Algorithms for Finding Almost Irreducible and Almost Primitive Trinomials

Richard P. Brent
Oxford University Computing Laboratory,
Wolfson Building, Parks Road,
Oxford OX1 3QD, UK

Paul Zimmermann
LORIA/INRIA Lorraine
615 rue du jardin botanique
BP 101, 54602 Villers-lès-Nancy, France

Dedicated to Hugh Cowie Williams on the occasion of his 60th birthday.

Abstract. Consider polynomials over GF(2). We describe efficient algorithms for finding trinomials with large irreducible (and possibly primitive) factors, and give examples of trinomials having a primitive factor of degree r for all Mersenne exponents $r = \pm 3 \bmod 8$ in the range $5 < r < 10^7$, although there is no irreducible trinomial of degree r. We also give trinomials with a primitive factor of degree $r = 2^k$ for $3 \le k \le 12$. These trinomials enable efficient representations of the finite field $\mathrm{GF}(2^r)$. We show how trinomials with large primitive factors can be used efficiently in applications where primitive trinomials would normally be used.

1 Introduction

Irreducible and primitive polynomials over finite fields have many applications in cryptography, coding theory, random number generation, etc. See, for example, [13, 15, 17, 20, 21].

For simplicity we restrict our attention to the finite field $\mathbb{Z}_2 = \mathrm{GF}(2)$; the generalization to other finite fields is straightforward. All polynomials are assumed to be in $\mathbb{Z}_2[x]$, and computations on polynomials are performed in $\mathbb{Z}_2[x]$ or in a specified quotient ring. A polynomial $P(x) \in \mathbb{Z}_2[x]$ may be written as P if the argument x is clear from the context. We recall some standard definitions.

Definition 1.1 A polynomial $P(x)$ with $P(0) \neq 0$ has *period* ρ if ρ is the least positive integer such that $x^\rho = 1 \bmod P(x)$. We say that x has order $\rho \bmod P(x)$.

1991 *Mathematics Subject Classification.* Primary 11B83, 11Y16; Secondary 11-04, 11K35, 11N35, 11R09, 11T06, 12-04, 12Y05, 68Q25 .

Definition 1.2 A polynomial $P(x)$ is *reducible* if it has nontrivial factors; otherwise it is *irreducible.*

Definition 1.3 A polynomial $P(x)$ of degree $n > 0$ is *primitive* if $P(x)$ is irreducible and has period $2^n - 1$. (Recall our assumption that $P(x) \in \mathbb{Z}_2[x]$.)

If $P(x)$ is primitive, then x is a generator for the multiplicative group of the field $\mathbb{Z}_2[x]/P(x)$, giving a concrete representation of $\mathrm{GF}(2^n)$. See Lidl and Niederreiter [20] or Menezes *et al.* [21] for background information.

There is an interest in discovering primitive polynomials of high degree n for applications in random number generation [4, 7] and cryptography [21]. In such applications it is often desirable to use primitive polynomials with a small number of nonzero terms, *i.e.* a small weight. In particular, we are interested in *trinomials* of the form $x^n + x^s + 1$, where $n > s > 0$ (so there are exactly three nonzero terms).

If $P(x)$ is irreducible and $\deg(P) = n > 1$, then the order of x in $\mathbb{Z}_2[x]/P(x)$ is a divisor of $2^n - 1$. To test if $P(x)$ is primitive, we must test if the order of x is exactly $2^n - 1$. To do this efficiently[1] it appears that we need to know the complete prime factorization of $2^n - 1$. At the time of writing these factorizations are known for $n < 713$ and certain larger n, see [8].

We say that n is a *Mersenne exponent* if $2^n - 1$ is prime. In this case the factorization of $2^n - 1$ is trivial and an irreducible polynomial of degree n is necessarily primitive. Large Mersenne exponents are known [14], so there is a possibility of finding primitive trinomials of high degree. To test if a trinomial of prime degree n is reducible takes time $O(n^2)$, so to test all trinomials of degree n takes time $O(n^3)$.

Several authors [16, 18, 19, 27] have computed primitive trinomials whose degree is a Mersenne exponent, up to some bound imposed by the computing resources available. Recently Brent, Larvala and Zimmermann [6] gave a new algorithm, more efficient than those used previously, and computed all the primitive trinomials of Mersenne exponent $n \le 3021377$ (subsequently extended to $n \le 6972593$).

For some $n \ge 2$, irreducible trinomials of given degree n do not exist. Swan's theorem (see §2) rules out $n = 0 \bmod 8$ and also most $n = \pm 3 \bmod 8$. Since about half of the known Mersenne exponents are $\pm 3 \bmod 8$, we can only hope to find primitive trinomials of degree n for about half the Mersenne exponents n.

In the cases where primitive trinomials are ruled out by Swan's theorem, the conventional approach is to use primitive polynomials with more than three nonzero terms. A polynomial with an even number of nonzero terms is divisible by $x + 1$, so we must use polynomials with five or more nonzero terms [18, 19, 21]. This is considerably more expensive in applications because the number of operations required for multiplication or division by a sparse polynomial is approximately proportional to the number of nonzero terms.

In §2 we discuss Swan's theorem, then in §3 we introduce "almost irreducible" and "almost primitive" polynomials as a way of circumventing the implications of Swan's theorem. An algorithm (AIT) for computing almost irreducible trinomials, and an extension (APT) for almost primitive trinomials, are described in §4. Algorithm APT has been used to find almost primitive trinomials with high degree in cases where Swan's theorem shows that primitive trinomials do not exist. Computational results and examples are given in §§5–6. In §7 we give some computational results on almost primitive trinomials that are useful for representing the finite

[1] Here "efficiently" means in time polynomial in the degree n.

fields $\mathrm{GF}(2^{2^k})$, $k \le 12$. In §8 we explain how to use almost irreducible/primitive trinomials efficiently in applications. Finally, in §9, we conclude with some theoretical results on the density of almost irreducible and almost primitive polynomials, and some computational results on the density of the corresponding trinomials. We thank Shuhong Gao and the referees for their comments on a draft of this paper.

2 Swan's theorem and its implications

Swan's theorem is a rediscovery of results of Pellet [23], Stickelberger [24], Dickson [10] and Dalen [9] – see Swan [25, p. 1099] and von zur Gathen [12]. Let $\nu(P)$ denote the number of irreducible factors (counted according to their multiplicity) of a polynomial $P \in \mathbb{Z}_2[x]$.

Theorem 2.1 Swan [25, Corollary 5]. *Suppose* $n > s > 0$, $n - s$ *odd. Then* $\nu(x^n + x^s + 1) = 0 \bmod 2$ *iff one of the following holds:*
a) n *even,* $n \ne 2s$, $ns/2 \bmod 4 \in \{0, 1\}$;
b) $2n \ne 0 \bmod s$, $n = \pm 3 \bmod 8$;
c) $2n = 0 \bmod s$, $n = \pm 1 \bmod 8$.

If both n and s are odd, we can replace s by $n - s$ (leaving the number of irreducible factors unchanged, since $\nu(x^n + x^s + 1) = \nu(x^n + x^{n-s} + 1)$) and apply Swan's theorem. If n and s are both even, then $T = x^n + x^s + 1$ is a square and $\nu(T)$ is even. Thus, in all cases we can determine $\nu(T) \bmod 2$ using Swan's theorem.

Since a polynomial that has an even number of irreducible factors is reducible, we have:

Corollary 2.2 *If* n *is prime,* $n = \pm 3 \bmod 8$, $s \ne 2$, $s \ne n - 2$, *then* $x^n + x^s + 1$ *is reducible over* $\mathbb{Z}_2$.

Corollary 2.2 shows that there are no irreducible trinomials with degree a Mersenne exponent $n = \pm 3 \bmod 8$ (except possibly for $s = 2$ or $n - 2$). This appears to prevent us from using trinomials with periods $2^n - 1$ in these cases. Fortunately, there is a way to circumvent Swan's theorem and avoid paying a significant speed penalty in most applications of irreducible/primitive trinomials. We describe this in the following section.

3 Almost primitive trinomials

Tromp, Zhang and Zhao [26] asked the following question: given an integer $r > 1$, do there exist integers n, s such that

$$G = \gcd(x^n + x^s + 1, x^{2^r - 1} + 1)$$

is a primitive polynomial of degree r? They verified that the answer is "yes" for $r \le 171$, and conjectured that the answer is always "yes".

Blake, Gao and Lambert [3] confirmed the conjecture for $r \le 500$. They also relaxed the condition slightly and asked: do there exist integers n, s such that G has a primitive factor of degree r? Motivated by [3], we make some definitions.

Definition 3.1 A polynomial $P(x)$ of degree n is *almost primitive (almost irreducible)* if $P(0) \ne 0$ and $P(x)$ has a primitive (irreducible) factor of degree r, for some $r > n/2$. We say that P has *exponent* r and *increment* $n - r$.

For example, the trinomial $x^{16} + x^3 + 1$ is almost primitive with exponent 13 and increment 3, because

$$x^{16} + x^3 + 1 = (x^3 + x^2 + 1)D_{13}(x),$$

where

$$D_{13}(x) = x^{13} + x^{12} + x^{11} + x^9 + x^6 + x^5 + x^4 + x^2 + 1$$

is primitive. From a computational viewpoint it is more efficient to work in the ring $\mathbb{Z}_2[x]/(x^{16} + x^3 + 1)$ than in the field $F = \mathbb{Z}_2[x]/D_{13}(x)$. In §8 we outline how it is possible to work in the field F, while performing most arithmetic in the ring $\mathbb{Z}_2[x]/(x^{16} + x^3 + 1)$, and without explicitly computing the dense primitive polynomial $D_{13}(x)$.

Note that, according to Definition 3.1, a primitive polynomial is *a fortiori* an almost primitive polynomial (the case $r = n$). Similarly, an irreducible polynomial other than 1 or x is almost irreducible. The restriction $r > n/2$ in Definition 3.1 ensures that polynomials such as $(x^3+x+1)^2$ are not regarded as almost irreducible.

In practice we choose the smallest possible increment δ for given exponent r, *e.g.* in Tables 1–2 we have $\delta \le 16$. For most practical purposes, almost primitive trinomials of exponent r and small increment are almost as useful as primitive trinomials of degree r (see §8).

4 Searching for almost irreducible/primitive trinomials

In this section we outline algorithms for finding almost irreducible or almost primitive trinomials with large exponent r. In the latter case we assume that the complete factorization of $2^r - 1$ is known. The algorithms are generalizations of those given in [6, 13, 21], which handle the case $\delta = 0$.

4.1 An algorithm for almost irreducible trinomials. Suppose $0 \le \delta < r$, $0 < s < r + \delta$, and we wish to test if the trinomial $T(x) = x^{r+\delta} + x^s + 1$ is almost irreducible with exponent r (see Definition 3.1). If it is not then we discard it, and (perhaps) try again with different (r, s, δ).

We first state the algorithm, then explain the steps whose justification is not immediately obvious. Input to the algorithm is (r, s, δ) and a sieving bound $B \in [\delta, r)$. The optimal B is implementation-dependent: see the discussion in [6]. In the computation of Table 1 we used $B = \min(r - 1, \max(\delta, 4 + \lfloor \log_2 r \rfloor))$. Recall that polynomials are in $\mathbb{Z}_2[x]$, so computations on polynomials are performed in $\mathbb{Z}_2[x]$ or in a quotient ring such as $\mathbb{Z}_2[x]/T(x)$.

Algorithm AIT(r, s, δ, B)

1. If $\gcd(r + \delta, s) = 0 \bmod 2$ then return false.
2. $d := 0$; $k := 0$; $S := 1$; $T := x^{r+\delta} + x^s + 1$;
   for $i := 2$ to δ do
      $g := \gcd(T, (x^{2^i} \bmod T) + x)$;
      $g := g/\gcd(g, S)$; $S := g \times S$;
      $d := d + \deg(g)$; $k := k + \deg(g)/i$;
3. if $(d \ne \delta)$ or $(k = \nu(T) \bmod 2)$ then return false.
4. for $i := \delta + 1$ to B do
      $g := \gcd(T, (x^{2^i} \bmod T) + x)$;
      if $S \bmod g \ne 0$ then return false.

5. if $((x^{2^r} \bmod T) + x)S \neq 0 \bmod T$ then return false.
6. for each prime divisor $p \neq r$ of r
   if $\gcd(((x^{2^{r/p}} \bmod T) + x)S, T) \neq S$ then return false.
7. return true. [T is almost irreducible with exponent r.] □

If $\delta = 0$, Algorithm AIT reduces to a standard algorithm for finding irreducible trinomials. We can assume that $\delta \neq 1$, because the only irreducible polynomials of degree 1 are x and $x+1$, and neither can be a factor of a trinomial. Hence, we need only consider $\delta \geq 2$.

Step 1 discards trinomials that are squares (see Theorem 4.1 below). If this step is passed then $\gcd(T, T') = 1$, so T is square-free.

Step 2 may be called *sieving*, although it is done by GCD computations. By computing $\gcd(T, (x^{2^i} \bmod T) + x)$ for $2 \leq i \leq \delta$, we find the product $S = P_1 \cdots P_k$ of all irreducible factors P_j of T such that $\deg(P_j) = d_j \leq \delta$. We have $T = SD$, where D is some polynomial of degree $n - d$, and $\gcd(S, D) = 1$.

Step 3 returns false if d or k is incompatible with the assumption that T has an irreducible factor of degree r. Note that Swan's theorem gives $\nu(T) \bmod 2$.

In Step 4, suppose $S \bmod g \neq 0$. Thus $f = g/\gcd(S, g)$ is a factor of $D = T/S$, and $f \neq 1$. If $f \neq D$ then D is reducible. If $f = D$ then D splits into factors of degree at most $B < r$, so again D is reducible. Thus, we can return false.

In Step 5, sieving has failed to discard T, so a full irreducibility test of D is required. We can discard T (*i.e.* return false) if $x^{2^r} \neq x \bmod D$, but D is in general a dense polynomial, so we perform an equivalent computation that only involves exponentiation mod T. Note that the computation of $x^{2^r} \bmod T$ takes only $O(r^2)$ bit-operations, since T is a trinomial.

Finally, we should return false if $\gcd(x^{2^q} + x, D) \neq 1$ for any divisor q of r, $q \neq r$. Step 6 implements an equivalent test that is more efficient because the operations are performed mod T and only maximal divisors $q = r/p$ of r are checked. Step 6 is trivial if r is prime.

4.2 Algorithm APT for almost primitive trinomials. To search for almost primitive trinomials with exponent r, we apply Theorem 4.2 below, and then algorithm AIT, to find a candidate trinomial that is almost irreducible with exponent r. Unless $2^r - 1$ is prime, it is necessary to verify that the irreducible factor D of degree r has period $2^r - 1$ and not some proper divisor of $2^r - 1$. This can be done by verifying that, for each prime divisor p of $2^r - 1$,

$$((x^{(2^r-1)/p} \bmod T) + 1)S \neq 0 \bmod T\ .$$

4.3 Refinements. Several refinements are possible.

1. The fast algorithm of [6, §4] can be used to accelerate the computation of $x^{2^i} \bmod T$ in steps 2, 4–6 of Algorithm AIT if $r + \delta$ is odd.

2. Sieving can often be curtailed. Suppose that step 2 of Algorithm AIT has been performed for $i \leq \widehat{\delta} < \delta$, so we have found all $\widehat{k}$ irreducible factors of degree $\leq \widehat{\delta}$. Suppose that the sum of their degrees is $\widehat{d}$. If

$$\widehat{d} < \delta < \widehat{d} + \widehat{\delta} + 1, \tag{4.1}$$

then the constraint $d = \delta$ can not be satisfied and we can return false. Also, if $\widehat{k} \neq \nu(T) \bmod 2$, then (4.1) can be replaced by the weaker condition

$$\widehat{d} < \delta < \widehat{d} + 2(\widehat{\delta} + 1). \tag{4.2}$$

3. If r is a Mersenne exponent, computation of the small factor S can be avoided. Define $F = \mathrm{lcm}(2^{d_j} - 1)$, so F is a multiple of the period of S, and $\gcd(F, 2^r - 1) = 1$. Step 2 of Algorithm AIT can easily be modified to compute F instead of S, and to save $g_i = \deg g$ at iteration i. Step 4 can be modified to return false if $\deg g > \sum_{j|i, 2 \le j \le \delta} g_j$. Step 5 can be modified to return false if

$$(x^F)^{2^r} \neq x^F \bmod T(x). \tag{4.3}$$

The computation involved is almost the same as for the "standard" method of testing irreducibility of a trinomial [6, §3]: the significant difference is that we start with x^F instead of x. This variation of algorithm AIT was used to compute most of the entries in Table 1.

4. Theorems 4.1–4.2 allow us to discard many trinomials quickly.

Theorem 4.1 *Let $T(x) = x^n + x^s + 1$ be an almost irreducible trinomial. Then $\gcd(n, s)$ is odd.*

Proof Assume that $\gcd(n, s)$ is even. Then $T(x) = (x^{n/2} + x^{s/2} + 1)^2$ is a square, so can not have an irreducible factor of degree greater than $n/2$. □

We remark that $x^6 + x^3 + 1$ is irreducible (though not primitive) over $\mathbb{Z}_2$, and in this case $\gcd(n, s) = 3$.

Theorem 4.2 *Let $T(x) = x^n + x^s + 1$ be an almost primitive trinomial. Then $\gcd(n, s) = 1$.*

Proof Suppose $g = \gcd(n, s) > 1$. From Theorem 4.1 we can assume that $g \ge 3$. Write $y = x^g$. Thus $T(x) = y^{\widehat{n}} + y^{\widehat{s}} + 1$, where $\widehat{n} = n/g$, $\widehat{s} = s/g$. The order of y is at most $2^{\widehat{n}} - 1$. Thus, the order of x is at most $g(2^{\widehat{n}} - 1) = g(2^{n/g} - 1)$. If $T(x)$ is almost primitive with exponent r, then the order of x is $2^r - 1$. Thus

$$2^r - 1 \le g(2^{n/g} - 1).$$

Now $n + 1 \le 2r$ by Definition 3.1, so

$$2^{(n+1)/2} - 1 \le g(2^{n/g} - 1). \tag{4.4}$$

The right-hand side of (4.4) is a decreasing function of g for $g \ge 3$. Thus,

$$2^{(n+1)/2} - 1 \le 3(2^{n/3} - 1). \tag{4.5}$$

It is easy to verify that (4.5) can not hold for $n \ge 6$, but if $n < 6$ then $n/g < 2$, which is a contradiction. Hence $g = 1$. □

5 Computational results

We conducted a search for almost primitive trinomials whose exponent r is also a Mersenne exponent. For all Mersenne exponents $r = \pm 1 \bmod 8$ with $r \le 6972593$, primitive trinomials of degree r are known, see [6]. Here we consider the cases $r = \pm 3 \bmod 8$, where the existence of irreducible trinomials $x^r + x^s + 1$ is ruled out by Swan's theorem (except for $s = 2$ or $r - 2$, but the only known cases are $r = 3, 5$). For each exponent r we searched for all almost primitive trinomials with the minimal increment δ for which at least one almost primitive trinomial exists. The search has been completed for all Mersenne exponents $r < 10^7$.

In all cases of Mersenne exponent $r = \pm 3 \bmod 8$, where $5 < r < 10^7$, we have found at least one almost primitive trinomial with exponent r and some increment $\delta \in [2, 12]$. The results are summarized in Table 1. The first four entries are

r	δ	s	f	Small factors and remarks
13	3	3	7	x^3+x^2+1
19	3	3	7	x^3+x+1
61	5	17	31	$x^5+x^3+x^2+x+1$
107	2	8	3	x^2+x+1
		14	3	x^2+x+1
		17	3	x^2+x+1
2203	3	355	7	x^3+x^2+1
4253	8	1806	255	$x^8+x^7+x^2+x+1$
		1960	85	$x^8+x^6+x^5+x^4+x^2+x+1$
9941	3	1077	7	x^3+x^2+1
11213	6	227	63	$x^6+x^5+x^3+x^2+1$
21701	3	6999	7	x^3+x^2+1
		7587	7	x^3+x^2+1
86243	2	2288	3	x^2+x+1
216091	12	42930	3937	$x^{12}+x^{11}+x^5+x^3+1$ $=(x^5+x^4+x^3+x+1)\cdot$ $(x^7+x^5+x^4+x^3+x^2+x+1)$
1257787	3	74343	7	x^3+x^2+1
1398269	5	417719	21	$x^5+x^4+1=(x^2+x+1)\cdot(x^3+x+1)$
2976221	8	1193004	85	$x^8+x^7+x^6+x^5+x^4+x^3+1$
13466917	?	?	?	None for $\delta<3$ or $\delta=4$

Table 1

Some almost primitive trinomials over $\mathbb{Z}_2$.
$x^{r+\delta}+x^s+1$ has a primitive factor of degree r;
δ is minimal; $2s \le r+\delta$; the period $\rho=(2^r-1)f$.

from [3, Table 4]; the other entries are new. They were computed using Algorithm APT, with some simplifications that are possible because r is a Mersenne exponent (see §4.3.3 above).

For all but two of the almost primitive trinomials $x^{r+\delta}+x^s+1$ given in Table 1, the period $\rho=(2^r-1)f$ satisfies $\rho>2^{r+\delta-1}$. Thus, the period is greater than the greatest period $(2^{r+\delta-1}-1)$ that can be obtained for any polynomial of degree less than $r+\delta$. In the two exceptional cases the small factors of degree 8 are not primitive, having period $85=255/3$.

For the largest known Mersenne exponent, $r=13466917$, we have not yet started an extensive computation, but we have shown that $\delta\ge 3$ and $\delta\ne 4$ (see Theorem 6.3).

6 Examples and special cases

We considered the almost primitive trinomial $x^{16}+x^3+1$ in §3. Here we give an example with much higher degree: $r=216091$, $\delta=12$. We have

$$x^{216103}+x^{42930}+1=S(x)D(x),$$

where

$$S(x)=x^{12}+x^{11}+x^5+x^3+1,$$

and $D(x)$ is a (dense) primitive polynomial of degree 216091. The factor $S(x)$ of degree 12 splits into a product of two primitive polynomials, $x^5 + x^4 + x^3 + x + 1$ and $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$. The contribution to the period from these factors is $f = \mathrm{lcm}(2^5 - 1, 2^7 - 1) = 3937$.

Theorem 6.1 *If T is an almost irreducible trinomial with exponent 216091 and increment δ, then $\delta \notin \{0, 1, 2, 4, 6\}$.*

Proof As T is a trinomial, it is not divisible by x or $x + 1$, so $\delta \neq 1$. Assume that $T = x^n + x^s + 1$ is almost irreducible with $\deg(T) = n = r + \delta$, where $\delta \in \{0, 2, 4, 6\}$. Thus $T = SD$ where D is irreducible, $\deg(D) = r = 216091$, n is odd and we can assume that s is even (otherwise replace s by $n - s$). Since r is a Mersenne exponent, D is primitive and T is almost primitive. Let $\nu_2 = \nu(T) \bmod 2$. We consider the cases $\delta = 0, 2, 4, 6$ in turn and show that each case leads to a contradiction.

A. $\delta = 0$. $n = 3 \bmod 8$ and $\nu_2 = 1$, so by Swan's theorem $s \mid 2n$. From Theorem 4.2, $\gcd(n, s) = 1$, so the only possibility is $s = 2$. Now $n = 1 \bmod 3$, so $x^n + x^2 + 1 = x^2 + x + 1 \bmod x^3 - 1$. Thus $x^2 + x + 1 \mid x^n + x^2 + 1$, a contradiction.

B. $\delta = 2$. $n = 0 \bmod 3$, so $T = x^s \bmod x^3 - 1$. Thus $x^2 + x + 1$ does not divide T, but $x^2 + x + 1$ is the only irreducible polynomial of degree 2, and hence the only possibility for S, a contradiction.

C. $\delta = 4$. $\deg(S) = 4$, but S can not have irreducible factors of degree 2, since $x^2 + x + 1$ is the only irreducible polynomial of degree 2, and T is square-free. Thus S is irreducible of degree 4 and a divisor of $x^{15} - 1$. We have $n = -1 \bmod 8$ and $\nu_2 = 0$, so by Swan's theorem and Theorem 4.2 we must have $s = 2$. Now $n = 5 \bmod 15$, so $T = x^5 + x^2 + 1 \bmod x^{15} - 1$, but $x^5 + x^2 + 1$ is irreducible. Thus T has no factor of degree 4, a contradiction.

D. $\delta = 6$. S could be of the form S_6, S_2S_4 or $S_3\widehat{S}_3$, where $S_j, \widehat{S}_j$ are irreducible of degree j. If $S = S_6$ then $\nu_2 = 0$ and, by Swan's theorem and Theorem 4.2, $s = 2$. However, $n = 1 \bmod 3$, so $x^2 + x + 1 \mid x^n + x^2 + 1$, a contradiction. If $S = S_2S_4$ then $\deg(\gcd(T, x^{15} - 1)) = 6$. Now $n = 7 \bmod 15$, so $T = x^7 + x^{s \bmod 15} + 1 \bmod x^{15} - 1$, and in each of the 15 cases we find that $\deg(\gcd(T, x^{15} - 1)) \leq 4$. If $S = S_3\widehat{S}_3$ then $\deg(\gcd(T, x^7 - 1)) = 6$. Now $n = 0 \bmod 7$, so $T = x^{s \bmod 7} \bmod x^7 - 1$, and $\gcd(T, x^7 - 1) = 1$. Thus $\delta \neq 6$. $\square$

Theorem 6.2 *If T is an almost irreducible trinomial with exponent 2976221 and increment δ, then $\delta \notin \{0, 1, 2, 4\}$.*

Proof The proof is similar to that of Theorem 6.1. Assume that $\delta \in \{0, 2, 4\}$ and that s is even. If $\delta = 0$ we must have $s = 2$. Now $n = 3 \bmod 7$, so $T = x^3 + x^2 + 1 \bmod x^7 - 1$, and thus T has an irreducible factor $x^3 + x^2 + 1$. If $\delta = 2$, again we must have $s = 2$. In this case $T = x^{118} + x^2 + 1 \bmod x^{255} - 1$, and a computation shows that $x^8 + x^7 + x^3 + x^2 + 1 \mid T$. Finally, if $\delta = 4$, we have $T = x^{s \bmod 15} \bmod x^{15} - 1$, so T has no irreducible factor of degree 4. $\square$

Theorem 6.3 *If T is an almost irreducible trinomial with exponent 13466917 and increment δ, then $\delta \notin \{0, 1, 2, 4\}$.*

Proof As above, we can assume that $\delta \neq 1$, $n = r + \delta$ is odd, and without loss of generality s is even. If $\delta = 0$ the only case to consider is $s = 2$, but $n = 1 \bmod 3$, so $T = x^2 + x + 1 \bmod x^3 - 1$, and thus T is divisible by $x^2 + x + 1$. If $\delta = 2$ then $T = x^{s \bmod 3} \bmod x^3 - 1$, so T is never divisible by $x^2 + x + 1$. If

k	r	δ	s	f	Small factor $S(x)$
3	8	5	1	31	$x^5+x^4+x^3+x+1$
			2	7	$(x^2+x+1)(x^3+x+1)$
4	16	11	2	7	$(x^3+x+1)(x^8+x^7+x^6+x^3+x^2+x+1)$
5	32	8	3	1	$x^8+x^6+x^5+x^4+x^2+x+1$
6	64	10	3	21	$(x^4+x+1)(x^6+x^5+x^4+x+1)$
			21	341	$x^{10}+x^7+x^6+x^5+x^3+x^2+1$
7	128	2	17	1	x^2+x+1
8	256	16	45	1	$x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^7+x^3+x+1$
9	512	9	252	31	$(x^4+x+1)(x^5+x^3+1)$
10	1024	3	22	7	x^3+x^2+1
11	2048	10	101	341	$x^{10}+x^9+x^8+x^7+x^5+x^4+1$
12	4096	3	600	7	x^3+x+1
			628	7	x^3+x+1
			1399	7	x^3+x^2+1

Table 2

Some almost primitive trinomials over $\mathbb{Z}_2$.
$x^{r+\delta}+x^s+1$ has a primitive factor of degree $r=2^k$;
δ is minimal; $2s \le r+\delta$; the period $\rho=(2^r-1)f$.

$\delta=4$ then S must be irreducible of degree 4, and the only possibility is $s=2$. Now $T=x^{11}+x^2+1 \bmod x^{15}-1$, but $x^{11}+x^2+1$ is irreducible, so T has no irreducible factor of degree 4. $\square$

7 The Fermat connection

If we have found an almost irreducible trinomial $T=x^n+x^s+1$ with exponent $r=n-\delta$, then to check if T is almost primitive we need the complete factorization of 2^r-1. In §5 we chose r so the factorization was trivial, because 2^r-1 was a Mersenne prime. Another case of interest, considered in this section, is when r is a power of two, say $r=2^k$. Then

$$2^r-1=F_0F_1\cdots F_{k-1},$$

where $F_j=2^{2^j}+1$ is the j-th Fermat number. The complete factorizations of these F_j are known for $j\le 11$ (see [5]) so we can factor $2^{2^k}-1$ for $k\le 12$.

In Table 2 we give almost primitive trinomials $T=x^{r+\delta}+x^s+1$ with exponent $r=2^k$ for $3\le k\le 12$. Thus $T=SD$ where D is primitive and has degree 2^k. We also give S in factored form. The irreducible factors of S are not always primitive. The period of T is $\mathrm{lcm}(2^r-1,\mathrm{period}(S))=(2^r-1)f$.

By Swan's theorem, a primitive trinomial of degree 2^k does not exist for $k\ge 3$. However, we can work efficiently in the finite fields $\mathrm{GF}(2^{2^k})$, $k\in[3,12]$, using the trinomials listed in Table 2 and the implicit algorithms of §8.

8 Implicit algorithms

Suppose we wish to work in the finite field $\mathrm{GF}(2^r)$ where r is the exponent of an almost primitive trinomial T. We can write $T=SD$, where $\deg(S)=\delta$,

$\deg(D) = r$. Thus

$$GF(2^r) \equiv \mathbb{Z}_2[x]/D(x),$$

but because D is dense we wish to avoid working directly with D, or even explicitly computing D. We show that it is possible to work modulo the trinomial T.

We can regard $\mathbb{Z}_2[x]/T(x)$ as a redundant representation of $\mathbb{Z}_2[x]/D(x)$. Each element $A \in \mathbb{Z}_2[x]/T(x)$ can be represented as

$$A = A_c + A_d D,$$

where $A_c \in \mathbb{Z}_2[x]/D(x)$ is the "canonical representation" that would be obtained if we worked in $\mathbb{Z}_2[x]/D(x)$, and $A_d \in \mathbb{Z}_2[x]$ is some polynomial of degree less than δ.

We can perform computations such as addition, multiplication and exponentiation in $\mathbb{Z}_2[x]/T(x)$, taking advantage of the sparsity of T in the usual way. If $A \in \mathbb{Z}_2[x]/T(x)$ and we wish to map A to its canonical representation A_c, we use the identity

$$A_c = (AS \bmod T)/S,$$

where the division by the (small) polynomial S is exact. A straightforward implementation requires only $O(\delta r)$ operations. We avoid computing $A_c = A \bmod D$ directly; in fact we never compute the (large and dense) polynomial D: it is sufficient that D is determined by the trinomial T and the small polynomial S.

In applications such as random number generation [7], where the trinomial $T = x^n + x^s + 1$ is the denominator of the generating function for a linear recurrence $u_k = u_{k-s} + u_{k-n}$, it is possible (by choosing appropriate initial conditions that annihilate the unwanted component) to generate a sequence that satisfies the recurrence defined by the polynomial D. However, this is not necessary if all that matters is that the linear recurrence generates a sequence with period at least $2^r - 1$.

9 The density of almost irreducible/primitive polynomials

In this section we state some theorems regarding the distribution of almost irreducible *polynomials*. The proofs are straightforward, and similar to the proof of Theorem 1.2 in [11], which generalizes our Corollary 9.2. We would like to prove similar theorems about almost irreducible *trinomials*, but this seems to be difficult.

Let I_n denote the number of irreducible polynomials of degree n, excluding the polynomial x, and let $N_{r,\delta}$ denote the number of almost irreducible polynomials with exponent r and increment δ. Thus $\sum_{d|n} dI_d = 2^n - 1$ and, by Möbius inversion,

$$I_n = \frac{1}{n}\sum_{d|n}\mu(d)\left(2^{n/d}-1\right) = \frac{2^n}{n}\left(1 + O(2^{-n/2})\right) .$$

Theorem 9.1 *If* $0 \le \delta < r$, *then* $N_{r,\delta} = 2^{\max(0,\delta-1)} I_r$.

Proof The case $\delta = 0$ is immediate, so assume that $\delta > 0$. Thus $r > 1$. For each irreducible polynomial D of degree r, and each polynomial S of degree δ such that $S(0) \ne 0$, there is an almost irreducible polynomial $P = SD$. Also, by the constraint $\delta < r$, P determines S and D uniquely. Thus, the result follows by a counting argument, since there are $2^{\delta-1}$ possibilities for S and I_r possibilities for D. $\square$

Corollary 9.2 *If $n = r + \delta$, $0 < \delta < r$, and P is chosen uniformly at random from the 2^{n-1} polynomials of degree n with $P(0) \neq 0$, then the probability that P is almost irreducible with exponent r is $\frac{1}{r}\left(1 + O(2^{-r/2})\right)$.*

Corollary 9.3 *If $n \geq 1$ and P is chosen uniformly at random from the 2^{n-1} polynomials of degree n with $P(0) \neq 0$, then the probability that P is almost irreducible with some valid exponent is $\ln 2 + O(1/n)$.*

An analogy. There is an analogy between polynomials of degree n and n-digit numbers, with irreducible polynomials corresponding to primes. A result analogous to Corollary 9.3 is: the probability that a random n-digit number has a prime factor exceeding $n/2$ digits is $\ln 2 + O(1/n)$ (see for example [22]).

The density of almost primitive polynomials. The number of primitive polynomials of degree n is $P_n = \phi(2^n - 1)/n$, where ϕ denotes Euler's phi function, see for example Lidl [20]. If I_r is replaced by P_r in Theorem 9.1, then we obtain the number of almost primitive polynomials with exponent r and increment δ. It is easy to deduce an analogue of Corollary 9.2. To obtain an analogue of Corollary 9.3 for almost primitive polynomials we would need to estimate $\sum_{n/2<r\leq n} \phi(2^r - 1)/(r2^r)$. For $n = 1000$ the approximate value is 0.507.

Computational results for trinomials. Let $N_{ait}(n)$ be the number of almost irreducible trinomials $x^n + x^s + 1$ with $0 < s < n$. Consider the smoothed and normalized value $E_{ait}(n) = \frac{2}{n(n-1)} \sum_{m=2}^{n} N_{ait}(m)$. If a result like Corollary 9.3 applies for *trinomials*, at least in the limit as r, $\delta \to \infty$, then it is plausible to conjecture that

$$\lim_{n\to\infty} E_{ait}(n) = c \tag{9.1}$$

for some positive constant c. We have computed $N_{ait}(n)$ and $E_{ait}(n)$ for $n \leq 1000$; the numerical results support the conjecture (9.1) with $c < \ln 2 \approx 0.6931$. For example, $E_{ait}(500) \approx 0.4765$ and $E_{ait}(1000) \approx 0.4713$. For almost primitive trinomials the corresponding limit seems smaller (if it exists). Our computations give $E_{apt}(500) \approx 0.3124$ and $E_{apt}(1000) \approx 0.3104$.

Existence of almost irreducible/primitive trinomials. We have shown by computation that an almost irreducible trinomial of degree n exists for all $n \in [2, 10000]$. Similarly, we have shown that an almost primitive trinomial of degree n exists for all $n \in [2, 2000]\backslash\{12\}$. In the exceptional case (degree 12), $x^{12} + x + 1$ has primitive factors of degrees 3, 4, and 5, but degree 5 is too small, so $x^{12} + x + 1$ is not "almost primitive" by Definition 3.1. The other candidate that is not excluded by Theorem 4.2 is $x^{12} + x^5 + 1$; this is irreducible but not primitive, having period $(2^{12} - 1)/5$.

Rather than asking for an almost irreducible (or almost primitive) trinomial of given degree, we can ask for one of given exponent. This is close to the spirit of [3, 26]. For all $r \in [2, 2000]$ there is an almost irreducible trinomial $x^{r+\delta} + x^s + 1$ with exponent r and (minimal) increment $\delta = \delta_{ait}(r) \leq 23$. The extreme increment $\delta_{ait}(r) = 23$ occurs for $(r, s) = (1930, 529)$, and the mean value of $\delta_{ait}(r)$ for $r \in (1000, 2000]$ is ≈ 2.14. A plausible conjecture is that $\delta_{ait}(r) = O(\log r)$.

Similarly, for all $r \in [2, 712]$ there is an almost primitive trinomial with exponent r and (minimal) increment $\delta_{apt}(r) \leq 43$. The extreme $\delta_{apt}(r) = 43$ occurs for $(r, s) = (544, 47)$, and the mean value of $\delta_{apt}(r)$ for $r \in (356, 712]$ is ≈ 3.41.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[2] I. F. Blake, S. Gao and R. J. Lambert, *Constructive problems for irreducible polynomials over finite fields*, in Information Theory and Applications (A. Gulliver and N. Secord, eds.), Lecture Notes in Computer Science **793**, Springer-Verlag, Berlin, 1994, 1–23.

[3] I. F. Blake, S. Gao and R. Lambert, *Construction and distribution problems for irreducible trinomials over finite fields*, in Applications of Finite Fields (D. Gollmann, ed.), Oxford, Clarendon Press, 1996, 19–32. `www.math.clemson.edu/~sgao/pub.html`

[4] R. P. Brent, *Uniform random number generators for supercomputers*, Proc. Fifth Australian Supercomputer Conference, Melbourne, Dec. 1992, 95–104.

[5] R. P. Brent, *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), 429–451.

[6] R. P. Brent, S. Larvala and P. Zimmermann, *A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377*, Math. Comp. **72** (2003), 1443–1452. Update at `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub199.html`

[7] R. P. Brent and P. Zimmermann, *Random number generators with period divisible by a Mersenne prime*, Proc. ICCSA 2003, Montreal, to appear in Lecture Notes in Computer Science. `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub211.html`

[8] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, third edition, Amer. Math. Soc., Providence, RI, 2002. `http://www.ams.org/online_bks/conm22/`

[9] K. Dalen, *On a theorem of Stickelberger*, Math. Scand. **3**, 124–126, 1955.

[10] L. E. Dickson, *Criteria for the irreducibility of functions in a finite field*, Bulletin Amer. Math. Soc. **13**(1) (1906), 1–8.

[11] S. Gao, *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc. **127**(6) (1999), 1615–1623.

[12] J. von zur Gathen, *Irreducible trinomials over finite fields*, Math. Comp. **71** (2002), 1699–1734.

[13] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge, UK, 1999.

[14] GIMPS, *The Great Internet Mersenne Prime Search*. `http://www.mersenne.org/`

[15] S. W. Golomb, *Shift Register Sequences,* Aegean Park Press, revised edition, 1982.

[16] J. R. Heringa, H. W. J. Blöte and A. Compagner, *New primitive trinomials of Mersenne-exponent degrees for random-number generation*, International J. of Modern Physics C **3** (1992), 561–564.

[17] D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Addison-Wesley, Menlo Park, CA, third edition, 1998.

[18] T. Kumada, H. Leeb, Y. Kurita and M. Matsumoto, *New primitive t-nomials* ($t = 3, 5$) *over* GF(2) *whose degree is a Mersenne exponent*, Math. Comp. **69** (2000), 811–814. Corrigenda: *ibid* **71** (2002), 1337–1338.

[19] Y. Kurita and M. Matsumoto, *Primitive t-nomials* ($t = 3, 5$) *over* GF(2) *whose degree is a Mersenne exponent* ≤ 44497, Math. Comp. **56** (1991), 817–821.

[20] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, Cambridge, second edition, 1994.

[21] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1997. `http://cacr.math.uwaterloo.ca/hac/`

[22] K. K. Norton, *Numbers with small prime factors, and the least k-th power nonresidue,* Memoirs Amer. Math. Soc. **106** (1971), 1–106.

[23] A.-E. Pellet, *Sur la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier p*, Comptes Rendus de l'Académie des Sciences Paris **86** (1878), 1071–1072.

[24] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich, 1897, 182–193.

[25] R. G. Swan, *Factorization of polynomials over finite fields,* Pacific J. Mathematics **12** (1962), 1099–1106.

[26] J. Tromp, L. Zhang and Y. Zhao, *Small weight bases for Hamming codes*, Theoretical Computer Science **181**(2), 1997, 337–345.

[27] N. Zierler, *Primitive trinomials whose degree is a Mersenne exponent,* Information and Control **15** (1969), 67–69.