Construction of Galois Fields of Characteristic Two and Irreducible Polynomials

By J. D. Swift

1. Introduction. The primary purpose of this paper is to provide a practical method of constructing Galois fields of characteristic 2 of large orders and thereby simultaneously give a practical way of generating a large supply of polynomials of high degree irreducible modulo 2. These polynomials are of special interest in connection with the theory of linear recursive sequences. See, for example [5]; some applications are suggested in [4].

The basic structure of Galois fields is extremely simple. For each prime q and each n there is one and (up to isomorphism) only one finite field of order q^n, designated by $GF(q^n)$. Its additive group is the elementary abelian group; the direct sum of n cyclic groups of order q. The multiplicative group of the non-zero elements is cyclic. The field $GF(q^{nm})$ may be constructed from a given $GF(q^n)$ by finding a polynomial of degree m, irreducible over $GF(q^n)$ and considering the set of polynomials with coefficients in $GF(q^n)$ modulis q and the irreducible polynomial. The subfields of $GF(q^n)$ are precisely $GF(q^d)$ where $d \mid n$; if g is a primitive generator of $GF(q^n)$, i.e. of the multiplicative subgroup of its non-zero elements, g^m is a primitive generator of $GF(q^d)$ where $m = (q^n - 1)/(q^d - 1)$.

These theorems, covered by many basic texts of algebra since the original work of L. E. Dickson [2], essentially dispose of the elementary theory of these fields. A particularly complete theory is contained in [1] which also has a bibliography listing a number of items from the extensive literature of the deeper arithmetic of the Galois fields. In general, results quoted without proof in this paper may either be found directly in [1] or are immediate consequences of statements proved therein.

From a practical standpoint, the only problems left by the structure theorems are those of finding an irreducible polynomial of degree m over the base field and of finding a primitive generator of the field with respect to this polynomial. In certain cases an irreducible polynomial is readily available and we are here concerned with the exploitation of these cases.

2. Cyclotomic polynomials over $GF(2)$. Let p be a prime for which 2 is a primitive root; then the cyclotomic polynomial $f_p(x) = (x^p + 1)/(x + 1)$ is irreducible over $GF(2)$. Thus for such primes the theory permits the realization of $GF(2^{p-1})$. Further, if g is a primitive generator of this field we may realize $GF(2^d)$ by considering powers of g^m, $m = (2^{p-1} - 1)/(2^d - 1)$ when $d \mid (p - 1)$. Since the only obvious restriction imposed on p by the condition that 2 be a primitive root of p is that $p \equiv \pm 3 \pmod 8$, it is likely that all fields $GF(2^n)$, $n \not\equiv 0 \pmod 8$, may be realized in this way for sufficiently large p. The smallest fields which cannot be constructed from polynomials listed in this paper are those for which $n = 8, 16, 17$.

If z is any element of $GF(2^n)$ the powers $z^0, z^1, \cdots, z^n$ will be linearly dependent over $GF(2)$ and the resulting relation of dependence $f(z) = 0$ will give an irreducible

Received October 19, 1959.

polynomial $f(z)$ if z does not lie in a proper subfield of $GF(2^n)$. If z is a primitive generator of $GF(2^n)$, $f(z)$ will be, by definition, primitive irreducible. All irreducible polynomials over $GF(2)$ may be constructed in this way.

By simple counting arguments we see that the number of irreducible polynomials of degree n is

$$\frac{1}{n}\left(2^n - \Sigma 2^{n/q_i} + \Sigma 2^{n/q_iq_j} - \cdots\right)$$

where the q_i are the distinct prime divisors of n. Similarly, the number of primitive irreducible polynomials of this degree is $(1/n)\varphi(2^n - 1)$ where φ is the Euler totient.

The actual problem of construction of these fields now reduces to finding a generator of the cyclic group. It is at this point that the theory carries us no further and resort must be taken to high speed computing machinery. It is easy to see that, for $p > 5$, any generator modulo the cyclotomic polynomial must be of degree at least 3. In particular, since $x^p = 1$, x and x^2 are of order p. To investigate the orders of the other linear and quadratic forms we study $z = x + 1/x$; define $h(z) = x^{-m}f_p(x)$ where $m = (p - 1)/2$; h is a polynomial of degree m in z. Thus z belongs to the sub-field $GF(2^m)$ and the order of z is a divisor of $2^m - 1$. Now $(x + 1)^2 = x^2 + 1 = xz$; thus the order of $x^2 + 1$ is a divisor of $p(2^m - 1)$ and the order of $x + 1$ is the same as that of its square. Again $x(x + 1)$ has the same order as $x + 1$. Finally $x^2 + x + 1 = x(z + 1)$ and $z + 1$ is also in $GF(2^m)$. Thus the order of all linear and quadratic forms divides $p(2^m - 1) < 2^{p-1} - 1$ for $p > 5$.

It is of interest to note that the order of z is precisely $2^m - 1$ for all suitable primes $p \leqq 139$ except for 37 and 101 for which it is $\frac{1}{3}$ the maximum.

We must, then, seek among the cubic or higher polynomials for our generators and we turn to a consideration of the computations by which this may be done.

3. The power routine. The primary tool in the investigation is a high-speed routine programmed for SWAC which finds prescribed powers of polynomials $F(x)$ modulis polynomials $G(x)$ and 2. The routine has two parts and the second part may be used as many times as desired without return to the first. The initial part receives $F(x)$ and $G(x)$ as inputs and computes n successive squares $(F(x))^2$, $(F(x))^4$, $\cdots$, $(F(x))^{2^n}$ where n is the degree of $G(x)$, reducing the results modulis 2 and $G(x)$. The last square is a check; if $G(x)$ is irreducible, $(F(x))^{2^n} = F(x)$. The second receives as input the exponent of the power of $F(x)$ desired, the upper limit being $2^n - 1$, and computes this power by multiplying together the appropriate stored powers from the first routine. The routines are quadruple precision and, since SWAC has a 36 bit word, degrees and powers are limited to 143 and $2^{143} - 1$ respectively. About $\frac{1}{2}$ second per multiplication is required in either routine. This means a maximum of 75 seconds for completion in either case.

To apply this routine to the problem of determining a primitive generator, $f_p(x)$ is used for $G(x)$ and possible generators are used as $F(x)$ in lexicographic succession. The exponents are $(2^{p-1} - 1)/q_i$ where q_i are the prime divisors of $(2^{p-1} - 1)$. (It is a fortunate circumstance that all necessary factorizations are known [3].) If the power of $F(x)$ is 1 for any of these exponents, $F(x)$ is not a primitive generator, and conversely. As a check the power is also calculated for $q_i = 1$; here the value must be 1. Table 1 lists the earliest primitive generator for each prime.

TABLE 1

Generating polynomials for $GF(2^{p-1})$*; to be used modulis* 2 *and* $(x^p + 1)/(x + 1)$

p	polynomial
3	x
5	$x + 1$
11	$x^3 + x + 1$
13	$x^3 + x + 1$
19	$x^4 + x + 1$
29	$x^5 + x^3 + x + 1$
37	$x^5 + x^2 + 1$
53	$x^4 + x + 1$
59	$x^3 + x + 1$
61	$x^3 + x + 1$
67	$x^5 + x^2 + 1$
83	$x^3 + x + 1$
101	$x^5 + x^4 + x^2 + x + 1$
107	$x^3 + x + 1$
131	$x^3 + x + 1$
139	$x^4 + x + 1$

4. Generators of subfields of the cyclotomic fields. There are 16 primes covered by Table 1. If subfields are considered, 24 additional fields may be constructed. Specifically, for each polynomial in Table 1 as $F(x)$ and its corresponding $f_p(x)$ as $G(x)$ we compute the $(2^{p-1} - 1)/(2^d - 1)$-th power of $F(x)$ for each divisor d of $p - 1$, $2 < d < p - 1$. The results are tabulated in Table 2. Here, in the largest case, the result is a polynomial of degree 138 and we have adopted a condensation of coefficients into octal notation to bring the result within manageable proportions. For example, $x^7 + x^5 + x^4 + x^2 + x + 1$ may be represented first by the ordered octuple of its coefficients: 10 110 111, and these may be read in groups of three as octal numbers. Thus the polynomial would appear as 267.

The polynomials of Table 2 are not necessarily the lexicographically earliest generators of their fields. It would be quite impossible to find such generators. However the disadvantages of polynomials of large degree are not as great as might be assumed at first thought. If a number of powers are to be computed, the full size of the registers is needed for the reduction modulo $f_p(x)$ and no more additions are needed to compute the irreducible polynomials than if the degrees were smaller. The only unavoidable disadvantage is the danger of an error in transcription. The entries in the table have been preserved against error by a comparison of output decks on successive runs and careful proofreading.

5. Utilization of generators to produce irreducible polynomials. As indicated in section 2, an irreducible polynomial is produced from an element z of $GF(2^n)$ not belonging to a proper subfield by finding the relation of dependence of $z^0, z^1, z^2, \cdots, z^n$. In one set of $n + 1$ registers are initially stored the powers of z. Another companion set is loaded initially with a single 1 in the ith place, $i = 0(1)n$. Whenever an operation is performed in one set of registers, the same is done to the companion set. By addition of other elements of the power registers the value 0 is obtained in the z^0 (or z^n) register. The irreducible polynomial is then read from

TABLE 2

Generating polynomials for proper sub-fields of $GF(2^{p-1})$. Fields are $GF(2^d)$ for $d \mid p-1$, $d \geqq 3$. Generators are to be used modulis 2 and $(x^p+1)/(x+1)$. See section 4 for use of octal notation to represent polynomials.

p	d	polynomial								
11	5									360
13	6									1760
	4									1156
	3									1321
19	9								4	77744
	6								1	26202
	3								7	63175
29	14								10777	77705
	7								6633	66330
	4								17577	56617
37	18							64	00000	00055
	12							75	23334	20271
	9							30	01030	20031
	6							71	22347	11234
	4							76	45677	73746
	3							75	23377	31274
53	26						117	77777	77777	77744
	13						117	42534	36165	21744
	4						26	50100	21003	22003
59	29						3777	77777	77777	77760
61	30						17777	77777	77777	77760
	20						17723	64723	51515	17760
	15						17003	60103	02017	00360
	12						34564	50135	07663	71022
	10						55263	06377	77143	15265
	6						14477	11710	23623	74461
	5						76200	51450	24624	01174
	4						36544	52035	07653	31207
	3						10124	50147	46024	52020
67	33					64	00000	00000	00000	00055
	22					75	24504	50000	00452	35255
	11					2	13043	36044	17304	32101
	6					25	46004	02150	47301	41023
	3					42	11170	41201	20436	22105
83	41				37	77777	77777	77777	77777	77760
101	50			1677	77777	77777	77777	77777	77777	77734
	25			1770	73777	77777	71554	77777	77776	70774
	20			1734	42260	36634	35312	16067	77653	36044
	10			620	20714	00420	64141	30210	01470	20231
	5			1000	60310	30220	00000	00220	60460	30004
	4			1667	35170	05511	25702	53322	77032	10443
107	53			37777	77777	77777	77777	77777	77777	77760
131	65		377	77777	77777	77777	77777	77777	77777	77760
	26			1634	45062	04144	04004	56032	04432	00042	36720
	13		1267	77723	45221	15105	11634	45045	44225	16277	77325
	10		6	52020	00200	22004	40100	66020	12043	06000	00030
	5		1727	52023	56373	62617	70360	77432	36763	56202	57274
139	69	4	77777	77777	77777	77777	77777	77777	77777	77777	77744
	46	4	76637	77731	75477	77777	77777	77775	47766	37777	54744
	23	4	72055	65424	32452	07006	07414	03412	45305	06566	41345
	6	1	57550	47372	56617	22064	32472	36641	62124	04335	10117
	3	3	50006	12434	15604	44500	03000	24444	16607	05214	00270

the companion register. The process can be carried out by systematic diagonalization.

As an example, we construct a primitive irreducible cubic using $z = x^9 + x^7 + x^6 + x^4 + 1$ (1321) for $p = 13$. We find $z^2 = x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x^2$ and $z^3 = x^9 + x^7 + x^6 + x^5$. The calculations can be arranged:

$$\begin{array}{llll} 1\colon 000 & 000 & 000 & 001 \\ z\colon 001 & 011 & 010 & 001 \\ z^2\colon 111 & 011 & 011 & 100 \\ z^3\colon 001 & 011 & 010 & 000 \end{array} \qquad \begin{array}{llll} 1\colon 000 & 000 & 000 & 001 \\ z^3+z\colon 000 & 000 & 000 & 001 \end{array}$$

$$z^3 + z + 1\colon 000 \quad 000 \quad 000 \cdot 000.$$

Specifically, z^2 is used (vacuously) to clear the first column; then discarded. The second column is now empty; z^3 is used to clear the third column and discarded. All but the last column are now clear and $z^3 + z$ is used to finish the job; the polynomial is $z^3 + z + 1$. Alternatively we could have started from 1 and the right hand column:

$$\begin{array}{llll} z+1\colon 001 & 011 & 010 & 000 \\ z^2\colon 111 & 011 & 011 & 100 \\ z^3\colon 001 & 011 & 010 & 000, \end{array}$$

$$\begin{array}{llll} z+1\colon 001 & 011 & 010 & 000 \\ z^3\colon 001 & 011 & 010 & 000 \end{array} \qquad z^3 + z + 1\colon 000 \quad 000 \quad 000 \quad 000.$$

The diagonalization process, while requiring large storage, is very rapid. No more than $2pn^2$ additions need be performed.

University of California
Los Angeles, California

1. A. A. ALBERT, *Fundamental Concepts of Higher Algebra*, University of Chicago, 1956.
2. L. E. DICKSON, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.
3. M. KRAITCHIK, *Introduction a la theorie des Nombres*, Paris, 1952.
4. R. PRICE & P. E. GREEN, JR., "A communication technique for multipath channels," *Proc.*, IRE, v. 46, 1958, p. 555.
N. ZIERLER, "Linear recursive sequences," Soc. Ind. Appl. Math., *Jn.*, v. 7, 1959, p. 31.