IRREDUCIBLE POLYNOMIALS OF MAXIMUM WEIGHT

OMRAN AHMADI AND ALFRED MENEZES

Abstract. We establish some necessary conditions for the existence of irreducible polynomials of degree n and weight n over $\mathbb{F}_2$. Such polynomials can be used to efficiently implement multiplication in $\mathbb{F}_{2^n}$. We also provide a simple proof of a result of Bluher concerning the reducibility of a certain family of polynomials.

1. Introduction

Let q be a prime power, and let $I_q(n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$. It is well known that $I_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}$ where μ is the Möbius function, and that $I_q(n) \approx \frac{q^n}{n}$. Many researchers have studied the distribution of irreducible polynomials having certain properties. In particular, much work has been done on the existence and distribution of irreducible trinomials over $\mathbb{F}_2$; for example see [15, 3, 4] and the references therein. The following theorem, due to Swan, is an important result about the non-existence of irreducible trinomials over $\mathbb{F}_2$.

Theorem 1. [15] Let $n > m > 0$ and assume that exactly one of n, m is odd. Then $x^n + x^m + 1$ has an even number of irreducible factors over $\mathbb{F}_2$ if and only if

(i) n is even, m is odd, $n \neq 2m$, and $nm/2 \equiv 0, 1 \pmod 4$.
(ii) n is odd, m is even, $m \nmid 2n$, and $n \equiv \pm 3 \pmod 8$.
(iii) n is odd, m is even, $m \mid 2n$, and $n \equiv \pm 1 \pmod 8$.

The case where n and m are both odd can be reduced to the case m even by considering $x^n + x^{n-m} + 1$.

For example, if $n \equiv 0 \pmod 8$ then Theorem 1(i) says that $x^n + x^m + 1$ has an even number of irreducible factors. Thus there does not exist an irreducible trinomial of degree n over $\mathbb{F}_2$ when $n \equiv 0 \pmod 8$.

There is overwhelming evidence in support of the conjecture that there exists an irreducible pentanomial of degree n over $\mathbb{F}_2$ for each $n \geq 4$ [11]; however existence has not yet been proven.

More generally, one can ask about the existence of an irreducible polynomial of degree n and weight t over $\mathbb{F}_2$ for each odd $t \in [3, n+1]$. (The weight of a polynomial is the number of its coefficients that are nonzero.)

Date: January 12, 2005.
Key words and phrases. Finite Fields, Irreducible Polynomials.

Shparlinski [12] and Ahmadi [1] respectively proved the existence of irreducible degree-n polynomials of weight $\frac{n}{4}+o(n)$ and $\frac{n}{2}+o(n)$ over $\mathbb{F}_2$. It is well known that there exists an irreducible degree-n polynomial of weight $n+1$ over $\mathbb{F}_2$ if and only if $n+1$ is prime (and hence n is even) and 2 is a generator of the multiplicative group of integers modulo $n+1$. In this paper, we consider the existence of irreducible degree-n polynomials of weight n (where n is odd) over $\mathbb{F}_2$.

The remainder of this paper is organized as follows. In Section 2 we show that irreducible polynomials of weight n can be used to implement fast multiplication in the field $\mathbb{F}_{2^n}$. In Section 3 we prove an analogue of Swan's theorem for weight-n polynomials over $\mathbb{F}_2$. The results of a computer search for irreducible polynomials of weight n are summarized in Section 4. In Section 5, we use the techniques of Section 3 to provide a simple proof of a theorem of Bluher about the reducibility of a certain family of polynomials over $\mathbb{F}_2$.

2. Fast multiplication in $\mathbb{F}_{2^n}$

Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_2$. Then $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$ is a finite field of order 2^n, and $f(x)$ is called the reduction polynomial. Elements of $\mathbb{F}_{2^n}$ are canonically represented as polynomials in $\mathbb{F}_2[x]$ of degree less than n. Multiplication of $a(x), b(x) \in \mathbb{F}_{2^n}$ can be performed by first computing the polynomial product $c(x)$ of $a(x)$ and $b(x)$, and then reducing $c(x)$ modulo $f(x)$. The reduction operation is considerably faster if $f(x)$ has small weight and if its middle terms (the nonzero terms not including the end terms x^n and 1) are close to each other and preferably all have small degree (see [9, Section 2.3.5]).

Another strategy for fast reduction is to select $f(x)$ so that it has a low-weight multiple $g(x)$ of degree slightly greater than n. Multiplication is then performed modulo $g(x)$, followed by a reduction by $f(x)$ whenever a representation in canonical form is desired. This strategy of using a redundant representation has been pursued by several authors; e.g., see [13, 6, 16]. For the case of weight-n polynomials, we have $f(x) = F_{n,m}(x)$ where

$$F_{n,m}(x) = x^n + x^{n-1} + \cdots + x^{m+1} + x^{m-1} + \cdots + x + 1 = \frac{x^{n+1}+1}{x+1} + x^m \tag{1}$$

and we can take

$$g(x) = (x+1)f(x) = x^{n+1} + x^{m+1} + x^m + 1.$$

The weight of $g(x)$ is 4, and its middle terms are consecutive. If m is small, then the middle terms also have small degree. Reduction using $g(x)$ instead of $F_{n,m}(x)$ can be as efficient as if the reduction polynomial were a trinomial or a pentanomial.

We illustrate the reduction operation with an example. The polynomial $F_{223,10}(x)$ is irreducible over $\mathbb{F}_2$ and therefore can be used as the reduction polynomial for $\mathbb{F}_{2^{223}}$. We have $g(x) = x^{224} + x^{11} + x^{10} + 1$. Let $c(x) = \sum_{i=0}^{446} c_i x^i$ be the product of two polynomials each of degree less than 224. On a 32-bit machine, $c(x)$ may be stored in an array $(C[13], C[12], \ldots, C[0])$ of 32-bit words, where the rightmost bit of $C[0]$ is c_0, the second leftmost bit of $C[13]$ is c_{446}, and the leftmost bit of $C[13]$ is unused (always set to 0). The high-order bits of $c(x)$ can be reduced modulo $g(x)$ one word at a time starting with $C[13]$. The pseudocode for the reduction operation is short and simple:

For i from 13 downto 7 to:
- $T \leftarrow C[i]$.
- $C[i-7] \leftarrow C[i-7] \oplus T \oplus (T \ll 10) \oplus (T \ll 11)$.
- $C[i-6] \leftarrow C[i-6] \oplus (T \gg 22) \oplus (T \gg 21)$.

The result is $(C[6], C[5], \ldots, C[0])$. Here, $\oplus$ denotes bitwise exclusive-or, $U \gg j$ is the right shift of U by j positions, and $U \ll j$ is the left shift of U by j positions.

3. Non-existence results

Let K be a field, and let $F(x) \in K[x]$ be a polynomial of degree n with leading coefficient a. The discriminant of $F(x)$ is

$$\mathrm{Disc}(F) = a^{2n-2} \prod_{i<j} (x_i - x_j)^2,$$

where $x_0, x_1, \ldots, x_{n-1}$ are the roots of $F(x)$ in some extension of K. We have $\mathrm{Disc}(F) \in K$. The following result, which is sometimes called the Stickelberger-Swan theorem, is our main tool for determining reducibility of a polynomial in $\mathbb{F}_2[x]$.

Theorem 2. [14, 15] Suppose that the degree-n polynomial $f(x) \in \mathbb{F}_2[x]$ is the product of r pairwise distinct irreducible polynomials over $\mathbb{F}_2$. Then $r \equiv n \pmod 2$ if and only if $\mathrm{Disc}(F) \equiv 1 \pmod 8$ where $F(x) \in \mathbb{Z}[x]$ is any monic lift of $f(x)$ to the integers.

If n is odd and $\mathrm{Disc}(F) \not\equiv 1 \pmod 8$, then Theorem 2 asserts that $f(x)$ has an even number of irreducible factors and therefore is reducible over $\mathbb{F}_2$. Thus one can find necessary conditions for the irreducibility of $f(x)$ by computing $\mathrm{Disc}(F)$ modulo 8.

Let $f(x), g(x) \in K[x]$. Let $f(x) = a \prod_{i=0}^{s-1}(x - x_i)$ and $g(x) = b \prod_{j=0}^{t-1}(x - y_j)$, where $a, b \in K$ and $x_0, x_1, \ldots, x_{s-1}$, $y_0, y_1, \ldots, y_{t-1}$ are in some extension of K. The resultant of $f(x)$ and $g(x)$ is

$$\mathrm{Res}(f, g) = (-1)^{st} b^s \prod_{j=0}^{t-1} f(y_j) = a^t \prod_{i=0}^{s-1} g(x_i). \tag{2}$$

We will use Lemma 3 to compute the discriminant of F.

Lemma 3. [7] Let K be a field, and let $F(x) \in K[x]$ have degree n. Suppose also that F is monic and $F(0) = 1$. Then

$$\operatorname{Disc}(F) = (-1)^{n(n-1)/2} \operatorname{Res}(F, nF - xF'),$$

where F' denotes the derivative of F with respect to x.

Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$, and let $x_0, x_1, \ldots, x_{n-1}$ be the roots of $f(x)$ in some extension of K. Then it is well known that the coefficients a_k are the elementary symmetric polynomials of x_i:

$$a_k = (-1)^k \sum_{0 \le i_1 < i_2 < \cdots < i_k < n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

for $1 \le k \le n$. Since each $a_k \in K$, it follows that $S(x_0, x_1, \ldots, x_{n-1}) \in K$ for any symmetric polynomial $S \in K[X_0, X_1, \ldots, X_{n-1}]$. Now for any integers k, p, q, let

$$s_k = \sum_{i=0}^{n-1} x_i^k \quad \text{and} \quad s_{p,q} = \sum_{\substack{i,j=0 \\ i \ne j}}^{n-1} x_i^p x_j^q. \tag{3}$$

Then $s_0 = n$ and

$$s_{p,q} = s_p s_q - s_{p+q}. \tag{4}$$

Note also that if $f(0) \ne 0$, then the power sum s_{-p} of $f(x)$ is equal to the pth power sum of its reciprocal, $x^n f(x^{-1})$. Newton's identity relates the coefficients a_k and power sums s_k.

Theorem 4. [10, Theorem 1.75] Let $f(x)$ and $x_0, x_1, \ldots, x_{n-1}$ be as above. Then for $1 \le k \le n$ we have

$$s_k + s_{k-1} a_1 + s_{k-2} a_2 + \cdots + s_1 a_{k-1} + k a_k = 0. \tag{5}$$

A polynomial $f(x) \in \mathbb{F}_2[x]$ having the property that $(x+1)f(x)$ has weight 4 is said to be of "tetranomial type." Note that polynomials of degree n and weight n are of tetranomial type. Hales and Newhart [7] obtained a Swan-like theorem for a certain subset of polynomials of "tetranomial type"[1]. Our main result is an analogue of Swan's theorem for all weight-n polynomials.

Theorem 5. Let $n > m > 0$ and assume that n is odd. Then $F_{n,m}(x) = (x^{n+1} + 1)/(x+1) + x^m$ has an odd number of irreducible factors over $\mathbb{F}_2$ if and only if one of the following conditions hold:

(i) $n \equiv 1 \pmod 8$ and either (a) $m \in \{2, n-2\}$; or (b) $m \equiv 0, 1 \pmod 4$ and $m \notin \{1, n-1, \frac{n-1}{2}, \frac{n+1}{2}\}$.

(ii) $n \equiv 3 \pmod 8$ and $m \in \{2, n-2\}$.

(iii) $n \equiv 5 \pmod 8$ and either (a) $m \in \{1, n-1\}$; or (b) $m \equiv 2, 3 \pmod 4$ and $m \notin \{2, n-2, \frac{n-1}{2}, \frac{n+1}{2}\}$ if $n > 5$.

[1] After completing this paper, we were informed that Hales and Newhart [8] have obtained a Swan-like theorem for all polynomials of tetranomial type. Theorem 2 of their paper implies our Theorem 5.

(iv) $n \equiv 7 \pmod 8$ and $m \notin \{2, n-2\}$.

Proof. Since $F_{n,m}(0) \neq 0$, we have $\gcd(F_{n,m}, F'_{n,m}) = 1$ and hence $F_{n,m}$ has no repeated factors. Let $g(x) = (x+1)F_{n,m}(x)$. Then $g(x)$ has degree $n+1$ and $G(x) = x^{n+1} + x^{m+1} + x^m + 1$ is a monic lift of $g(x)$ to $\mathbb{Z}[x]$.

Suppose now that $F_{n,m}(x)$ is the product of r pairwise distinct irreducible polynomials over $\mathbb{F}_2$. Then $g(x)$ is the product of $r+1$ pairwise distinct irreducible polynomials over $\mathbb{F}_2$. Hence, by Theorem 2, $n+1 \equiv r+1 \pmod 2$ or, equivalently, $n \equiv r \pmod 2$, if and only if $\mathrm{Disc}(G) \equiv 1 \pmod 8$. Thus the theorem can be proved by computing $\mathrm{Disc}(G)$.

First we apply Lemma 3 to $G(x)$. We see that

$$(n+1)G(x) - xG'(x) = (n-m)x^{m+1} + (n-m+1)x^m + (n+1).$$

Now setting $u = n-m$, $v = n-m+1$ and $w = n+1$, we have

$$\mathrm{Disc}(G) = (-1)^{n(n+1)/2}\,\mathrm{Res}(G, ux^{m+1} + vx^m + w). \tag{6}$$

Let $x_0, x_1, \ldots, x_n$ be the roots of $G(x)$ in some extension of the rational numbers. Using (6) and (2) we have

$$\mathrm{Disc}(G) = (-1)^{n(n+1)/2} \prod_{i=0}^{n} (ux_i^{m+1} + vx_i^m + w). \tag{7}$$

Let $D = (-1)^{(n+1)n/2}\,\mathrm{Disc}(G)$. Upon expanding the right hand side of (7) and using the fact that $\prod_{i=0}^{n} x_i = 1$, we have

$$\begin{aligned} D \ &= u^{n+1} + v^{n+1} + u^n v \sum_{i=0}^{n} x_i^{-1} + uv^n \sum_{i=0}^{n} x_i + u^{n-1}v^2 \sum_{i<j} x_i^{-1}x_j^{-1} \\ &\quad + u^2 v^{n-1} \sum_{i<j} x_i x_j + u^n w \sum_{i=0}^{n} (x_i^{-1})^{m+1} + v^n w \sum_{i=0}^{n} (x_i^{-1})^m \\ &\quad + u^{n-1}w^2 \sum_{i<j} (x_i^{-1}x_j^{-1})^{m+1} + v^{n-1}w^2 \sum_{i<j} (x_i^{-1}x_j^{-1})^m \\ &\quad + u^{n-1}vw \sum_{i\neq j} x_i^{-1}x_j^{-m-1} + uv^{n-1}w \sum_{i\neq j} x_i x_j^{-m} + S(x_0, x_1, \ldots, x_n), \end{aligned} \tag{8}$$

where $S(x_0, x_1, \ldots, x_n) \in \mathbb{Z}[x_0, x_1, \ldots, x_n]$. Since $\mathrm{Disc}(G)$ is a symmetric polynomial in $x_0, x_1, \ldots, x_n$ and all the terms given explicitly in the right hand side of equation (8) are symmetric polynomials, $S(x_0, x_1, \ldots, x_n)$ is also a symmetric polynomial in $x_0, x_1, \ldots, x_n$. The coefficients of the monomials of S have one of the following forms: (a) $u^i v^{n+1-i}$ with $3 \leq i \leq n-2$; (b) $u^i v^{n-i} w$ with $2 \leq i \leq n-2$; (c) $u^i v^j w^2$ with $i \geq 1$ and $j \geq 1$; or (d) $u^i v^j w^k$ with $k \geq 3$. Since n is odd and u, v are consecutive integers, we have $w \equiv uv \equiv 0 \pmod 2$ and so the coefficients of all monomials in $S(x_0, x_1, \ldots, x_n)$ are divisible by 8. Therefore $S(x_0, x_1, \ldots, x_n)$ is an integer divisible by 8. Also for any integer p we have $2\sum_{i<j} x_i^p x_j^p = \sum_{i\neq j} x_i^p x_j^p =$

$s_{p,p}$. Hence

$$\begin{aligned} D &\equiv u^{n+1} + v^{n+1} + u^n v s_{-1} + u v^n s_1 \\ &\quad + \frac{1}{2}(u^{n-1}v^2 s_{-1,-1} + u^2 v^{n-1} s_{1,1}) + u^n w s_{-m-1} + v^n w s_{-m} \\ &\quad + \frac{1}{2}(u^{n-1}w^2 s_{-m-1,-m-1} + v^{n-1} w^2 s_{-m,-m}) + u^{n-1} v w s_{-1,-m-1} \\ &\quad + u v^{n-1} w s_{1,-m} \pmod 8. \end{aligned}$$

Applying Newton's identity (5) to the polynomial $G(x)$ and its reciprocal, $x^{n+1}G(x^{-1})$, we can compute all the unknown terms in the above equation and thus evaluate $D \bmod 8$ for all permissible values of m and n.

For example, suppose that $n \equiv 7 \pmod 8$. Then $w \equiv 0 \pmod 8$ and

$$\begin{aligned} D &\equiv u^{n+1} + v^{n+1} + u^n v s_{-1} + u v^n s_1 + \frac{1}{2} u^{n-1} v^2 s_{-1,-1} \\ &\quad + \frac{1}{2} u^2 v^{n-1} s_{1,1} \pmod 8. \end{aligned}$$

We consider three cases.

(a) If $m \notin \{1, 2, n-2, n-1\}$, then (5) implies that $s_{-1} = s_{-2} = s_1 = s_2 = 0$. Since $s_{1,1} = s_1^2 - s_2$, we have $s_{1,1} = 0$ and similarly $s_{-1,-1} = 0$. Hence $D \equiv u^{n+1} + v^{n+1} \pmod 8$. Now since $n+1$ is even and one of u, v is even and the other is odd, we have $D \equiv 1 \pmod 8$.

(b) If $m = n-1$, then $s_1 = s_2 = -1$ and $s_{-1} = s_{-2} = 0$, so $s_{1,1} = s_1^2 - s_2 = 2$ and $s_{-1,-1} = s_{-1}^2 - s_{-2} = 0$. Hence $D \equiv u^{n+1} + v^{n+1} - uv^n + u^2 v^{n-1} \pmod 8$. Since $m = n-1$, we have $u = 1$, $v = 2$ and $D \equiv u^{n+1} \equiv 1 \pmod 8$. Similarly we have $D \equiv 1 \pmod 8$ if $m = 1$.

(c) If $m = n-2$, then $s_1 = s_{-1} = s_{-2} = 0$ and $s_2 = -2$ whence $s_{1,1} = 2$, $s_{-1,-1} = 0$, and $D \equiv u^{n+1} + v^{n+1} + u^2 v^{n-1} \pmod 8$. In this case since $u = 2$, v is odd, and $n-1$ is even, we have $D \equiv 5 \pmod 8$. Similarly we have $D \equiv 5 \pmod 8$ if $m = 2$.

Part (iv) of the theorem now follows since $\mathrm{Disc}(G) = D$ when $n \equiv 7 \pmod 8$.

The cases $n \equiv 1, 3, 5 \pmod 8$ are more tedious but can be handled in a similar way. □

Corollary 6. Let $n > m > 0$ and assume that n is odd. Suppose that $F_{n,m}(x) = (x^{n+1}+1)/(x+1) + x^m$ is irreducible over $\mathbb{F}_2$.

(i) If $n \equiv 1 \pmod 8$ then either $m \in \{2, n-2\}$ or $m \equiv 0, 1 \pmod 4$. Moreover, $m \notin \{1, n-1, \frac{n-1}{2}, \frac{n+1}{2}\}$.

(ii) If $n \equiv 3 \pmod 8$ then $m \in \{2, n-2\}$.

(iii) If $n \equiv 5 \pmod 8$ then either $m \in \{1, n-1\}$ or $m \equiv 2, 3 \pmod 4$. Moreover, if $n > 5$ then $m \notin \{2, n-2, \frac{n-1}{2}, \frac{n+1}{2}\}$.

(iv) If $n \equiv 7 \pmod 8$ then $m \notin \{2, n-2\}$.

4. Existence

Corollary 6 states that if $n \equiv 3 \pmod 8$ then $F_{n,m}(x)$ can only be irreducible if $m = 2$ or $m = n - 2$. A computer search shows that the only integers $n \in [3, 100000]$ congruent to 3 (mod 8) for which $F_{n,2}(x)$ is irreducible are $n \in \{3, 11, 35, 107, 195, 483, 1019, 2643\}$.

One would expect there to be more irreducibles $F_{n,m}(x)$ for $n \equiv 7 \pmod 8$ than for $n \equiv 1, 5 \pmod 8$ since Corollary 6 rules out only two values of m in the former case, and about half of all possible m in the latter case. This is reflected in Table 1 which lists all irreducible polynomials $F_{n,m}$ for $n \in [5, 340]$ and $n \equiv 1, 5, 7 \pmod 8$. Irreducibles $F_{n,m}(x)$ are more abundant than expected in the case $n \equiv 7 \pmod 8$. A computer search shows that the only $n \in [7, 5000]$ congruent to 7 (mod 8) for which no irreducible polynomial $F_{n,m}(x)$ exists are

$$n \in \{575, 823, 1543, 2063, 2103, 2335, 3439, 3607, 3847, 3895, 4167, 4375, 4567, 4911\}.$$

Blake, Gao and Lambert [4] observed experimentally that the number of irreducible trinomials of degree $\leq n$ is approximately $3n$. Similarly, we have noticed that the number of irreducible polynomials $F_{n,m}$ of degree $\leq n$ is approximately $2n$. Table 2 lists the total number of such polynomials for n belonging to consecutive intervals of length 200. There are approximately 400 irreducible polynomials in each interval, giving an average of approximately 2 irreducible weight-n polynomials for each degree n. An explanation for this phenomenon would be of interest.

5. A family of reducible polynomials over $\mathbb{F}_2$

Experimental evidence was provided in [2] that if $n \equiv \pm 3 \pmod 8$ and $f(x) = x^n + x^{m_1} + x^{m_2} + x^{m_3} + 1$ is an irreducible pentanomial over $\mathbb{F}_2$, where $m_1 > m_2 > m_3 > 0$ and m_1, m_2, m_3 are odd, then $m_1 \geq n/3$. (Such polynomials have the property that the corresponding polynomial basis has exactly one element of trace one.) Motivated by this observation Bluher [5] proved the following.

Theorem 7. [5] Let $n \equiv \pm 3 \pmod 8$. Let $I = \{i : i \text{ even}, 2n/3 < i < n\}$ and $J = \{j : j \equiv 0 \pmod 4, 0 < j < n\} \setminus I$. Then the polynomial

$$f(x) = x^n + \sum_{i \in I} a_i x^{n-i} + \sum_{j \in J} a_j x^{n-j} + 1 \quad \in \mathbb{F}_2[x]$$

is reducible over $\mathbb{F}_2$.

Bluher's proof involves computing $\mathrm{Disc}(F) \bmod 8$ using properties of determinants. Here we use Newton's identity to give a simpler proof similar to the one for Theorem 5.

n	m
5	1 2
13	1 3
21	–
29	6 11
37	1 3 6 10 15
45	7
53	6
61	22
69	–
77	30 34
85	1
93	22 35
101	6 18
109	–
117	14 19
125	6 31 38 46
133	22 31 46
141	67
149	6 43 55 70
157	3 46
165	–
173	43
181	67 75 78
189	34 62 71
197	11 27
205	–
213	26 67
221	35 74
229	39 63
237	59 86 94
245	3 87 102
253	42 70
261	34
269	7 95 123
277	90 130 135
285	127
293	47 131
301	6 66
309	–
317	58 90 134
325	–
333	62 86 103 107

n	m
7	1 3
15	1 4 7
23	1 6 8 10
31	3 6 7 13
39	4 7 11 19
47	1 3 8 16 17 18 19
55	9 12 16 19 24
63	1 5 11 31
71	9 14 20
79	16 22 27
87	4 28
95	4 7 28 44 46
103	7 37 43
111	19 34 43
119	9 13 15 24
127	1 7 15 30 63
135	28 58 62 64
143	40 41 68
151	46
159	5 7 17 37
167	6 17 32 43 56 57 72
175	18
183	1 35 56
191	23 42 69 76 77
199	3 60
207	11 53 83
215	7 18 44 59 78
223	10 22 60 106
231	82 94 97
239	9 11 15 29 49 51 77
247	10 42
255	52 56 82
263	23 51 62 81 128
271	36 84 91 99 108
279	37 47 52 56 59 79 80 100 101 109 130 131
287	6 59 69 93 95 104 131
295	6 58 102
303	50 133
311	25 62 66
319	72 76 82 105
327	19 110 217 308
335	53 96 117

n	m
9	2
17	4 5
25	4 9
33	–
41	5 12 16
49	4
57	8 16
65	16 21 28
73	–
81	2 25
89	5 17 32 33
97	4 12 36 45
105	17 32
113	16 36 37 41
121	–
129	–
137	20 33 41 44
145	12 33 57
153	52 56
161	65 73
169	–
177	41
185	12 53
193	21 61
201	32 88
209	5 8 24 81 96
217	–
225	16 37
233	36 100
241	48
249	–
257	68 72 84
265	24 129
273	68
281	20 21 36 105 113 133
289	100
297	28 112 133
305	72 121 184 233
313	28 285
321	44 277
329	53 276
337	21 316

TABLE 1. Irreducible $F_{n,m}(x) = (x^{n+1}+1)/(x+1) + x^m$ with $m \leq n/2$, for $5 \leq n \leq 340$ and $n \equiv 1, 5, 7 \pmod 8$. The three tables list n that are congruent to $5, 7, 1 \pmod 8$.

n	1	3	5	7	Total	Cumulative
3– 200	92	10	92	182	376	376
201– 400	96	0	112	220	428	804
401– 600	94	2	106	226	428	1232
601– 800	100	0	114	212	426	1658
801–1000	114	0	72	204	390	2048
1001–1200	86	2	120	202	410	2458
1201–1400	84	0	86	212	382	2840
1401–1600	114	0	90	206	410	3250
1601–1800	90	0	84	214	388	3638
1801–2000	116	0	94	192	402	4040
2001–2200	90	0	112	204	406	4446
2201–2400	116	0	112	194	422	4868
2401–2600	94	0	96	212	402	5270
2601–2800	96	2	88	200	386	5656
2801–3000	88	0	98	214	400	6056
3001–3200	84	0	112	202	398	6454
3201–3400	110	0	96	194	400	6854
3401–3600	112	0	116	176	404	7258
3601–3800	90	0	136	228	454	7712
3801–4000	108	0	130	204	442	8154
4001–4200	96	0	80	234	410	8564
4201–4400	104	0	102	210	416	8980
4401–4600	86	0	100	198	384	9364
4601–4800	96	0	112	214	422	9786
4801–5000	126	0	100	218	444	10230
5001–5200	114	0	140	156	410	10640
5201–5400	110	0	110	174	394	11034
5401–5600	94	0	94	216	404	11438
5601–5800	92	0	120	178	390	11828
5801–6000	104	0	100	222	426	12254
6001–6200	82	0	98	250	430	12684
6201–6400	104	0	110	178	392	13076
6401–6600	106	0	78	238	422	13498
6601–6800	78	0	120	216	414	13912
6801–7000	114	0	82	214	410	14322
7001–7200	102	0	64	168	334	14656
7201–7400	88	0	132	190	410	15066
7401–7600	92	0	142	188	422	15488
7601–7800	124	0	84	204	412	15900
7801–8000	114	0	102	180	396	16296

TABLE 2. The total number of irreducible polynomials $F_{n,m}(x) = (x^{n+1}+1)/(x+1) + x^m$. The ranges for n are indicated in the first column. The second, third, fourth and fifth columns give the total number for $n \equiv 1, 3, 5, 7 \pmod 8$, respectively.

Proof. Let $F(x) \in \mathbb{Z}[x]$ be any monic lift of $f(x)$ with $F(0) = 1$, and let $x_0, x_1, \ldots, x_{n-1}$ be the roots of $F(x)$ in some extension of the rational numbers. Then

$$nF - xF' = \sum_{i \in I} ia_i x^{n-i} + \sum_{j \in J} ja_j x^{n-j} + n.$$

Setting $D = (-1)^{n(n-1)/2} \operatorname{Disc}(F)$ and using (2) and Lemma 3 we obtain

$$D = \prod_{k=0}^{n-1} \left(\sum_{i \in I} ia_i x_k^{n-i} + \sum_{j \in J} ja_j x_k^{n-j} + n \right). \tag{9}$$

Expanding the right hand side of (9) yields

$$\begin{aligned} D &= n^n + n^{n-1} \sum_{i \in I} \sum_{k=0}^{n-1} ia_i x_k^{n-i} + n^{n-1} \sum_{j \in J} \sum_{k=0}^{n-1} ja_j x_k^{n-j} \\ &\quad + n^{n-2} \sum_{\substack{i_1, i_2 \in I \\ i_1 < i_2}} \sum_{\substack{k_1, k_2 = 0 \\ k_1 \neq k_2}}^{n-1} i_1 i_2 a_{i_1} a_{i_2} x_{k_1}^{n-i_1} x_{k_2}^{n-i_2} \\ &\quad + n^{n-2} \sum_{i \in I} \sum_{\substack{k_1, k_2 = 0 \\ k_1 < k_2}}^{n-1} i^2 a_i^2 x_{k_1}^{n-i} x_{k_2}^{n-i} + S(x_0, x_1, \ldots, x_{n-1}), \end{aligned}$$

where $S(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{Z}[x_0, x_1, \ldots, x_{n-1}]$ is a symmetric polynomial. It can easily be verified that the coefficients of each monomial in S is divisible by 8, and hence $S(x_0, x_1, \ldots, x_{n-1})$ is an integer divisible by 8. Using the notation introduced in (3) for power sums of the x_i's, we have

$$\begin{aligned} D &\equiv n^n + n^{n-1} \sum_{i \in I} ia_i s_{n-i} + n^{n-1} \sum_{j \in J} ja_j s_{n-j} \\ &\quad + n^{n-2} \sum_{\substack{i_1, i_2 \in I \\ i_1 < i_2}} i_1 i_2 a_{i_1} a_{i_2} s_{n-i_1, n-i_2} + \frac{1}{2} n^{n-2} \sum_{i \in I} i^2 a_i^2 s_{n-i, n-i} \pmod 8. \end{aligned} \tag{10}$$

Now, if $a_k \neq 0$ for some $1 \leq k \leq 2n/3$, then $4 \mid k$. Hence Newton's identity (5) simplifies to

$$s_k + s_{k-1} a_1 + s_{k-2} a_2 + \cdots + s_1 a_{k-1} \equiv 0 \pmod 4$$

for $1 \leq k \leq 2n/3$. It follows that $s_k \equiv 0 \pmod 4$ for $1 \leq k \leq 2n/3$. Similarly, since $2 \mid k$ for all k satisfying $a_k \neq 0$ and $2n/3 < k \leq n-1$, one can conclude that $s_k \equiv 0 \pmod 2$ for $2n/3 < k \leq n-1$. Also, if $p, q \geq 1$ and $p + q \leq 2n/3$, then $s_p \equiv s_q \equiv s_{p+q} \equiv 0 \pmod 4$ and (4) implies that $s_{p,q} \equiv 0 \pmod 4$.

Thus (10) simplifies to $D \equiv n^n \pmod 8$, and so $\operatorname{Disc}(F) \equiv 5 \pmod 8$ if $n \equiv \pm 3 \pmod 8$. Since $\operatorname{Disc}(f) \equiv \operatorname{Disc}(F) \pmod 2$, this implies that $f(x)$ has nonzero discriminant and hence no repeated factors. The reducibility of $f(x)$ is now a consequence of Theorem 2. $\square$

References

[1] O. Ahmadi, "The trace spectra of polynomial bases for $\mathbb{F}_{2^n}$", preprint, 2004.
[2] O. Ahmadi and A. Menezes, "On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$", *Designs, Codes and Cryptography*, to appear.
[3] I. Blake, S. Gao and R. Lambert, "Constructive problems for irreducible polynomials over finite fields", *Information Theory and Applications*, Lecture Notes in Computer Science 793 (1994), 1-23.
[4] I. Blake, S. Gao and R. Lambert, "Construction and distribution problems for irreducible polynomials over finite fields", *Applications of Finite Field* (D. Gollmann, Ed.), Clarendon Press, 1996, 19-32.
[5] A. Bluher, "A Swan-like theorem", preprint, 2004.
[6] W. Geiselmann and H. Lukhaub, "Redundant representation of finite fields" *Public Key Cryptography – PKC 2001*, Lecture Notes in Computer Science 1992 (2001), 339-352.
[7] A. Hales and D. Newhart, "Irreducibles of tetranomial type", in *Mathematical Properties of Sequences and Other Combinatorial Structures*, Kluwer, 2003.
[8] A. Hales and D. Newhart, "Swan's theorem for binary tetranomials", preprint, 2004.
[9] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2003.
[10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1984.
[11] G. Seroussi, "Table of low-weight binary irreducible polynomials", Hewlett-Packard Technical Report HPL-98-135, 1998.
[12] I. Shparlinski, "On primitive polynomials", *Problemy Peredachi Inform.*, 23, (1987), 100-103 (in Russian).
[13] J. Silverman, "Fast multiplication in finite fields $GF(2^N)$", *Cryptographic Hardware and Embedded Systems – CHES '99*, Lecture Notes in Computer Science 1717 (1999), 122-134.
[14] L. Stickelberger, "Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper", Verh. 1 Internat. Math. Kongresses, Zurich 1897, 182-193.
[15] R. Swan, "Factorization of polynomials over finite fields", *Pacific Journal of Mathematics*, 12 (1962), 1099-1106.
[16] H. Wu, M. Anwar Hasan, I. Blake and S. Gao, "Finite field multiplier using redundant representation", *IEEE Transactions on Computers*, 51 (2002), 1306-1316.

Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
E-mail address: oahmadid@uwaterloo.ca ajmeneze@uwaterloo.ca