

while the characteristic polynomials of the LFSRs in Figure 4.2 and Figure 4.3a are non-primitive. Primitive polynomials with a minimum number of non-zero coefficients are the desired characteristic polynomials for LFSRs to be used for TPGs in BIST applications. Table 4.1 gives primitive polynomials with minimum non-zero coefficients (and, therefore, minimum exclusive-OR gates) for degrees  $2 \leq n \leq 74$ .<sup>1</sup> As can be seen from the table, the minimum number of exclusive-OR gates required to implement any of these primitive polynomials is between 1 and 3.

**TABLE 4.1** Primitive polynomials through degree 74.

Degree ( $n$ )	Polynomial	Degree ( $n$ )	Polynomial
2, 3, 4, 6, 7, 15, 22, 60, 63	$x^n + x + 1$	12	$x^n + x^7 + x^4 + x^3 + 1$
5, 11, 21, 29, 35	$x^n + x^2 + 1$	33	$x^n + x^{13} + 1$
8, 19, 38, 43	$x^n + x^6 + x^5 + x + 1$	34	$x^n + x^{15} + x^{14} + x + 1$
9, 39	$x^n + x^4 + 1$	36	$x^n + x^{11} + 1$
10, 17, 20, 25, 28, 31, 41, 52	$x^n + x^3 + 1$	37	$x^n + x^{12} + x^{10} + x^2 + 1$
13, 24, 45, 64	$x^n + x^4 + x^3 + x + 1$	40	$x^n + x^{21} + x^{19} + x^2 + 1$
14, 16	$x^n + x^5 + x^4 + x^3 + 1$	42	$x^n + x^{23} + x^{22} + x + 1$
18, 57	$x^n + x^7 + 1$	46	$x^n + x^{21} + x^{20} + x + 1$
23, 47	$x^n + x^5 + 1$	54	$x^n + x^{37} + x^{36} + x + 1$
26, 27	$x^n + x^{12} + x^{11} + x + 1$	55	$x^n + x^{24} + 1$
30, 51, 53, 61, 70	$x^n + x^{16} + x^{15} + x + 1$	58	$x^n + x^{19} + 1$
32, 48	$x^n + x^{28} + x^{27} + x + 1$	65	$x^n + x^{18} + 1$
44, 50	$x^n + x^{27} + x^{26} + x + 1$	69	$x^n + x^{29} + x^{27} + x^2 + 1$
49, 68	$x^n + x^9 + 1$	71	$x^n + x^6 + 1$
56, 59	$x^n + x^{22} + x^{21} + x + 1$	72	$x^n + x^{53} + x^{47} + x^6 + 1$
66, 67, 74	$x^n + x^{10} + x^9 + x + 1$	73	$x^n + x^{25} + 1$

Like the counter, we are limited to values of  $n$  around 22 to 25 if we intend to run the full maximum length sequence in any reasonable amount of time. However, LFSRs are also good for output response analysis circuits (discussed in Chapter 5) which do not have the same size constraints. LFSRs with primitive characteristic polynomials are also the basic component in Cyclic Redundancy Check (CRC) circuits that are commonly used as on-line concurrent fault detection circuits, as will be discussed in Chapter 15 [122].

---

1. This number should be sufficient for most BIST applications encountered in practice but primitive polynomials for larger degrees can be found in [50] for  $n \leq 100$  and in [32] for  $n \leq 300$ .