MATHEMATICS OF COMPUTATION, VOLUME 26, NUMBER 120, OCTOBER 1972

Table of Irreducible Polynomials Over GF[2] of Degrees 10 Through 20*

By Svein Mossige

Abstract. The construction of the tables was based on linear recurring sequences over GF[2]. For each degree n, the polynomials are sorted with respect to their periods. Each polynomial is listed in octal representation with period and decimation.

In the present tables, all irreducible polynomials over GF[2] are given, with the period of their roots and its "decimation" (cf. below), from degree 10 through degree 20. Polynomials are listed in octal representation, such that each octal digit represents three binary digits. In the binary representation of the leftmost octal digit, the first 1 from the left is the coefficient of x^n. The binary equivalent of 2527 is 010101010111, and the corresponding polynomial is thus $x^{10} + x^8 + x^6 + x^4 + x^2 + x^1 + 1$. Of any pair consisting of a polynomial and its reciprocal polynomial, only that one is listed which has the smaller binary number representation.

For each degree n, the polynomials are sorted with respect to their periods, beginning with the primitive polynomials, of period $2^n - 1$. Within each period, the polynomials are arranged in lexicographical order. The decimation stands to the left of the octal representation.

For given degree n, the possible periods e are the divisors of $2^n - 1$, such that 2 belongs to the exponent $n \pmod e$. For given e, the number of different irreducible polynomials of degree n and period e is $\varphi(e)/n$. These polynomials are either all symmetric (self-reciprocal) or all nonsymmetric. Preceding the tables, the possible periods e are listed for each n, together with the numbers $\varphi(e)/n$. Since only one of a nonsymmetric polynomial and its reciprocal polynomial is given, the tables contain only $\frac{1}{2}\varphi(e)/n$ polynomials in the nonsymmetric cases.

The page indexing uses a double decimal number, where the first part shows the degree n.

The construction of the tables was based on linear recurring sequences over GF[2]. We describe the construction in the notation of Selmer [4].

For each degree n, one primitive polynomial $f(x)$ was chosen to represent the decimation 1.

If $f(\alpha) = 0$, $\alpha \in \mathrm{GF}[2^n]$, all the roots of $f(x)$ are given by α^{2^i}, $i = 0, 1, \cdots, n - 1$. The linear recurrence relation with characteristic polynomial $f(x)$ generates binary maximal recurring sequences $(s_t) = s_0, s_1, s_2, \cdots$. With an appropriate starting point, we get the "power sum sequence" $(\bar{s}_t)$, defined by

Received November 12, 1971.

AMS 1970 *subject classifications.* Primary 12C05, 12C10, 12-04.

Key words and phrases. Irreducible polynomals over GF[2], linear recurring sequences, period.

* The table is available for a nominal cost per copy from: Universitetet I Bergen, Matematisk Institutt, avd. A, 5014 Bergen, Norway. A copy has been placed in the UMT files of this journal.

$$\tilde{s}_t = \sum_{i=0}^{n-1} \alpha^{t \cdot 2^i}, \qquad t = 0, 1, 2, \cdots .$$

"Decimation" of $(\tilde{s}_t)$ by d means to pick every dth element:

$$(\tilde{s}_t)^{(d)} = \tilde{s}_0, \tilde{s}_d, \tilde{s}_{2d}, \cdots ,$$

of period

$$e = (2^n - 1)/(d, 2^n - 1),$$

and generated by the irreducible polynomial $f_d(x)$ which has α^d as a root. This polynomial has degree n if and only if 2 belongs to the exponent n (mod e), and only values of d satisfying this condition are permitted. Since $(\tilde{s}_t)$ is invariant under decimation by 2^h, $h = 0, 1, \cdots , n - 1$, $(\tilde{s}_t)^{(d)}$ exhausts the decimations of the complete cyclotomic coset $\{d \cdot 2^h\} = \mathcal{C}(d)$. Since further decimation by $-d$ gives the reciprocal polynomial $f_d^*(x)$ of $f_d(x)$, it suffices to choose one representative decimation from each "equivalence class" $\mathcal{C}(d) \cup \mathcal{C}(-d)$. Each time a new class was selected, the smallest unused d between 1 and 2^{n-1} was chosen to represent this class.

Knowing the first $2n$ elements of $(\tilde{s}_t)^{(d)}$, the coefficients of $f_d(x)$ can be determined by solving a set of linear congruences (mod 2), resulting from the corresponding recurrence relation. An extremely efficient method of solution has been developed by Berlekamp [1, p. 194].

A computer program was written in IBM 360/50H Assembler Language and run on the University of Bergen computer. The program consisted of the following main steps:

1. Given n and a primitive $f(x)$, generate and store $(\tilde{s}_t)$ as a bit string.

2. Each decimation d, one from each of the above-mentioned equivalence classes, are stored as a correctly placed bit in a bit string of length 2^{n-2}.

3. For each d, determine the corresponding period e, the first $2n$ elements of $(\tilde{s}_t)^{(d)}$ and use Berlekamp's algorithm to determine the coefficients of $f_d(x)$.

4. If $f_d(x)$ has a larger binary number representation than the reciprocal polynomial $f_d^*(x)$, replace $f_d(x)$ by $f_d^*(x)$ and d by the smallest number between 1 and $2^n - 1$ of the cyclotomic coset $\mathcal{C}(-d)$.

5. Sort and print in the desired layout of the tables.

For $n = 20$, the steps 1 through 4 used only 19 minutes of CPU time to determine all the 52377 irreducible polynomials. Step 5, however, took considerably more time.

Earlier tables. Peterson [3] gives all the irreducible polynomials over GF[2] of degree $\leqq 16$. For each n, the polynomials are sorted with respect to the decimation d, which is listed (but not the period e). His table also shows whether the roots of each $f_d(x)$ and/or its reciprocal polynomial are linearly dependent or independent.

Marsh [2] gives all the irreducible polynomials over GF[2] of degree $\leqq 19$. For each n, all the polynomials are listed lexicographically (in octal representation), with a letter indicating the period. The decimation did not enter into his computational method.

Department of Mathematics
University of Bergen
Bergen, Norway

1. E. R. BERLEKAMP, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968. MR **38** #6873.

2. R. W. MARSH, *Table of Irreducible Polynomials over* GF(2) *Through Degree* 19, NSA, Washington, 1957; Distributed by U.S. Dept. of Commerce, Office of Techn. Service, Washington 25, D.C.

3. W. W. PETERSON, *Error-Correcting Codes*, M.I.T. Press, Cambridge, Mass.; Wiley, New York, 1961. MR **22** #12003.

4. E. S. SELMER, *Linear Recurrence Relations Over Finite Fields.**

---

* Mimeographed lecture notes available for $5.00 from Department of Mathematics, University of Bergen, Norway.