Primitive trinomials
and record nontrivial factorizations
of polynomials over GF(2)

Richard P. Brent
ANU & CARMA

joint work with
Paul Zimmermann
INRIA, Nancy

CARMA Retreat
17 August 2013
Very Brief Introduction

• $\text{GF}(2) = \mathbb{Z}/2\mathbb{Z}$ is the field with two elements $\{0, 1\}$ and operations of addition and multiplication mod 2.
Very Brief Introduction

- \( \text{GF}(2) = \mathbb{Z}/2\mathbb{Z} \) is the field with two elements \( \{0, 1\} \) and operations of addition and multiplication mod 2.
- A polynomial over \( \text{GF}(2) \) is a polynomial in \( \text{GF}(2)[x] \), that is a polynomial whose coefficients are in \( \text{GF}(2) \).
Very Brief Introduction

- \( \text{GF}(2) = \mathbb{Z}/2\mathbb{Z} \) is the field with two elements \{0, 1\} and operations of addition and multiplication mod 2.

- A polynomial over \( \text{GF}(2) \) is a polynomial in \( \text{GF}(2)[x] \), that is a polynomial whose coefficients are in \( \text{GF}(2) \). From now on all polynomials are assumed to be over \( \text{GF}(2) \).
Very Brief Introduction

- **GF(2) = \( \mathbb{Z}/2\mathbb{Z} \)** is the field with two elements \( \{0, 1\} \) and operations of addition and multiplication mod 2.
- A polynomial over GF(2) is a polynomial in GF(2)[x], that is a polynomial whose coefficients are in GF(2). From now on all polynomials are assumed to be over GF(2).
- A trinomial is a polynomial with three nonzero coefficients, e.g. \( x^7 + x^3 + 1 \).
Very Brief Introduction

- \(\text{GF}(2) = \mathbb{Z}/2\mathbb{Z}\) is the field with two elements \(\{0, 1\}\) and operations of addition and multiplication mod 2.
- A polynomial over \(\text{GF}(2)\) is a polynomial in \(\text{GF}(2)[x]\), that is a polynomial whose coefficients are in \(\text{GF}(2)\). From now on all polynomials are assumed to be over \(\text{GF}(2)\).
- A trinomial is a polynomial with three nonzero coefficients, e.g. \(x^7 + x^3 + 1\).
- A trinomial is the generating function for a 3-term recurrence, e.g. \(x_n = x_{n-3} + x_{n-7}, n \geq 0\).
Very Brief Introduction

- **GF(2) = \( \mathbb{Z}/2\mathbb{Z} \)** is the field with two elements \{0, 1\} and operations of addition and multiplication mod 2.

- A polynomial over GF(2) is a polynomial in GF(2)[x], that is a polynomial whose coefficients are in GF(2). From now on all polynomials are assumed to be over GF(2).

- A trinomial is a polynomial with three nonzero coefficients, e.g. \( x^7 + x^3 + 1 \).

- A trinomial is the generating function for a 3-term recurrence, e.g. \( x_n = x_{n-3} + x_{n-7}, \ n \geq 0 \).

- A polynomial is irreducible if it has no nontrivial factors.
Very Brief Introduction

- \( \mathbb{GF}(2) = \mathbb{Z}/2\mathbb{Z} \) is the field with two elements \{0, 1\} and operations of addition and multiplication mod 2.
- A polynomial over \( \mathbb{GF}(2) \) is a polynomial in \( \mathbb{GF}(2)[x] \), that is a polynomial whose coefficients are in \( \mathbb{GF}(2) \). From now on all polynomials are assumed to be over \( \mathbb{GF}(2) \).
- A trinomial is a polynomial with three nonzero coefficients, e.g. \( x^7 + x^3 + 1 \).
- A trinomial is the generating function for a 3-term recurrence, e.g. \( x_n = x_{n-3} + x_{n-7}, \, n \geq 0 \).
- A polynomial is irreducible if it has no nontrivial factors.
- A polynomial is primitive if it is irreducible and satisfies a certain technical condition (see later).
Very Brief Introduction

- $\text{GF}(2) = \mathbb{Z}/2\mathbb{Z}$ is the field with two elements $\{0, 1\}$ and operations of addition and multiplication mod 2.

- A polynomial over $\text{GF}(2)$ is a polynomial in $\text{GF}(2)[x]$, that is a polynomial whose coefficients are in $\text{GF}(2)$. From now on all polynomials are assumed to be over $\text{GF}(2)$.

- A trinomial is a polynomial with three nonzero coefficients, e.g. $x^7 + x^3 + 1$.

- A trinomial is the generating function for a 3-term recurrence, e.g. $x_n = x_{n-3} + x_{n-7}$, $n \geq 0$.

- A polynomial is irreducible if it has no nontrivial factors.

- A polynomial is primitive if it is irreducible and satisfies a certain technical condition (see later).

- If a trinomial of degree $n$ is primitive then the corresponding recurrence has period $2^n - 1$ for any nonzero initial vector $(x_0, \ldots, x_{n-1})$. 

Richard Brent

Introduction
Hardware Implementation of a Recurrence

It is easy to build hardware to implement the recurrence corresponding to a trinomial $x^n + x^s + 1$. We need a shift register capable of storing $n$ bits, and a circuit capable of computing the addition mod 2 ("exclusive or") of two bits separated by $n - s$ positions and feeding the output back.
Hardware Implementation of a Recurrence

It is easy to build hardware to implement the recurrence corresponding to a trinomial $x^n + x^s + 1$. We need a shift register capable of storing $n$ bits, and a circuit capable of computing the addition mod 2 (“exclusive or”) of two bits separated by $n - s$ positions and feeding the output back. For example, with $n = 7$, $s = 3$:

![Diagram of recurrence implementation]

Output
An irreducible polynomial $P$ of degree $n > 0$ is primitive iff $P(x) \neq x$ and the residue classes $x^k \mod P$, $0 \leq k < 2^n - 1$, are distinct.
An irreducible polynomial $P$ of degree $n > 0$ is primitive iff $P(x) \neq x$ and the residue classes $x^k \mod P$, $0 \leq k < 2^n - 1$, are distinct.

In other words, $P$ is primitive if $x$ is a generator of the multiplicative group of $\text{GF}(2^n) \simeq \text{GF}(2)[x]/P(x)$. 

Richard Brent
An irreducible polynomial $P$ of degree $n > 0$ is primitive iff $P(x) \neq x$ and the residue classes $x^k \mod P$, $0 \leq k < 2^n - 1$, are distinct.

In other words, $P$ is primitive if $x$ is a generator of the multiplicative group of $\mathbb{GF}(2^n) \simeq \mathbb{GF}(2)[x]/P(x)$.

In order to check primitivity of an irreducible polynomial $P(x) \neq x$, it is only necessary to check that $x^k \neq 1 \mod P$ for those $k$ that are maximal non-trivial divisors of $2^n - 1$. 
Primitive Polynomials

An irreducible polynomial $P$ of degree $n > 0$ is **primitive** iff $P(x) \neq x$ and the residue classes $x^k \mod P$, $0 \leq k < 2^n - 1$, are distinct.

In other words, $P$ is primitive if $x$ is a generator of the multiplicative group of $GF(2^n) \cong GF(2)[x]/P(x)$.

In order to check primitivity of an irreducible polynomial $P(x) \neq x$, it is only necessary to check that $x^k \neq 1 \mod P$ for those $k$ that are maximal non-trivial divisors of $2^n - 1$.

For example, $x^6 + x^3 + 1$ is irreducible but not primitive, since $x^9 = 1 \mod (x^6 + x^3 + 1)$. 
Use of Mersenne primes

To test the primitivity of a polynomial of degree $n$ we need to be able to factorize $2^n - 1$. In general, this is difficult if $n$ is larger than about 1200.
Use of Mersenne primes

To test the primitivity of a polynomial of degree $n$ we need to be able to factorize $2^n - 1$. In general, this is difficult if $n$ is larger than about 1200.

The Cunningham Project has factored $2^n - 1$ for all $n < 991$ (as of 31 July 2013), and some other $n \leq 2400$. 

Examples: $M_1 = 2^2 - 1$, $M_2 = 2^3 - 1$, ..., $M_{47} = 2^{43112609} - 1$ (the numbering assumes there are no unknown Mersenne primes smaller than $M_{47}$).

Since the year 2000, whenever the GIMPS Project has found a new Mersenne prime, Paul Zimmermann and I have searched (successfully) for a primitive trinomial whose degree is the same as the Mersenne exponent.
Use of Mersenne primes

To test the primitivity of a polynomial of degree $n$ we need to be able to factorize $2^n - 1$. In general, this is difficult if $n$ is larger than about 1200.

The Cunningham Project has factored $2^n - 1$ for all $n < 991$ (as of 31 July 2013), and some other $n \leq 2400$.

If $2^n - 1$ is a prime then the factorization problem goes away. The GIMPS Project looks for primes of the form $2^n - 1$, known as Mersenne primes after Marin Mersenne (1588–1648).
Use of Mersenne primes

To test the primitivity of a polynomial of degree \( n \) we need to be able to factorize \( 2^n - 1 \). In general, this is difficult if \( n \) is larger than about 1200.

The Cunningham Project has factored \( 2^n - 1 \) for all \( n < 991 \) (as of 31 July 2013), and some other \( n \leq 2400 \).

If \( 2^n - 1 \) is a prime then the factorization problem goes away. The GIMPS Project looks for primes of the form \( 2^n - 1 \), known as Mersenne primes after Marin Mersenne (1588–1648).

Examples: \( M_1 = 2^2 - 1 \), \( M_2 = 2^3 - 1 \), \ldots, \( M_{47} = 2^{43112609} - 1 \) (the numbering assumes there are no unknown Mersenne primes smaller than \( M_{47} \)).
Use of Mersenne primes

To test the primitivity of a polynomial of degree $n$ we need to be able to factorize $2^n - 1$. In general, this is difficult if $n$ is larger than about 1200.

The Cunningham Project has factored $2^n - 1$ for all $n < 991$ (as of 31 July 2013), and some other $n \leq 2400$.

If $2^n - 1$ is a prime then the factorization problem goes away. The GIMPS Project looks for primes of the form $2^n - 1$, known as Mersenne primes after Marin Mersenne (1588–1648).

Examples: $M_1 = 2^2 - 1, M_2 = 2^3 - 1, \ldots, M_{47} = 2^{43112609} - 1$ (the numbering assumes there are no unknown Mersenne primes smaller than $M_{47}$).

Since the year 2000, whenever the GIMPS Project has found a new Mersenne prime, Paul Zimmermann and I have searched (successfully) for a primitive trinomial whose degree is the same as the Mersenne exponent.
Swan’s theorem [Swan, 1962] tells us the parity of the number of irreducible factors of a trinomial $x^n + x^s + 1$, $0 < s < n$. 
Reducing the Search Space

Swan’s theorem [Swan, 1962] tells us the parity of the number of irreducible factors of a trinomial $x^n + x^s + 1$, $0 < s < n$. The theorem reduces the search for primitive trinomials of Mersenne exponent degree $n > 5$ to the cases $n \equiv \pm 1 \mod 8$, because in other cases the trinomial has an even number of irreducible factors (unless $s = \pm 2 \mod n$, and this special case is usually easy to check).
Swan’s theorem [Swan, 1962] tells us the parity of the number of irreducible factors of a trinomial $x^n + x^s + 1$, $0 < s < n$. The theorem reduces the search for primitive trinomials of Mersenne exponent degree $n > 5$ to the cases $n \equiv \pm 1 \mod 8$, because in other cases the trinomial has an even number of irreducible factors (unless $s = \pm 2 \mod n$, and this special case is usually easy to check).

Also, $x^n + x^s + 1$ is primitive iff the reciprocal trinomial $x^n + x^{n-s} + 1$ is primitive, so we can assume that $2s \leq n$. 
Of the 47 Mersenne exponents derived from $M_1, \ldots, M_{47}$, there are 17 that are ruled out by Swan’s theorem. For each of the remaining 30 “eligible” exponents\(^1\) there is at least one primitive trinomial.

\(^1\)This includes the small exponents 2, 3, 5.
Of the 47 Mersenne exponents derived from $M_1, \ldots, M_{47}$, there are 17 that are ruled out by Swan’s theorem. For each of the remaining 30 “eligible” exponents\(^1\) there is at least one primitive trinomial.

For example, $M_{47} = 2^{43112609} - 1$, and a primitive trinomial of degree 43112609 (found October 2008) is

$$x^{43112609} + x^{21078848} + 1$$

(there are 3 others, not counting reciprocal trinomials).

\(^1\)This includes the small exponents 2, 3, 5.
Empirical Observation

If we consider Mersenne exponents \( n \equiv \pm 1 \mod 8 \) and trinomials \( x^n + x^s + 1, \ 2s \leq n \), then the number of primitive (or irreducible) trinomials of given degree \( n \) appears to have a Poisson distribution with mean about 3.07.
If we consider Mersenne exponents $n \equiv \pm 1 \mod 8$ and trinomials $x^n + x^s + 1$, $2s \leq n$, then the number of primitive (or irreducible) trinomials of given degree $n$ appears to have a Poisson distribution with mean about 3.07.

There is a plausible heuristic argument to explain this. The probability that a trinomial $x^n + x^s + 1$ is irreducible is (heuristically) of order $1/n$. 
Empirical Observation

If we consider Mersenne exponents $n \equiv \pm 1 \mod 8$ and trinomials $x^n + x^s + 1$, $2s \leq n$, then the number of primitive (or irreducible) trinomials of given degree $n$ appears to have a Poisson distribution with mean about 3.07.

There is a plausible heuristic argument to explain this. The probability that a trinomial $x^n + x^s + 1$ is irreducible is (heuristically) of order $1/n$. Thus, the expected number for given $n$ and all $s \leq n/2$ is of order unity, and should have a Poisson distribution.
Remark

If $X$ is a random variable with Poisson distribution and mean $\mu$, then

$$\text{Prob}[X = 0] = e^{-\mu}.$$ 

For $\mu = 3.07$ the probability is about 0.046, or 1 in 22.
Remark

If $X$ is a random variable with Poisson distribution and mean $\mu$, then

$$\text{Prob}[X = 0] = e^{-\mu}.$$ 

For $\mu = 3.07$ the probability is about 0.046, or 1 in 22. Thus, there is about a 1 in 22 chance that an eligible Mersenne exponent will fail to give a primitive trinomial. This phenomenon has not been observed up to $M_{47}$. 

Richard Brent

The probability of zero
Remark

If $X$ is a random variable with Poisson distribution and mean $\mu$, then

$$\text{Prob}[X = 0] = e^{-\mu}.$$  

For $\mu = 3.07$ the probability is about 0.046, or 1 in 22. Thus, there is about a 1 in 22 chance that an eligible Mersenne exponent will fail to give a primitive trinomial. This phenomenon has not been observed up to $M_{47}$.

If we relax the restriction on the degree and consider prime degrees $n \equiv \pm 1 \mod 8$, then the phenomenon does occur, even if we replace “primitive” by “irreducible”.

Richard Brent
Remark

If $X$ is a random variable with Poisson distribution and mean $\mu$, then

$$\text{Prob}[X = 0] = e^{-\mu}.$$  

For $\mu = 3.07$ the probability is about 0.046, or 1 in 22. Thus, there is about a 1 in 22 chance that an eligible Mersenne exponent will fail to give a primitive trinomial. This phenomenon has not been observed up to $M_{47}$.

If we relax the restriction on the degree and consider prime degrees $n \equiv \pm 1 \mod 8$, then the phenomenon does occur, even if we replace “primitive” by “irreducible”. All trinomials of the prime degrees $n = 311, 863$ and 929 are reducible.
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$  

The exponent 57885161 is “eligible” since it is $+1$ mod 8.
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$ 

The exponent 57885161 is “eligible” since it is $+1 \mod 8$. In February Paul Zimmermann and I started a search for primitive trinomials of degree 57885161. The search was completed in two months, with computational assistance provided by Bill Hart (Warwick) and Alex Kruppa (TUM).
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$ 

The exponent 57885161 is “eligible” since it is $\pm 1 \mod 8$. In February Paul Zimmermann and I started a search for primitive trinomials of degree 57885161. The search was completed in two months, with computational assistance provided by Bill Hart (Warwick) and Alex Kruppa (TUM). The number of new primitive trinomials found was exactly ZERO. In retrospect this was not too surprising, since there was about a 1 in 22 chance of it happening. Paul was unhappy that we had a “negative” result that was not publishable; I was happy that we had found an “unusual” case.
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$ 

The exponent 57885161 is “eligible” since it is $+1 \mod 8$.

In February Paul Zimmermann and I started a search for primitive trinomials of degree 57885161. The search was completed in two months, with computational assistance provided by Bill Hart (Warwick) and Alex Kruppa (TUM). The number of new primitive trinomials found was exactly

ZERO
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$ 

The exponent 57885161 is “eligible” since it is $+1 \mod 8$.

In February Paul Zimmermann and I started a search for primitive trinomials of degree 57885161. The search was completed in two months, with computational assistance provided by Bill Hart (Warwick) and Alex Kruppa (TUM).

The number of new primitive trinomials found was exactly **ZERO**

In retrospect this was not too surprising, since there was about a 1 in 22 chance of it happening.
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$ 

The exponent 57885161 is “eligible” since it is $\equiv 1 \mod 8$. In February Paul Zimmermann and I started a search for primitive trinomials of degree 57885161. The search was completed in two months, with computational assistance provided by Bill Hart (Warwick) and Alex Kruppa (TUM). The number of new primitive trinomials found was exactly

ZERO

In retrospect this was not too surprising, since there was about a 1 in 22 chance of it happening. Paul was unhappy that we had a “negative” result that was not publishable;
Results for $M_{48}$

In January 2013 the GIMPS project announced a new Mersenne prime

$$M_{48} = 2^{57885161} - 1.$$  

The exponent 57885161 is “eligible” since it is +1 mod 8.

In February Paul Zimmermann and I started a search for primitive trinomials of degree 57885161. The search was completed in two months, with computational assistance provided by Bill Hart (Warwick) and Alex Kruppa (TUM).

The number of new primitive trinomials found was exactly

ZERO

In retrospect this was not too surprising, since there was about a 1 in 22 chance of it happening. Paul was unhappy that we had a “negative” result that was not publishable; I was happy that we had found an “unusual” case.
Can you believe our result?

For each trinomial \( x^n + x^s + 1 \), where \( n = 57885161 \) and \( 0 < s < n/2 \), we have found a “certificate of reducibility”, specifically a nontrivial factor.
Can you believe our result?

For each trinomial $x^n + x^s + 1$, where $n = 57885161$ and $0 < s < n/2$, we have found a “certificate of reducibility”, specifically a nontrivial factor.

The certificates can be checked using a simple NTL program that is independent of the programs/algorithms that we used to find the certificates.
Can you believe our result?

For each trinomial $x^n + x^s + 1$, where $n = 57885161$ and $0 < s < n/2$, we have found a “certificate of reducibility”, specifically a nontrivial factor.

The certificates can be checked using a simple NTL program that is independent of the programs/algorithms that we used to find the certificates.

A complete check takes less than one hour on a 2GHz machine.
Can you believe our result?

For each trinomial $x^n + x^s + 1$, where $n = 57885161$ and $0 < s < n/2$, we have found a “certificate of reducibility”, specifically a nontrivial factor.

The certificates can be checked using a simple NTL program that is independent of the programs/algorithms that we used to find the certificates.

A complete check takes less than one hour on a 2GHz machine.

Finding the certificates took two months on several hundred cores at INRIA (Zimmermann, Kruppa), ANU (Brent) and Warwick (Hart).
Can you believe our result?

For each trinomial $x^n + x^s + 1$, where $n = 57885161$ and $0 < s < n/2$, we have found a “certificate of reducibility”, specifically a nontrivial factor.

The certificates can be checked using a simple NTL program that is independent of the programs/algorithms that we used to find the certificates.

A complete check takes less than one hour on a 2GHz machine.

Finding the certificates took two months on several hundred cores at INRIA (Zimmermann, Kruppa), ANU (Brent) and Warwick (Hart).

Our code is written in C and is based on gf2x [Brent, Gaudry, Thomé and Zimmermann], which is now available in Sage.
The ten largest smallest factors

<table>
<thead>
<tr>
<th>s</th>
<th>degree</th>
<th>truncated factor in hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>6341306</td>
<td>7777044</td>
<td>1d8dc2db418379bdc6cf995156d7...</td>
</tr>
<tr>
<td>28796931</td>
<td>7632548</td>
<td>1ac74b27640966154c267c38d08e...</td>
</tr>
<tr>
<td>14623521</td>
<td>6938910</td>
<td>637da59bf74b7559e50df8ca963e...</td>
</tr>
<tr>
<td>13729530</td>
<td>6667114</td>
<td>6e09d9e21dab910ef41f091a8253...</td>
</tr>
<tr>
<td>23184608</td>
<td>5599493</td>
<td>3347a3e1ec88f85cacac600e72fd...</td>
</tr>
<tr>
<td>24971268</td>
<td>5497488</td>
<td>121ec44f0c13e356940004c32661...</td>
</tr>
<tr>
<td>25014894</td>
<td>4909663</td>
<td>905370b6ed155d752ceca262d395...</td>
</tr>
<tr>
<td>22379289</td>
<td>4775998</td>
<td>5b31b2b306eac9a9a8f8756b7d3e...</td>
</tr>
<tr>
<td>28919925</td>
<td>4758397</td>
<td>26158781a4a27b1984b8a1822a84...</td>
</tr>
<tr>
<td>4941804</td>
<td>4643119</td>
<td>ae341af330a9a1f242798080e7da...</td>
</tr>
</tbody>
</table>
Some positive results

We completely factored several trinomials. For example:

$$T(x) = x^{57885161} + x^{6341306} + 1.$$ 

The smallest factor has degree 7777044.
Some positive results

We completely factored several trinomials. For example:

$$T(x) = x^{57885161} + x^{6341306} + 1.$$ 

The smallest factor has degree 7777044.

By finding two other (irreducible) factors, of degrees 13311143 and 36796974, we completely factored $T(x)$. 
Some positive results

We completely factored several trinomials. For example:

\[ T(x) = x^{57885161} + x^{6341306} + 1. \]

The smallest factor has degree 7777044.

By finding two other (irreducible) factors, of degrees 13311143 and 36796974, we completely factored \( T(x) \).

Although \( T(x) \) is “sparse”, its factors are dense and take 8MB to store, even when compressed with gzip.
Some positive results

We completely factored several trinomials. For example:

\[ T(x) = x^{57885161} + x^{6341306} + 1. \]

The smallest factor has degree 7777044. By finding two other (irreducible) factors, of degrees 13311143 and 36796974, we completely factored \( T(x) \).

Although \( T(x) \) is “sparse”, its factors are dense and take 8MB to store, even when compressed with gzip.

This is a world record for a nontrivial (nonalgebraic) complete factorization of a polynomial over GF(2).
References


