Almost Irreducible and Almost Primitive Trinomials[*]

Richard P. Brent
Computing Laboratory
University of Oxford, UK
Banff@rpbrent.co.uk

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

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

[*] Presented at Banff, Canada, 26 May 2003.

Abstract

Consider polynomials over GF(2). We define *almost irreducible* and *almost primitive* polynomials, explain why they are useful, and give some examples and conjectures relating to them.

Introduction

Irreducible and primitive polynomials over finite fields have many applications in cryptography, coding theory, random number generation, etc.

For simplicity we restrict our attention to the finite field $\mathbf{Z}_2 = \mathrm{GF}(2)$; the generalization to other finite fields is straightforward. All polynomials are assumed to be in $\mathbf{Z}_2[x]$, and computations on polynomials are performed in $\mathbf{Z}_2[x]$ or in a specified quotient ring.

A polynomial $P(x) \in \mathbf{Z}_2[x]$ may be written as P if the argument x is clear from the context.

We are often concerned with trinomials of the form $T(x) = x^n + x^s + 1$, and in such cases we can assume that $s \le n/2$ (else consider $x^n T(1/x) = x^n + x^{n-s} + 1$).

Definitions

We recall some standard definitions.

Definition 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 $\rho \bmod P(x)$.*

Definition 2 *A polynomial $P(x)$ is* reducible *if it has nontrivial factors; otherwise it is* irreducible.

Definition 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 $P(x) \in \mathbf{Z}_2[x]$.)*

If $P(x)$ is primitive, then x is a generator for the multiplicative group of the field $\mathbf{Z}_2[x]/P(x)$, giving a concrete representation of $\mathrm{GF}(2^n)$.

Almost irreducible/primitive polynomials

Tromp, Zhang and Zhao [20] 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 $r \leq 171$, and conjectured that the answer is always "yes".

Blake, Gao and Lambert [2] confirmed the conjecture for $r \leq 500$. 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 [2], we make some definitions.

Definition 4 *A polynomial $P(x)$ of degree n is* almost primitive (almost irreducible) *if $P(0) \neq 0$ 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 $n - r$.

Special cases

Note that, according to Definition 4, 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.

A small example

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

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

where

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

is primitive.

Representing finite fields

$\mathbf{Z}_2[x]/D(x)$ represents the finite field $\mathrm{GF}(2^{13})$, but from a computational viewpoint it is more efficient to work in the ring $\mathbf{Z}_2[x]/(x^{16} + x^3 + 1)$ than in the field $F = \mathbf{Z}_2[x]/D(x)$.

We shall outline how it is possible to work in the field F, while performing most arithmetic in the ring $\mathbf{Z}_2[x]/(x^{16} + x^3 + 1)$, and without explicitly computing the dense primitive polynomial $D(x)$.

We can not replace $D(x)$ by a primitive trinomial of degree 13, because such a trinomial does not exist! We could use a primitive pentanomial of degree 13, but this would be less efficient than using an almost primitive trinomial of degree 16.

Long-period linear recurrences

The linear recurrence

$$z_n = z_{n-16} + z_{n-3} \bmod 2$$

has a generating function of the form

$$\frac{A(x)}{x^3 + x^2 + 1} + \frac{B(x)}{D(x)},$$

where the polynomials A and B are determined by $z_0, \ldots, z_{15}$.

Provided we ensure that $B \neq 0$ (easily done), the period of the sequence (z_n) will be a multiple of $2^{13} - 1$.

Similar sequences could be useful in cryptographic applications, and for random number generation.

We see that, for many practical purposes, almost primitive trinomials of exponent r and small increment are almost as useful as primitive trinomials of degree r.

Swan's theorem and its implications

Swan's theorem is a rediscovery of 19th century results. Let $\nu(P)$ denote the number of irreducible factors (counted according to their multiplicity) of a polynomial $P \in \mathbf{Z}_2[x]$.

Theorem 1 Swan [19, 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, $n \neq 2s$, $ns/2 \bmod 4 \in \{0, 1\}$;
b) $2n \neq 0 \bmod s$, $n = \pm 3 \bmod 8$;
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), 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 1 *If n is prime, $n = \pm 3 \bmod 8$, $s \neq 2$, $s \neq n - 2$, then $x^n + x^s + 1$ is reducible over $\mathbf{Z}_2$.*

Corollary 1 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.

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. This is considerably more expensive, because the number of operations required for multiplication or division by a sparse polynomial is approximately proportional to the number of nonzero terms.

Fortunately, we can circumvent Swan's theorem by using almost irreducible trinomials.

A large example

Let $T(x) = x^{2976229} + x^{1193004} + 1$. Then a computation shows that

$$T(x) = S(x)D(x) ,$$

where

$$S(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$$

is irreducible of degree 8, and $D(x)$ is irreducible of degree 2976221.

NTL can verify these statements in less than ten hours on a fast PC.

Since 2976221 is a Mersenne exponent, $D(x)$ is primitive.

Since $D(x)$ is dense, with about 1.5×10^6 nonzero terms, we shall not try to write it out explicitly!

By Swan's theorem, there is no irreducible trinomial of degee 2976221.

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

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

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

$$A = A_c + A_d D,$$

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

Implicit algorithms cont.

We can perform computations such as addition, multiplication and exponentiation in $\mathbf{Z}_2[x]/T(x)$, taking advantage of the sparsity of T in the usual way.

If $A \in \mathbf{Z}_2[x]/T(x)$ 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.

Finding almost irreducible trinomials

In the spirit of implicit algorithms, we can modify the standard algorithms for finding irreducible trinomials for the almost irreducible case. Details are given in our paper[1] in the Proceedings (Algorithm AIT).

Similarly for almost primitive trinomials, assuming that the complete factorization of $2^r - 1$ is known (where r is the exponent, i.e. the degree of the large irreducible factor).

[1] Preprint at `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub212.html`

Algorithm AIT – preliminaries

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. If it is not then we discard it, and (perhaps) try again with different (r, s, δ).

Input to the algorithm is (r, s, δ) and a sieving bound $B \in [\delta, r)$.

Recall that polynomials are in $\mathbf{Z}_2[x]$, so computations on polynomials are performed in $\mathbf{Z}_2[x]$ or in a quotient ring such as $\mathbf{Z}_2[x]/T(x)$.

Algorithm AIT follows on the next slide. For the justification of each step, and various extensions and refinements, see §4 of the Proceedings paper.

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 $\delta$ 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 $((x^{2^r} \bmod T) + x)S \ne 0 \bmod T$ then
   return false.

6. for each prime divisor $p \ne r$ of $r$
       if $\gcd(((x^{2^{r/p}} \bmod T) + x)S, T) \ne S$
   then return false.

7. return true. [$T$ is almost irreducible with
   exponent $r$.]
```

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 $r < 10^7$, primitive trinomials of degree r are known, see [4]. 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 $r < 2976221$.

For each Mersenne exponent $r < 10^7$, there is an almost primitive trinomial with exponent r and increment $\delta \leq 12$ (allowing the case $\delta = 0$ if a primitive trinomial of degree r exists).

The new results for $r = \pm 3 \bmod 8$, where $500 < r < 10^7$, are summarized in Table 1.

Table 1 – Mersenne exponents

r	δ	s	f
2203	3	355	7
4253	8	1806	255
		1960	85
9941	3	1077	7
11213	6	227	63
21701	3	6999	7
		7587	7
86243	2	2288	3
216091	12	42930	3937
1257787	3	74343	7
1398269	5	417719	21
2976221	8	1193004	85

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

The Fermat connection

Another case of interest is when r is a power of two, say $r = 2^k$. Then

$$2^r - 1 = F_0 F_1 \cdots F_{k-1},$$

where $F_j = 2^{2^j} + 1$ is the j-th Fermat number. The complete factorizations of these F_j are known for $j \leq 11$, so we can factor $2^{2^k} - 1$ for $k \leq 12$.

In Table 2 we give almost primitive trinomials $T = x^{r+\delta} + x^s + 1$ with exponent $r = 2^k$ for $3 \leq k \leq 12$. Thus $T = SD$, where D is primitive and has degree 2^k. 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 $k \geq 3$. 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 implicit algorithms.

Table 2 – power of 2 exponents

k	r	δ	s	f
3	8	5	1	31
			2	7
4	16	11	2	7
5	32	8	3	1
6	64	10	3	21
			21	341
7	128	2	17	1
8	256	16	45	1
9	512	9	252	31
10	1024	3	22	7
11	2048	10	101	341
12	4096	3	600	7
			628	7
			1399	7

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

Existence questions – given degree

We have shown by computation that an almost irreducible trinomial of degree n exists for all $n \in [2, 10000]$. We conjecture that this holds for all $n > 1$.

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 our Definition. The other candidate that is not easily excluded is $x^{12} + x^5 + 1$; this is irreducible but not primitive, having period $(2^{12} - 1)/5$.

Existence questions – given exponent

For all $r \in [2, 2000]$ there is an almost irreducible trinomial $x^{r+\delta} + x^s + 1$ with exponent r and (minimal) increment $\delta = \delta_{ait}(r) \le 23$. 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 $\delta_{apt}(r) \le 43$. 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.

We can not go any further (at least not rigorously) because the complete factorization of $2^{713} - 1$ is not known.

References

[1] 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.), LNCS **793**, Springer-Verlag, Berlin, 1994, 1–23.

[2] 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`

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

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

[5] R. P. Brent and P. Zimmermann, *Random number generators with period divisible by a Mersenne prime*, Proc. ICCSA 2003, Montreal, to appear in LNCS. Preprint at `.../pub211.html`

[6] 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/`

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

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

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

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

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

[12] 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.

[13] 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.

[14] 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.

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

[16] 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/`

[17] 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.

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

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

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

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