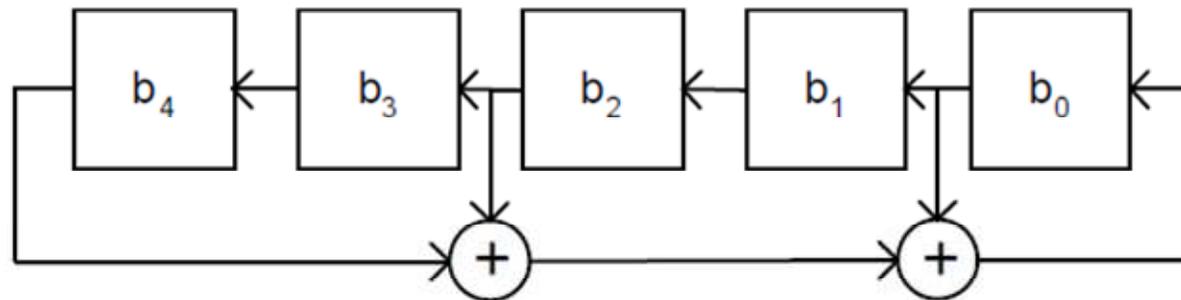


Figure 2: A Fibonacci implementation for the polynomial $p(x) = x^5 + x^4 + x^2 + 1$

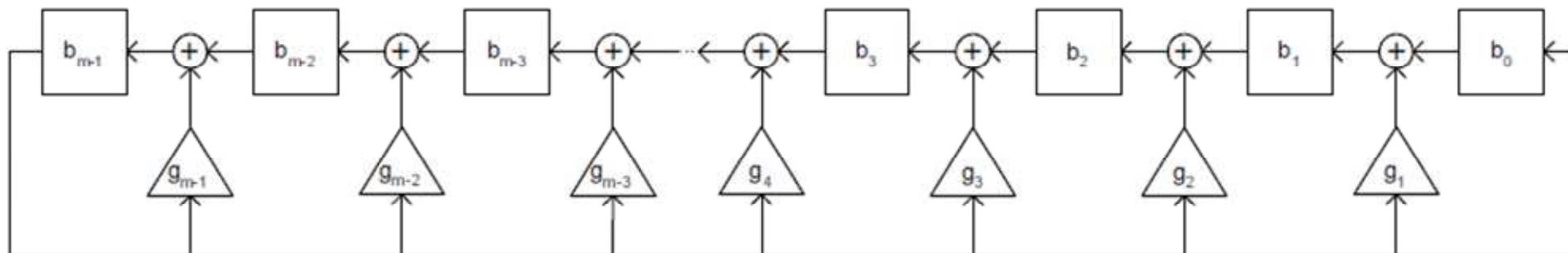


Figure 3: A generalized Galois implementation of the linear feedback shift register.

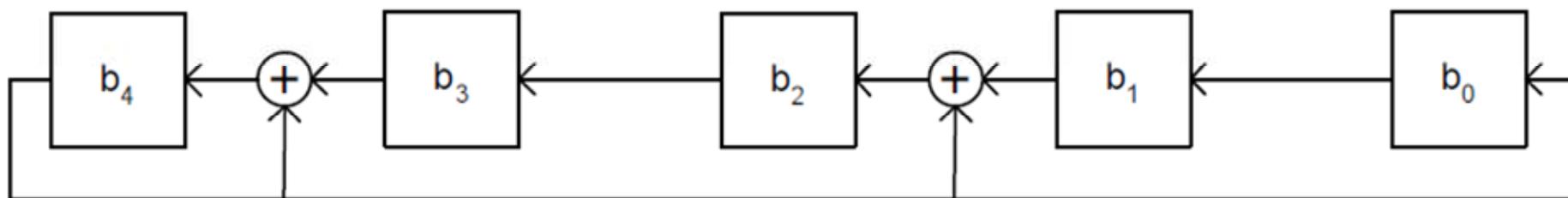


Figure 4: A Galois implementation for the polynomial $p(x) = x^5 + x^4 + x^2 + 1$

Number of Bits	Number of Taps	Tap Points
32	4	32, 31, 30, 10
	6	32, 31, 30, 29, 26, 16
	16	32, 31, 29, 26, 24, 23, 21, 18, 16, 15, 13, 10, 8, 7, 5, 1
30	4	30, 28, 27, 6
	6	30, 29, 28, 26, 24, 9
	16	30, 29, 26, 25, 23, 20, 19, 16, 14, 13, 10, 9, 8, 7, 4, 3
16	4	16, 14, 9, 4
	6	16, 15, 14, 11, 10, 6
	14	16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 3, 2

Table 1: Some useful m -sequences of various lengths. [3] The tap points indicate the terms in the polynomial that have non-zero coefficients. For example, tap points 32, 31, 30, and 10 correspond to the order-32 polynomial $p(x) = x^{31} + x^{30} + x^{10} + 1$.