The Great Trinomial Hunt: an Update

Richard P. Brent
MSI, ANU and
CARMA, Newcastle

joint work with
Paul Zimmermann
INRIA, Nancy

8 April 2016

Introduction

In 2011 we[1] published *The Great Trinomial Hunt*. In this talk I will bring you up to date with recent results of the "hunt".

Questions about the integers often suggest analogous (but in many cases easier) questions about polynomials over finite fields.

For example, the unique prime factorisation theorem for positive integers corresponds to unique factorisation of polynomials into irreducible polynomials (modulo multiplication by units).

There is a polynomial-time factorisation algorithm for polynomials over finite fields, but no such polynomial-time factorisation algorithm is known for the integers.

[1] Brent & Zimmermann, *Notices of the AMS* **58** (2011), 233–239.

Polynomials over finite fields

We consider univariate polynomials $P(x)$ over a finite field F. The algorithms apply, with minor changes, for any small positive characteristic, but in this talk we assume that the characteristic is 2, and $F = \mathbb{Z}/2\mathbb{Z} = \mathrm{GF}(2)$.

$P(x)$ is *irreducible* if it has no nontrivial factors. If $P(x)$ is irreducible of degree r, then [Gauss]

$$x^{2^r} = x \bmod P(x).$$

Thus $P(x)$ divides the polynomial $\mathcal{P}_r(x) = x^{2^r} - x$. In fact, $\mathcal{P}_r(x)$ is the product of all irreducible polynomials of degree d, where d runs over the divisors of r.

Counting irreducible polynomials

Let $N(d)$ be the number of irreducible polynomials of degree d. Thus

$$\sum_{d|r} dN(d) = \deg(\mathcal{P}_r) = 2^r \ .$$

By Möbius inversion we see that

$$rN(r) = \sum_{d|r} \mu(d) 2^{r/d} \ .$$

Thus, the number of irreducible polynomials of degree r is

$$N(r) = \frac{2^r}{r} + O\left(\frac{2^{r/2}}{r}\right) .$$

Since there are 2^r polynomials of degree r, the probability that a randomly selected polynomial is irreducible is $\sim 1/r \to 0$ as $r \to +\infty$. *Almost all* polynomials over (fixed) finite fields are reducible (unlike polynomials over the integers).

Analogy

Irreducible polynomials are analogous to primes.
Polynomials of degree r are analogous to integers of r *digits*.

By the prime number theorem, the number of r-digit primes in base 2 is about

$$\int_{2^{r-1}}^{2^r} \frac{dt}{\ln t}.$$

The Riemann Hypothesis implies an error term $O(r2^{r/2})$ as $r \to +\infty$ [von Koch].

On the other hand, we saw on the previous slide an easily-proved error term $O(r^{-1}2^{r/2})$ in the polynomial case.

Representing finite fields, and primitive polynomials

Irreducible polynomials over finite fields are useful in several applications. As one example, observe that, if $P(x)$ is an irreducible polynomial of degree r over $\mathrm{GF}(2)$, then

$$\mathrm{GF}(2)[x]/P(x) \cong \mathrm{GF}(2^r).$$

In other words, the ring of polynomials mod $P(x)$ gives a representation of the finite field with 2^r elements.

If, in addition, x is a generator of the multiplicative group, that is if every nonzero element of $\mathrm{GF}(2)[x]/P(x)$ can be represented as a power of x, then $P(x)$ is said to be *primitive*.

Warning: there are several different meanings of "primitive" in the literature. In the context of polynomials over $\mathrm{GF}(2)$ this meaning seems to be standard.

Primitive polynomials and shift registers

Primitive polynomials can be used to obtain linear feedback shift registers (LFSRs) with maximal period $2^r - 1$, where r is the degree of the polynomial. These have applications to stream ciphers and pseudo-random number generators.

Testing primitivity can be difficult, because we need to know the prime factorisation of $2^r - 1$. Of course, this is trivial if $2^r - 1$ is prime (a *Mersenne prime*).

The number of primitive polynomials of degree r over $\mathrm{GF}(2)$ is

$$\frac{\phi(2^r - 1)}{r} \le N(r) \le \frac{2^r - 2}{r},$$

with equality when $2^r - 1$ is prime.

Sparsity

In applications we usually want $P(x)$ to be *sparse*, that is to have only a small number of nonzero coefficients, for reasons of efficiency. The binomial case is usually trivial, so in most cases we want $P(x)$ to be a *trinomial*

$$x^r + x^s + 1\,, \quad r > s > 0\,.$$

In stating computational results we always assume that $s \le r/2$, since for any trinomial $T(x) = x^r + x^s + 1$ there is a "reciprocal" trinomial $x^r T(1/x) = x^r + x^{r-s} + 1$ with the same reducibility/primitivity properties as $T(x)$.

Mersenne primes

A *Mersenne prime* is a prime of the form $2^n - 1$, for example $3, 7, 31, 127, 8191, \ldots$.

There are *conjectured* to be infinitely many Mersenne primes, and the number for $n \leq N$ is conjectured to be of order $\log N$.

The GIMPS project is searching systematically for Mersenne primes. So far 49 Mersenne primes are known, the largest being

$$2^{74207281} - 1 \ .$$

If $2^n - 1$ is prime we say that n is a *Mersenne exponent*. A Mersenne exponent is necessarily prime, but not conversely (e.g. $2^{11} - 1 = 23 \times 89$ so 11 is not a Mersenne exponent).

Trinomials whose degree is a Mersenne exponent

In the following we consider mainly trinomials

$$T(x) = x^r + x^s + 1$$

where $r > s > 0$ and r is a Mersenne exponent (so $2^r - 1$ is prime). If $T(x)$ is irreducible it is necessarily primitive.

Primitive trinomials are analogous to primes of a special form. Various properties can be conjectured using probabilistic models, but nontrivial properties that can currently be proved are rare.

A useful and nontrivial result on trinomials is Swan's theorem.

Historical note: Swan (1962) rediscovered results of Pellet (1878) and Stickelberger (1897), so the name of the theorem depends on your nationality.

Theorem 1 [Swan]

Let $r > s > 0$, and assume $r + s$ is odd. Then $T_{r,s}(x) = x^r + x^s + 1$ has an even number of irreducible factors over $\mathrm{GF}(2)$ in the following cases:
a) r even, $r \neq 2s$, $rs/2 = 0$ or $1 \bmod 4$.
b) r odd, s not a divisor of $2r$, $r = \pm 3 \bmod 8$.
c) r odd, s a divisor of $2r$, $r = \pm 1 \bmod 8$.
In all other cases $x^r + x^s + 1$ has an odd number of irreducible factors.

Remark

If both r and s are even, then $T_{r,s}$ is a square. If both r and s are odd, we can apply the theorem to $T_{r,r-s}$. Thus, Theorem 1 tells us the parity of the number of irreducible factors of *any* trinomial over $\mathrm{GF}(2)$.

Application of Swan's theorem

For r an odd prime, and excluding the easily-checked cases $s = 2$ or $r - 2$, case (b) of Swan's theorem says that the trinomial has an even number of irreducible factors, and hence must be reducible, if $r = \pm 3 \bmod 8$.

Thus, we only need to consider those Mersenne exponents r with $r = \pm 1 \bmod 8$.

Of the 48 known Mersenne exponents other than 2, there are 29 with $r = \pm 1 \bmod 8$ and 19 with $r = \pm 3 \bmod 8$.

A condition for irreducibility

$P(x)$ of degree $r > 1$ is irreducible iff

$$x^{2^r} = x \bmod P(x)$$

and, for all prime divisors d of r, we have

$$\mathrm{GCD}\left(x^{2^{r/d}} - x, P(x)\right) = 1 \ .$$

The second condition is required to rule out the possibility that $P(x)$ is a product of irreducible factors of some degree(s) $k = r/d$, where $d > 1$ and $d|r$.

In our examples r is a Mersenne exponent, hence prime, so the second condition can be omitted, and $P(x)$ is irreducible iff

$$x^{2^r} = x \bmod P(x).$$

A brief comment on algorithms

Unfortunately, there is no time to discuss algorithms for testing irreducibility and factoring (reducible) polynomials over $\mathrm{GF}(2)$.

If you are interested in such algorithms, see the bibliography at the end of this talk, and the slides related to "The Great Trinomial Hunt" on my website `http://maths-people.anu.edu.au/~brent/talks.html#CARMA1`

Our algorithms do not depend on the assumption that the degree r is a Mersenne exponent. This assumption is only required to deduce that an irreducible factor is primititive.

Irreducible and primitive trinomials

We have given formulas for the number of irreducible or primitive *polynomials* of degree r over $\mathrm{GF}(2)$, but there is no known formula for the number of irreducible or primitive *trinomials*.

Since the number of irreducible polynomials $N(r) \approx 2^r/r$, the probability that a randomly chosen polynomial of degree r will be irreducible is about $1/r$.

It is *plausible* to assume that the same applies to trinomials. There are $r-1$ trinomials of degree r, so we might expect $O(1)$ of them to be irreducible. More precisely, we might expect a Poisson distribution with some constant mean μ.

This plausible argument is too simplistic, as shown by Swan's theorem. However, we might expect a Poisson distribution in the cases that are not ruled out by Swan's theorem (i.e. the cases $r = \pm 1 \bmod 8$).

Implications of Swan's Theorem

For r an odd prime, case (b) of Swan's Theorem says that the trinomial has an *even* number of irreducible factors, and hence must be *reducible*, if $r = \pm 3 \bmod 8$, provided we exclude the special cases $s = 2$ and $r - s = 2$.

For prime $r = \pm 1 \bmod 8$, the heuristic Poisson distribution seems to apply [based on computations for prime $r < 1000$], with mean $\mu \approx 3$. Similarly for primitive trinomials, with a correction factor $\phi(2^r - 1)/(2^r - 2)$.

Recent computational results

The history of the search for primitive trinomials is described in our 2011 AMS Notices paper. Here we give new results for the two Mersenne exponents found by GIMPS in 2013 and 2016.

r	s	date
57 885 161	none	25/1-3/4/2013
74 207 281	9 156 813, 9 999 621, 30 684 570	28/1-23/3/2016

Table: Three new primitive trinomials $x^r + x^s + 1$, $s \le r/2$.

Note that $57885161 \equiv 1 \bmod 8$ so this exponent is *not* ruled out by Swan's theorem. This is the only known Mersenne exponent for which Swan's theorem permits a primitive trinomial but none exists. This should not have been a surprise, because the phenomenon occurs for other prime exponents, e.g. 311.

Reproducibility — aka quality assurance

How can we be sure that we have found all the primitive trinomials of a given degree r? In particular, how can we be sure that there are no primitive trinomals of degree 57885161?

Our programs produce an easily-verified "certificate" for each reducible trinomial $T(x) = x^r + x^s + 1$. The certificate is just an encoding of a smallest nontrivial factor of $T(x)$. To ensure uniqueness (which is useful for program debugging), the lexicographically least such factor is given if there are several factors of equal smallest degree.

The certificates can be verified (much faster than the original computation) using an independent NTL or Magma program.

We remark that earlier authors did not go to the trouble of producing certificates of reducibility, and in at least one case a primitive trinomial was missed because of a software error.

The number of primitive trinomials of given degree

The table gives the precise number of primitive trinomials $x^r + x^s + 1$ for given (Mersenne exponent) r and $s \le r/2$. The known Mersenne exponents $r > 3 \times 10^6$ are listed.

degree r	number	notes
3 021 377	2	
6 972 593	1	
13 466 917	0	Swan's thm
20 996 011	0	Swan's thm
24 036 583	2	
25 964 951	4	
30 402 457	1	
32 582 657	3	
37 156 667	0	Swan's thm
42 643 801	5	
43 112 609	4	
57 885 161	0	exceptional
74 207 281	3	

Table: Counts of primitive trinomials of degree r

Distribution of degrees of factors

In order to predict the expected behaviour of our algorithms, we need to know the expected distribution of degrees of irreducible factors. Our complexity estimates are based on the assumption that trinomials of degree r behave like the set of all polynomials of the same degree, up to a constant factor:

Assumption 1. Over all trinomials $x^r + x^s + 1$ of degree r over $\mathrm{GF}(2)$, the probability π_d that a trinomial has no nontrivial factor of degree $\le d$ is at most c/d, where c is a constant and $1 < d \le r/\ln r$.

This assumption is plausible and in agreement with experiments, though not proven.

Some empirical evidence for Assumption 1 in the case $r = 6\,972\,593$ is given on the next slide. Results for other large Mersenne exponents are similar.

Statistics for $r = 6972593$

d	$d\pi_d$
2	1.33
3	1.43
4	1.52
5	1.54
6	1.60
7	1.60
8	1.67
9	1.64
10	1.65
100	1.77
1000	1.76
10000	1.88
100000	1.62
226887	2.08 (max)
$r-1$	2.00

Analogies

The following have similar distributions in the limit as $n \to \infty$:

1. Degree of smallest irreducible factor of a random monic polynomial of degree n over a finite field (say $\mathrm{GF}(2)$).
2. Size of smallest cycle in a random permutation of n objects.
3. Size (in base-b digits) of smallest prime factor in a random integer of n digits.

Analogies — more details

More precisely, let P_d be the limiting probability that the smallest irreducible factor has degree $> d$, that the smallest cycle has length $> d$, or that the smallest prime factor has $> d$ digits, in cases 1–3 respectively. Then

$$P_d \sim c/d \quad \text{as} \quad d \to \infty$$

(the constant c is different in each case).

For example, in case 3, let $x = b^d$; then

$$P_d = \prod_{\text{prime } p<x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln x} = \left(\frac{e^{-\gamma}}{\ln b}\right) \frac{1}{d}$$

by the theorem of Mertens.

Remarks on complexity

Using Assumption 1, we can show that the search for primitive trinomials of Mersenne exponent degree r takes time

$$\widetilde{O}(r^2),$$

where the tilde indicates that logarithmic factors are neglected.

This is the same complexity (up to logarithmic factors) as the verification of a single Mersenne exponent r. Thus GIMPS has a harder task than we do. Whenever GIMPS finds a new Mersenne exponent, we should be able to find the primitive trinomials of that degree within a few months.

We remark that the correctness of our algorithms is independent of Assumption 1. The assumption only affects the expected running time of the algorithms.

The largest smallest factor

For each of the 37 103 637 reducible trinomials of degree $r = 74\,207\,281$, we know a smallest factor, and these factors have been verified using Magma.

The largest smallest factor F is a factor of degree $d = 19\,865\,299$ of the trinomial $T = x^r + x^s + 1$ with $s = 9\,788\,851$.

We can not display F explicitly, since it is a dense polynomial of degree d.

Since $5d > r$, it follows from Swan's theorem that T has precisely three irreducible factors. We are currently searching for the second-largest factor, which will suffice to give the complete factorisation of T.

Acknowledgements

Thanks to the `gf2x` team for helping to speed up our software, and to Allan Steel for verifying many of our primitive trinomials using Magma.

INRIA and the Australian National University provided computing facilities for the new results reported here.

We thank the ARC for support under grant DP140101417.

Bibliography

W. Bosma and J. Cannon, *Handbook of Magma Functions*, School of Mathematics and Statistics, University of Sydney, 1995. `http://magma.maths.usyd.edu.au/`

R. P. Brent, P. Gaudry, E. Thomé and P. Zimmermann, Faster multiplication in $GF(2)[x]$, *Proc. ANTS VIII 2008*, *Lecture Notes in Computer Science* **5011**, 153–166.

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.

R. P. Brent, S. Larvala and P. Zimmermann, A primitive trinomial of degree 6972593, *Math. Comp.* **74** (2005), 1001–1002,

R. P. Brent and P. Zimmermann, A multi-level blocking distinct-degree factorization algorithm, *Finite Fields and Applications: Contemporary Mathematics* **461** (2008), 47–58.

R. P. Brent and P. Zimmermann, Ten new primitive binary trinomials, *Math. Comp.* **78** (2009), 1197–1199.

R. P. Brent and P. Zimmermann, The great trinomial hunt, *Notices of the AMS* **58** (2011), 233–239.

J. von zur Gathen and V. Shoup, Computing Frobenius maps and factoring polynomials, *Computational Complexity* **2** (1992), 187–224.

T. Kumada, H. Leeb, Y. Kurita and M. Matsumoto, New primitive t-nomials ($t = 3, 5$) over $\mathrm{GF}(2)$ whose degree is a Mersenne exponent, *Math. Comp.* **69** (2000), 811–814. (They missed $x^{859433} + x^{170340} + 1$.) Corrigenda: *ibid* **71** (2002), 1337–1338.

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.

A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2, *Acta Informatica* **7** (1977), 395–398.

V. Shoup, NTL: A library for doing number theory. `http:www.shoup.net/ntl/`

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

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

S. Wagstaff, Jr., The Cunningham Project. `http://homes.cerias.purdue.edu/~ssw/cun/`

G. Woltman *et al.*, GIMPS, The Great Internet Mersenne Prime Search. `http://www.mersenne.org/`