Division of Trinomials by Pentanomials and Orthogonal Arrays

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Joint work with
M. Dewar, L. Moura, B. Stevens and Q. Wang

Workshop on Covering Arrays, May 2006

Definitions: Finite Fields Ingredients

We consider polynomials over the binary field, $\mathbb{F}_2$.

- A polynomial f of degree m is called primitive if $k = 2^m - 1$ is the smallest positive integer such that f divides $x^k + 1$.

Definitions: Finite Fields Ingredients

We consider polynomials over the binary field, $\mathbb{F}_2$.

- A polynomial f of degree m is called primitive if $k = 2^m - 1$ is the smallest positive integer such that f divides $x^k + 1$.
- A shift-register sequence with characteristic polynomial $f(x) = x^m + \sum_{i=0}^{m-1} c_i x^i$ is the sequence $a = (a_0, a_1, \ldots)$ defined by the recurrence relation

$$a_{n+m} = \sum_{i=0}^{m-1} c_i a_{i+n}, \qquad \text{for } n \geq 0.$$

If f is primitive, the sequence has period $2^m - 1$.

Definitions: Finite Fields Ingredients

We consider polynomials over the binary field, $\mathbb{F}_2$.

- A polynomial f of degree m is called primitive if $k = 2^m - 1$ is the smallest positive integer such that f divides $x^k + 1$.
- A shift-register sequence with characteristic polynomial $f(x) = x^m + \sum_{i=0}^{m-1} c_i x^i$ is the sequence $a = (a_0, a_1, \ldots)$ defined by the recurrence relation

$$a_{n+m} = \sum_{i=0}^{m-1} c_i a_{i+n}, \qquad \text{for } n \geq 0.$$

If f is primitive, the sequence has period $2^m - 1$.

For more information on primitive polynomials and shift-register sequences see Golomb or Lidl and Niederreiter books.

Definitions: Ortogonal Arrays

- A subset C of $\mathbb{F}_2^n$ is called an orthogonal array of strength t if for any t-subset $T = \{i_1, i_2, \ldots, i_t\}$ of $\{1, 2, \ldots, n\}$ and any t-tuple $(b_1, b_2, \ldots, b_t) \in \mathbb{F}_2^t$, there exists exactly $|C|/2^t$ elements $c = (c_1, c_2, \ldots, c_n)$ of C such that $c_{i_j} = b_j$ for all $1 \leq j \leq t$.

Definitions: Ortogonal Arrays

- A subset C of $\mathbb{F}_2^n$ is called an orthogonal array of strength t if for any t-subset $T = \{i_1, i_2, \ldots, i_t\}$ of $\{1, 2, \ldots, n\}$ and any t-tuple $(b_1, b_2, \ldots, b_t) \in \mathbb{F}_2^t$, there exists exactly $|C|/2^t$ elements $c = (c_1, c_2, \ldots, c_n)$ of C such that $c_{i_j} = b_j$ for all $1 \leq j \leq t$.

From the definition, if C is an orthogonal array of strength t, then it is also an orthogonal array of strength s for all $1 \leq s \leq t$.

Previous Results

The next theorem relates orthogonal arrays with codes.

Theorem 1: Delsarte 1973

Let C be a linear code over $\mathbb{F}_q$. Then, C is an orthogonal array of maximal strength t if and only if $C^{\perp}$, its dual code, has minimum weight $t+1$.

Let C_n^f be the set of all subintervals of the shift-register sequence with length n generated by f, together with the zero vector.

Since $(C_{2^m-1}^f)^{\perp}$ is the Hamming code, then by Theorem 1, C_n^f is an orthogonal array of strength 2, for all $2 \leq n \leq 2^m - 1$.

Previous Results (cont.)

The dual code of the code generated by shift register sequences can be described in terms of multiples of its characteristic polynomial.

Theorem 2: Munemasa 1998

Let f be a primitive polynomial of degree m over $\mathbb{F}_2$ and let $2 \leq n \leq 2^m - 1$. Let C_n^f be the set of all subintervals of the shift-register sequence with length n generated by f, together with the zero vector of length n. The dual code of C_n^f is given by

$$(C_n^f)^\perp = \{(b_1, \ldots, b_n) : \sum_{i=0}^{n-1} b_{i+1} x^i \text{ is divisible by } f\}.$$

Previous Results (cont.)

Munemasa considers the case when the polynomial f generating the sequence is a trinomial.

Theorem 3: Munemasa 1998

Let $f(x) = x^m + x^l + 1$ be a trinomial over $\mathbb{F}_2$ such that $\gcd(m, l) = 1$. If g is a trinomial of degree at most 2m that is divisible by f, then $g(x) = x^{\deg g - m} f(x)$, $g(x) = f(x)^2$, or $g(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ or, its reciprocal, $g(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

Using Theorems 1, 2 and 3, Munemasa concludes that C_n^f corresponds to an orthogonal array of strength 2 that has a property very close to being an orthogonal array of strength 3.

Pentanomials over $\mathbb{F}_2$

- We consider shift-register sequence with length n generated by a pentanomial f over $\mathbb{F}_2$ (that is, a polynomial with 5 nonzero terms) of degree m.

Pentanomials over $\mathbb{F}_2$

- We consider shift-register sequence with length n generated by a pentanomial f over $\mathbb{F}_2$ (that is, a polynomial with 5 nonzero terms) of degree m.

- We show that no trinomial of degree at most $2m$ is divisible by the given pentanomial f, provided that f is not in a finite list of exceptions that we give.

Pentanomials over $\mathbb{F}_2$

- We consider shift-register sequence with length n generated by a pentanomial f over $\mathbb{F}_2$ (that is, a polynomial with 5 nonzero terms) of degree m.
- We show that no trinomial of degree at most $2m$ is divisible by the given pentanomial f, provided that f is not in a finite list of exceptions that we give.
- Using Theorem 1 (Delsarte) and Theorem 2 (Munemasa) we get that C_n^f, the set of all subintervals of the sequence of length n, corresponds to an orthogonal array of strength 3.

Why Pentanomials?

- Primitive trinomials over $\mathbb{F}_2$ do not exist for every degree (for example, see von zur Gathen 2003 and Seroussi 1998).

Why Pentanomials?

- Primitive trinomials over $\mathbb{F}_2$ do not exist for every degree (for example, see von zur Gathen 2003 and Seroussi 1998).

- There exists some empirical evidence that irreducible pentanomials over $\mathbb{F}_2$ do exist for every degree (von zur Gathen 2003 and Seroussi 1998).

Why Pentanomials?

- Primitive trinomials over $\mathbb{F}_2$ do not exist for every degree (for example, see von zur Gathen 2003 and Seroussi 1998).
- There exists some empirical evidence that irreducible pentanomials over $\mathbb{F}_2$ do exist for every degree (von zur Gathen 2003 and Seroussi 1998).
- Pentanomials have the next smallest number of terms, after trinomials, that is possible in a primitive polynomial over $\mathbb{F}_2$. This allows fast generation of a shift-register sequence when primitive trinomials are not available.

Why Pentanomials?

- Primitive trinomials over $\mathbb{F}_2$ do not exist for every degree (for example, see von zur Gathen 2003 and Seroussi 1998).

- There exists some empirical evidence that irreducible pentanomials over $\mathbb{F}_2$ do exist for every degree (von zur Gathen 2003 and Seroussi 1998).

- Pentanomials have the next smallest number of terms, after trinomials, that is possible in a primitive polynomial over $\mathbb{F}_2$. This allows fast generation of a shift-register sequence when primitive trinomials are not available.

- The usage of pentanomials when trinomials do not exist is in the IEEE standard specifications for public-key cryptography (IEEE 2000).

Main Theorem

Main Theorem

Let $f(x) = x^m + x^l + x^k + x^j + 1$ be a pentanomial over $\mathbb{F}_2$ such that $\gcd(m, l, k, j) = 1$. If g is a trinomial of degree at most $2m$ divisible by f, with $g = fh$, then

1. f is one of the polynomial exceptions given in Table 1; or
2. $m \equiv 1 \bmod 3$ and f, g, h are as follows

$$\begin{aligned} f(x) &= 1 + x + x^2 + x^{m-3} + x^m \\ &= (1 + x + x^2)(1 + x^{m-3} + x^{m-2}), \\ h(x) &= (1 + x) + (x^3 + x^4) + \cdots + \\ &\quad (x^{m-7} + x^{m-6}) + x^{m-4}, \\ g(x) &= 1 + x^{2m-6} + x^{2m-4}; \ \textit{or} \end{aligned}$$

3. f is the reciprocal of one of the polynomials above.

No.	$f(x)$	$h(x)$	type
1	$x^5+x^4+x^3+x^2+1$	x^3+x^2+1	p
2	$x^5+x^3+x^2+x+1$	x^3+x+1	p
3	$x^5+x^3+x^2+x+1$	x^4+x+1	p
4	$x^5+x^4+x^3+x+1$	x^2+x+1	p
5	$x^6+x^5+x^4+x^3+1$	x^4+x^3+1	r
6	$x^6+x^4+x^2+x+1$	x^3+x+1	i
7	$x^6+x^4+x^3+x+1$	x^2+x+1	p
8	$x^6+x^5+x^2+x+1$	$x^5+x^4+x^3+x+1$	p
9	$x^6+x^5+x^3+x+1$	x^2+x+1	r
10	$x^7+x^4+x^2+x+1$	x^3+x+1	r
11	$x^7+x^4+x^3+x^2+1$	x^3+x^2+1	p
12	$x^7+x^5+x^2+x+1$	$x^7+x^6+x^5+x^4+x^3+x+1$	p
13	$x^7+x^5+x^3+x^2+1$	$x^5+x^4+x^3+x^2+1$	r
14	$x^8+x^5+x^3+x+1$	$x^5+x^4+x^2+x+1$	p
15	$x^8+x^5+x^3+x^2+1$	$x^8+x^7+x^5+x^4+x^3+x^2+1$	p
16	$x^8+x^6+x^3+x+1$	$x^6+x^4+x^2+x+1$	r
17	$x^8+x^7+x^5+x^2+1$	$x^6+x^5+x^4+x^2+1$	r
18	$x^9+x^6+x^5+x^2+1$	$x^8+x^5+x^4+x^2+1$	i
19	$x^9+x^7+x^4+x^3+1$	$x^8+x^6+x^4+x^3+1$	i
20	$x^9+x^8+x^5+x^2+1$	$x^6+x^5+x^4+x^2+1$	r
21	$x^{10}+x^4+x^3+x^2+1$	$x^8+x^7+x^4+x^2+1$	i
22	$x^{10}+x^7+x^2+x+1$	$x^6+x^4+x^3+x+1$	r
23	$x^{11}+x^7+x^6+x^2+1$	$x^8+x^7+x^4+x^2+1$	r
24	$x^{13}+x^{10}+x^2+x+1$	$x^9+x^7+x^6+x^4+x^3+x+1$	r
25	$x^{13}+x^{10}+x^9+x^2+1$	$x^{12}+x^9+x^8+x^6+x^4+x^2+1$	p

Corollaries

The infinite family of pentanomial exceptions are all factorable and the largest degree of the irreducible polynomial exceptions is 13.

Corollary 5

If $f(x) = x^m + x^l + x^k + x^j + 1$ is irreducible over $\mathbb{F}_2$ with $\gcd(m, l, k, j) = 1$ and $m \geq 14$, then f does not divide any trinomials of degree less than or equal to $2m$.

In particular, this is true for f primitive, since primitive polynomials are irreducible. In addition, it can be shown that for any primitive pentanomial f, the above GCD condition is satisfied.

Using Theorems 1 (Delsarte) and Theorem 2 (Munemasa) we get our results about the strength of orthogonal arrays given by shift-register sequences generated by primitive pentanomials.

Corollary 6

If $f(x) = x^m + x^l + x^k + x^j + 1$ is primitive over $\mathbb{F}_2$ and not one of the exceptions in Table 1 or their reciprocals, then, for $m < n \leq 2m$,

1. C_n^f is an orthogonal array of strength at least 3; or equivalently,
2. $(C_n^f)^\perp$, the dual code of C_n^f, has minimum weight at least 4.

Since C_n^f has strength 3, the third moment of the Hamming weight of the shift-register sequence is minimized, as desired for less statistical bias (Jordan and Wood 1973, Lindholm 1968).

Sketch of Proof

The complete proof involves a great number of subcases.
The complete case analysis can be found on the technical report (Dewar, Moura, Panario, Stevens and Wang 2006).
The polynomial exceptions were also checked by computer.

We separately consider the top-left portion and the bottom-right portion of the box diagram (next slide).

Key observation: the top and bottom portions are independent and the proof combines each possible top subcases with each possible bottom case.

Sketch of Munemasa's Proof

Let $f(x) = x^m + x^l + 1$ be a trinomial. If $g = hf$ is also trinomial for some h, then h must have an odd number of non-zero terms. We write

$$h(x) = \sum_{s=0}^{t} x^{i_s},$$

where t is even, i_t is the degree of h and i_0=0.

Theorem 3: Munemasa 1998

Let $f(x) = x^m + x^l + 1$ be a trinomial over $\mathbb{F}_2$ such that $\gcd(m, l) = 1$. If g is a trinomial of degree at most 2m that is divisible by f, then $g(x) = x^{\deg g - m} f(x)$, $g(x) = f(x)^2$, or $g(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ or, its reciprocal, $g(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

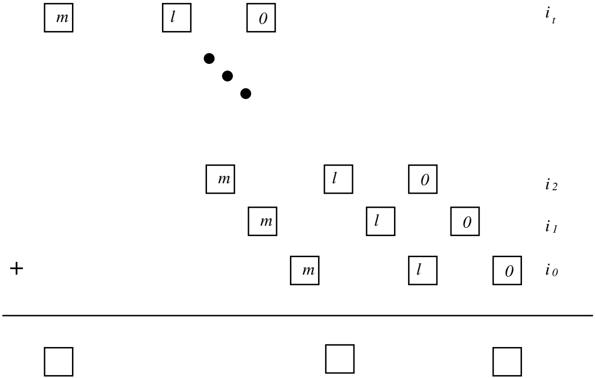

Figure: An illustration of equation $g(x) = \sum_{s=0}^{t} x^{i_s} f(x)$, with f, g trinomials.

We have $g = fh$ if and only if rec$(g) =$ rec(f)rec(h). Thus, by taking reciprocals, we can reduce the problem in either of two ways:

· the first is to assume that $m \geq 2l$ (Munemasa);

· the second, which we use, is to assume that the middle term of $g(x)$ is either an "m" (that is, it equals $m + i_s$ for some s) or it is an "l" from the top $t/2$ rows.

The top 0 must cancel and it must cancel down.

If the top 0 cancels down with an m:

- Since $i_t \leq m$, we get $0 + i_t = m + i_0$.

If the top 0 cancels down with an m:

- Since $i_t \leq m$, we get $0 + i_t = m + i_0$.
- Since all 0's must cancel (with the exception of the 0 in row i_0), they cancel with l's.

If the top 0 cancels down with an m:

- Since $i_t \leq m$, we get $0 + i_t = m + i_0$.
- Since all 0's must cancel (with the exception of the 0 in row i_0), they cancel with l's.
- At most one of the remaining $t - 1$ m's can be left-over and two m's cannot cancel themselves, so we have that $t \leq 3$ and its parity forces $t = 2$.

If the top 0 cancels down with an m:

- Since $i_t \leq m$, we get $0 + i_t = m + i_0$.
- Since all 0's must cancel (with the exception of the 0 in row i_0), they cancel with l's.
- At most one of the remaining $t - 1$ m's can be left-over and two m's cannot cancel themselves, so we have that $t \leq 3$ and its parity forces $t = 2$.
- It is easy to check that in this case $h = f$ and $g = f^2$.

If the top 0 cancels down with an l:

- Then, $0 + i_t = l + i_z$ for some $z < t$.

$\square$

If the top 0 cancels down with an l:

- Then, $0 + i_t = l + i_z$ for some $z < t$.
- By contradiction all 0's must cancel down with l's.

$\square$

If the top 0 cancels down with an l:

- Then, $0 + i_t = l + i_z$ for some $z < t$.
- By contradiction all 0's must cancel down with l's.
- There are exactly $t - 1$ 0's that cancel, which uses all but one l, namely $l + i_t$.

$\square$

If the top 0 cancels down with an l:

- Then, $0 + i_t = l + i_z$ for some $z < t$.
- By contradiction all 0's must cancel down with l's.
- There are exactly $t - 1$ 0's that cancel, which uses all but one l, namely $l + i_t$.
- Again, at most one m cancels up with an l and at most one m can be left-over. This gives us $t = 2$.

□

If the top 0 cancels down with an l:

- Then, $0 + i_t = l + i_z$ for some $z < t$.
- By contradiction all 0's must cancel down with l's.
- There are exactly $t - 1$ 0's that cancel, which uses all but one l, namely $l + i_t$.
- Again, at most one m cancels up with an l and at most one m can be left-over. This gives us $t = 2$.
  - If $l + i_2 = m + i_1$, then $m - l = l$. The GCD condition gives $l = 1$, $m = 2$ and $h = f$ and $g = f^2$.

□

If the top 0 cancels down with an l:

- Then, $0 + i_t = l + i_z$ for some $z < t$.
- By contradiction all 0's must cancel down with l's.
- There are exactly $t - 1$ 0's that cancel, which uses all but one l, namely $l + i_t$.
- Again, at most one m cancels up with an l and at most one m can be left-over. This gives us $t = 2$.
  - If $l + i_2 = m + i_1$, then $m - l = l$. The GCD condition gives $l = 1$, $m = 2$ and $h = f$ and $g = f^2$.
  - If $l + i_2 = m + i_0$, then $l + i_2 = 3l$. The GCD condition forces $l = 1$, $m = 3$ and we get $f(x) = 1 + x + x^3$, $h(x) = 1 + x + x^2$ and $g(x) = x^5 + x^4 + 1$, which is the only exception. Given our symmetry assumption, we get the reciprocal exception.

□

Further Work

Our results guarantee that the orthogonal arrays constructed, C_n^f, have strength at least 3. What can be said about strength 4? This requires the analysis of pentanomials dividing tetranomials.

Another question is concerned with generalizations of our main theorem for polynomials with more than five terms as well as for finite fields other than $\mathbb{F}_2$.

Under which conditions, given t, does there exist a positive integer d such that if a polynomial f of degree m has precisely t non-zero coefficients and $m \geq d$, then f does not divide any polynomials with exactly s non-zero coefficients and degree less than or equal to some function of m, for all $s \leq t$?

P. Delsarte.
Four fundamental parameters of a code and their combinatorial significance. *Inform. Control*, 23:407–438, 1973.

M. Dewar, L. Moura, D. Panario, B. Stevens and Q. Wang.
Division of trinomials by pentanomials and orthogonal arrays. Technical report SITE, University of Ottawa, 2006, 72 pages.

J. von zur Gathen.
Irreducible trinomials over finite fields. *Math. Comp.*, 72:1987–2000, 2003.

S. W. Golomb.
Shift Register Sequences. Aegean Park Press, 1982.

IEEE
Standard Specifications for Public-Key Cryptography. Technical Report IEEE Std 1361-2000. IEEE Inc., 3 Park Ave., NY 10016-5997, USA.

H. F. Jordan and D. C. M. Wood.
On the distribution of sums of successive bits of shift-register sequences. *IEEE Trans. Computers*, 22:400–408, 1973.

R. Lidl and H. Niederreiter.
Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge, first edition, 1994.

J. H. Lindholm.
An analysis of the pseudo-randomness properties of subsequences of long m-sequences. *IEEE Trans. Inform. Theory*, 14:569–576,1968.

A. Munemasa.
Orthogonal arrays, primitive trinomials, and shift-register sequences. *Finite Fields and Their Applications*, 4(3):252–260, 1998.

G. Seroussi.
Table of low-weight binary irreducible polynomials. HP Labs Technical Report HPL-98–135, 1998.