AN ITERATED QUADRATIC EXTENSION OF $GF(2)$

DOUG WIEDEMANN
University of Waterloo, Waterloo, Ontario, Canada

(Submitted November 1986)

1. A CONSTRUCTION

It is well known (see, for example, Ex. 3.96 of [1]) that the polynomials $x^{2\cdot 3^j} + x^{3^j} + 1$ are irreducible in $GF(2)[x]$ for $j = 0, 1, 2, \ldots$. Since

$$(x^{2\cdot 3^j} + x^{3^j} + 1)(x^{3^j} + 1) = x^{3^{j+1}} + 1$$

is a square-free polynomial, it follows that the period of each root of $x^{2\cdot 3^j} + x^{3^j} + 1$ is precisely 3^{j+1}, only one and a half times the degree of the polynomial. The field

$$C_j \approx GF(2)[x]/(x^{2\cdot 3^j} + x^{3^j} + 1) \approx GF(2^{2\cdot 3^j})$$

may be obtained by iterated cubic extensions beginning with $C_0 \approx GF(2)(x_0)$, where $x_0 \neq 1$ is a cube root of unity. We have $C_1 \approx C_0(x_1)$, where x_1 is any solution to $x_1^3 = x_0$. Iterating, $C_{j+1} \approx C_j(x_{j+1})$, where $x_{j+1}^3 = x_j$.

This paper deals with an iterated quadratic extension of $GF(2)$, whose generators are described by

$$x_{j+1} + x_{j+1}^{-1} = x_j \text{ for } j \geqslant 0, \text{ where } x_0 + x_0^{-1} = 1. \tag{1}$$

Let

$$E_0 \approx GF(2)(x_0),\ E_1 \approx E_0(x_1),\ \ldots,\ E_{j+1} \approx E_j(x_{j+1}).$$

Note that $x_0^2 + x_0 + 1 = 0$ has no root in $GF(2)$ so the first extension is quadratic. To show that each subsequent extension is quadratic, it need only be shown that the equation for x_{j+1}, which may be rewritten $x_{j+1}^2 + x_{j+1}x_j + 1 = 0$, has no root in E_j, for all $j \geqslant 0$. Although this follows almost immediately from theorems about finite fields, for example, Theorem 6.69 of Berlekamp [2], a more elementary proof will be given here. Let

$$Tr^{(n)}(x) = \sum_{i=1}^{2^n-1} x^{2^i}.$$

Also, let $|E|$ denote the order or number of elements of a finite field E.

Theorem 1: For $j \geqslant 0$, $x_{j+1} \notin E_j$, $|E_{j+1}| = 2^{2^{j+2}}$ and

$$Tr^{(j+2)}(x_{j+1}) = Tr^{(j+2)}(x_{j+1}^{-1}) = 1.$$

Proof (mathematical induction): Note $x_0 \notin GF(2)$ and $Tr^{(1)}(x_0) = Tr^{(1)}(x_0^{-1}) = 1$. The statement of the theorem is therefore true for $j = -1$ if E_{-1} is defined to be $GF(2)$. In a field of characteristic 2, assume $x^2 = xz + 1$. Then,

$$x^4 = x^2z^2 + 1 = xz^3 + z^2 + 1,\ x^8 = xz^7 + z^6 + z^4 + 1,$$

and, in general,

$$x^{2^k} = xz^{2^k - 1} + \sum_{i=1}^{k} z^{2^k - 2^i}.$$

Hence,

$$x_{j+1}^{2^{2^{j+1}}} = x_{j+1}x_j^{2^{2^{j+1}-1}} + x_j^{2^{2^{j+1}}}(Tr^{(j+1)}(x_j^{-1}))^2. \tag{2}$$

Now assume that the statement of the theorem holds for $j - 1$. Then E_j has order $2^{2^{j+1}}$ so, if x_{j+1} were in E_j, by the Fermat theorem and (2), $x_{j+1} = x_{j+1} + x_j(Tr^{(j+1)}(x_j^{-1}))^2$. But $Tr^{(j+1)}(x_j^{-1}) = 1$ by hypothesis, so, by contradiction, x_{j+1} is not in E_j itself but in a quadratic extension of E_j. The order of E_{j+1} is, therefore, $|E_j|^2 = 2^{2^{j+2}}$, using the second statement of the hypothesis.

Note that the other root to (1) for x_{j+1} is x_{j+1}^{-1}. Also, $Gal(E_{j+1}/E_j)$ has order 2 so, if σ denotes the nontrivial Galois automorphism, $\sigma(x_{j+1}) = x_{j+1}^{-1}$. Finally, $Tr^{(j+2)}$ is the trace map of E_{j+1} to $GF(2)$, so

$$Tr^{(j+2)}(x_{j+1}^{-1}) = Tr^{(j+2)}(x_{j+1}) = Tr^{(j+1)}(x_{j+1} + \sigma(x_{j+1})) = Tr^{(j+1)}(x_j) = 1$$

by the last part of the hypothesis, completing the statement of the theorem for j. ■

Corollary: $x_n^{F_n} = 1$, when $n \geqslant 0$ and $F_n = 2^{2^n} + 1$ is the Fermat number.

Proof: Define E_{-1} to be $GF(2)$. Since $|E_n| = 2^{2^{n+1}}$, the nontrivial member of $Gal(E_n/E_{n-1})$ is given by $\sigma_n(y) = y^{2^{2^n}}$. Since the conjugate of x_n over the field E_{n-1} is x^{-1}, $x_n^{2^{2^n}} = x_n^{-1}$. Thus, $x_n^{F_n} = 1$. ■

The order of a field element is defined to be the smallest nonnegative power which equals 1. In the case where F_n is prime, the above result implies that x_n has order F_n. In any case, the order of x_n divides F_n. Since the Fermat numbers are known to be mutually relatively prime, for example, see Theorem 16 of [3], the order of $x_nx_{n-1} \cdots x_0$ is the product of the orders of the x_i, $i \leqslant n$. We say an element of a field is primitive if its order is the same as the number of nonzero field elements. If the order of x_i is, in fact, F_i for $i \leqslant n$, then $x_nx_{n-1} \cdots x_0$ is a primitive element of E_n, because

$$F_nF_{n-1} \cdots F_0 = 2^{2^{n+1}} - 1 = |E_n| - 1.$$

We have not been able to determine if $x_nx_{n-1} \cdots x_0$ is always primitive.

2. BASIS SETS

There are several natural ways to construct a basis of E_n as a vector space over $GF(2)$. One such is of course the set of powers x_n^i, $0 \leqslant i < 2^{n+1}$, because $E_n = GF(2)(x_n)$ is a degree 2^{n+1} extension of $GF(2)$. Another basis is the collection of elements of the form $x_n^{\delta_n} \cdots x_0^{\delta_0}$, where each $\delta_i \in \{0, 1\}$. This can be shown by induction on n. Clearly, $x_0^0 = 1$ and x_0^1 span E_0. Since E_n is a quadratic extension of E_{n-1}, every member of E_n is uniquely expressible as $ax_n + b$, where $a, b \in E_{n-1}$. Assuming a and b can be expressed as sums of the $x_{n-1}^{\delta_{n-1}} \cdots x_0^{\delta_0}$, it follows easily that E_n is spanned by the $x_n^{\delta_n} \cdots x_0^{\delta_0}$. It immediately follows that these elements form a basis because the number of them is the same as the dimension of the space spanned.

Another basis consists of elements of the form $x_n^{\varepsilon_n} \cdots x_0^{\varepsilon_0}$, where $\varepsilon_i \in \{\pm 1\}$. This is shown by a similar argument which uses the fact that each element of E_n equals $ax_n + b = ax_n + cx_{n-1} = (a + c)x_n + cx_n^{-1}$ for some $a, b, c \in E_{n-1}$.

Theorem 2: The following are bases of E_n:

i) $x_n^{\delta_n} \cdots x_0^{\delta_0}$ $\quad \delta_i \in \{0, 1\}$ $\qquad$ ii) $x_n^{\varepsilon_n} \cdots x_0^{\varepsilon_0}$ $\quad \varepsilon_i \in \{-1, 1\}$

iii) $x_n^{2^i}$ $\quad 0 \leqslant i < 2^{n+1}$

Proof: It has already been shown that i) and ii) each form a basis. The elements iii) are the conjugates of x_n over $GF(2)$, and it will be shown that they are linearly independent. This will be done by induction. Certainly, x_0 and $x_0^2 = x_0 + 1$ are linearly independent over $GF(2)$. Assume that the conjugates of x_{n-1} in E_{n-1} are linearly independent. The transformation $\sigma_n(y) = y^{2^{2^n}}$ takes each conjugate of x_n to its reciprocal. If a combination of the conjugates vanishes, then grouping by reciprocal pairs gives

$$\sum_{i=0}^{2^n - 1} (\alpha_i x_n^{2^i} + \beta_i x_n^{-2^i}) = 0, \tag{3}$$

where $\alpha_i, \beta_i \in GF(2)$. Applying σ_n to both sides interchanges α_i and β_i. Adding this to the original equation gives

$$0 = \sum_{i=0}^{2^n - 1} (\alpha_i + \beta_i)(x_n^{2^i} + x_n^{-2^i}) = \sum_{i=0}^{2^n - 1} (\alpha_i + \beta_i) x_{n-1}^{2^i}.$$

By the inductive hypothesis, $\alpha_i + \beta_i \equiv 0$. Thus, the sum (3) can be rewritten:

$$\sum_{i=0}^{2^n - 1} \alpha_i x_{n-1}^{2^i};$$

this time the hypothesis implies $\alpha_i \equiv \beta_i \equiv 0$. Thus, iii) forms a basis. ■

In some sense the most interesting is the basis i) because the set for E_{n-1} is contained in the set for E_n. Therefore, the union of all bases given by i) is a basis for the infinite field which is the union of all the E_n. Another interesting property of the basis i) is that every boolean polynomial in n variables corresponds to an element of E_n. These boolean polynomials can be multiplied as elements of E_n in a straightforward if tedious manner. To multiply two such elements, collect all terms containing x_n to one side. Then using

$$(ax_n + b)(cx_n + d) = (acx_{n-1} + bc + ad)x_n + (ac + bd)$$

the product is computable in terms of a few products in E_{n-1}. Using this formula, it can be seen, though the proof is omitted, that the "degree" of the product of the two elements does not exceed the sum of their degrees. By the degree of a field element, we mean the degree of the associated boolean polynomial.

Each basis element of i) can be identified with the 0-1 vector, or bit vector, $(\delta_n, \ldots, \delta_0)$ which, in turn, can be identified with the integer

$$\delta_n 2^n + \cdots + \delta_0 2^0.$$

Let b_i be the basis element associated with the integer i. We now prove a fact regarding the expansion of a product of two basis elements as the sum of basis elements.

Theorem 3: For any i, j, and k the expansion of $b_i b_j$ contains b_k if and only if the expansion of $b_i b_k$ contains b_j.

Lemma: For all i and j, $b_i b_j$ contains the basis element $b_0 = 1$ if and only if $i = j$.

Proof of the Lemma: Once again, we use induction on n. Obviously, the Lemma holds whenever the two basis elements are in E_{-1}. Assume it holds whenever the two basis elements are in E_{n-1}. Now, in E_n, if both b_i and b_j are in E_{n-1}, the statement of the Lemma is true. If x_n is a factor of one but not the other, the product is in $x_n E_{n-1}$ and b_0 cannot occur in the expansion. If $b_i = x_n c$ and $b_j = x_n d$, where c, $d \in E_{n-1}$, then $b_i b_j = x_n x_{n-1} cd + cd$. The first term is in $x_n E_{n-1}$ and does not contain b_0. By hypothesis, the second term contains b_0 if and only if $c = d$, meaning $i = j$. This establishes the statement of the Lemma for E_n in all cases. ∎

Proof of Theorem 3: Consider the coefficient of b_0 in $(b_i b_j) b_k$. By the Lemma, it is the coefficient of b_k in $b_i b_j$. Since

$$(b_i b_j)b_k = (b_i b_k)b_j$$

it is also the coefficient of b_j in $b_i b_k$. ■

Corollary 1: Let $i \oplus j$ be the mod 2 sum of i and j as bit vectors. The coefficient of $b_{i \oplus j}$ in $b_i b_j$ is one.

Proof: Let $i \cap j$, $i \cup j$ be the bitwise AND, bitwise OR of i and j, respectively. It will be shown that the coefficient of b_0 in $b_{i \oplus j} b_i b_j$ is one which, together with the Lemma proves the Corollary. Now, by rearranging terms,

$$b_{i \oplus j} b_i b_j = (b_{i \oplus j} b_{i \cap j})^2 = (b_{i \cup j})^2,$$

and by the Lemma, this contains a b_0 in its expansion. ■

The following corollary is an immediate consequence of the Lemma.

Corollary 2: For any $a \in E_n$, a^2 contains b_0 in its expansion if and only if a is the sum of an odd number of basis elements.

3. MINIMAL POLYNOMIALS

The minimal polynomials over $GF(2)$ of the x_n are quite easy to compute. Starting with $p_0(y) = y^2 + y + 1$, let $p_1(y) = y^2 p_0(y + y^{-1})$ and, in general, $p_n(y) = y^{2^n} p_n(y + y^{-1})$. It is clear that $p_n(x_n) = 0$ for all n because

$$p_{k+1}(x_{k+1}) = x_{k+1}^{2^{k+1}} p_k(x_k) = 0.$$

Since p has degree 2^{n+1}, it is the minimal polynomial of x_n. The following result gives a method for computing the p_n which is probably better suited to calculation.

Theorem 4: Let sequences of polynomials $a_n(y)$ and $b_n(y)$ be defined as follows:

$$a_0 = 1 + y^2,\ b_0 = y \text{ and } a_{n+1} = a_n^2 + b_n^2,\ b_{n+1} = a_n b_n, \text{ for } n = 1, 2, 3, \ldots .$$

Then $a_n + b_n$ is the minimal polynomial of x_n.

Proof: Let $x_{-1} = 1$ and observe that, for $n \geqslant 0$, $y = x_{n+1}$ is a root of $a_0 + x_n b_0$ and, therefore, a root of

$$(a_0 + x_n b_0)(a_0 + x_n^{-1} b_0) = a_1 + x_{n-1} b_1.$$

If $n \geqslant 1$, $y = x_{n+1}$ is a root of

$$(a_1 + x_{n-1} b_1)(a_1 + x_{n-1}^{-1} b_1) = a_2 + x_{n-2} b_2.$$

After repeating this $n + 1$ times, we see that $y = x_{n+1}$ is a root of $a_{n+1} + b_{n+1}$. It follows from the definition that a_n has degree 2^{n+1} and that b_n has degree

$2^{n+1} - 1$. Thus, $a_n + b_n$ has degree 2^{n+1} with x_n as a root, so it must be the minimal polynomial of x_n. ■

4. EXPERIMENT

The numbers F_0, F_1, F_2, F_3, F_4 are prime so, by the Corollary to Theorem 1, x_n has order F_n for $n \leqslant 4$. In addition, using the complete factorizations [4, 5] of F_n for $5 \leqslant n \leqslant 8$, it has been checked on a computer that $x_{n_k} \neq 1$ for any proper divisor k of F_n for $n \leqslant 8$. It would be desirable to know whether x_n always has order F_n. If this is true, then $y_n = x_{n-1} \ldots x_0$ is primitive. It would be useful to have a good way to compute the minimal polynomials of the y_n.

5. A FIELD USED BY CONWAY

J. H. Conway has given an iterated quadratic extension [6, 7] of $GF(2)$ that comes from the theory of Nim-like games. In our terminology, this extension would be defined by

$$c_n^2 + c_n = c_{n-1} \ldots c_0 \text{ for } n \geqslant 1 \quad \text{and} \quad c_0^2 + c_0 = 1.$$

It is well known that any two finite fields of the same order are isomorphic. However, we do not yet know of an explicit isomorphism between $GF(2)(x_n)$ and $GF(2)(c_n)$.

ACKNOWLEDGMENT

The author would like to thank Norman Herzberg and Neal Zierler for their assistance.

REFERENCES

1. R. Lidl & H. Niederreiter. *Introduction to Finite Fields and Their Applications.* Cambridge: Cambridge University Press, 1986.
2. E. R. Berlekamp. *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.
3. G. H. Hardy & E. M. Wright. *The Theory of Numbers.* Oxford: Oxford University Press, 1971. Fourth Edition.
4. R. P. Brent & J. M. Pollard. "Factorization of the Eighth Fermat Number." *Math. Comp.* **36** (1981):627-630.
5. J. C. Hallyburton, Jr., & J. Brillhart. "Two New Factors of Fermat Numbers." *Math. Comp.* **29** (1975):109-112; see also Corrigenda, *Math. Comp.* **30** (1976):198.
6. J. H. Conway. *On Numbers and Games.* New York: Academic Press, 1976.
7. J. H. Conway & N. J. A. Sloane. "Lexicographic Codes: Error-Correcting Codes from Game Theory." *IEEE Transactions on Information Theory* **32** (May 1986).

◆◇◆◇◆