An Interesting Family of Polynomials in $\mathbb{Z}_2[x]$

Katie Anders

University of Illinois at Urbana-Champaign

October 21, 2012

Introduction

Recall that every number has a unique binary representation and can be written as $\sum_{j=0}^{\infty} c_j 2^j$, where $c_j \in \{0, 1\}$.

Introduction

Recall that every number has a unique binary representation and can be written as $\sum_{j=0}^{\infty} c_j 2^j$, where $c_j \in \{0, 1\}$.

Question: What happens if we take the coefficients from a different set?

The Stern Sequence

Example: If we take coefficients from the set $\{0, 1, 2\}$, then the binary representation is no longer unique. For example, there are three ways to write $n = 4$:

$$4 = 2 \cdot 1 + 1 \cdot 2 = 0 \cdot 1 + 0 \cdot 2 + 1 \cdot 2^2 = 0 \cdot 1 + 2 \cdot 2.$$

The Stern Sequence

Example: If we take coefficients from the set $\{0, 1, 2\}$, then the binary representation is no longer unique. For example, there are three ways to write $n = 4$:

$$4 = 2 \cdot 1 + 1 \cdot 2 = 0 \cdot 1 + 0 \cdot 2 + 1 \cdot 2^2 = 0 \cdot 1 + 2 \cdot 2.$$

Taking coefficients from this set, the number of representations of $n - 1$ corresponds to the nth term in the Stern sequence, which is defined by $s(2n) = s(n)$ and $s(2n + 1) = s(n) + s(n + 1)$, with $s(0) = 0$ and $s(1) = 1$.

Generalizing the Ideas

Let $\mathcal{A} = \{0 = a_0 < a_1 < \cdots < a_j\}$ denote a finite subset of $\mathbb{N}$ containing 0. Let $f_{\mathcal{A}}(n)$ denote the number of ways to write n in the form

$$n = \sum_{k=0}^{\infty} \epsilon_k 2^k, \quad \epsilon_k \in \mathcal{A}.$$

Generalizing the Ideas

Let $\mathcal{A} = \{0 = a_0 < a_1 < \cdots < a_j\}$ denote a finite subset of $\mathbb{N}$ containing 0. Let $f_{\mathcal{A}}(n)$ denote the number of ways to write n in the form

$$n = \sum_{k=0}^{\infty} \epsilon_k 2^k, \quad \epsilon_k \in \mathcal{A}.$$

We associate to $\mathcal{A}$ its characteristic function $\chi_{\mathcal{A}}(n)$ and the generating function

$$\phi_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} \chi_{\mathcal{A}}(n) x^n = \sum_{a \in \mathcal{A}} x^a = 1 + x^{a_1} + \cdots + x^{a_j}.$$

Product Representation

Denote the generating function of $f_{\mathcal{A}}(n)$ by

$$F_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} f_{\mathcal{A}}(n)x^n.$$

Product Representation

Denote the generating function of $f_{\mathcal{A}}(n)$ by

$$F_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} f_{\mathcal{A}}(n)x^n.$$

Viewing the number of ways to write n as a partition problem, we obtain the following product representation for $F_{\mathcal{A}}(x)$.

$$F_{\mathcal{A}}(x) = \prod_{k=0}^{\infty} \left(1 + x^{a_1 2^k} + \cdots + x^{a_j 2^k}\right) = \prod_{k=0}^{\infty} \phi_{\mathcal{A}}(x^{2^k})$$

In *Congruence Properties of Binary Partition Functions*, Anders, Dennison, Lansing, and Reznick studied the behavior of $f_{\mathcal{A}}(n)$ mod 2. Theorem 1.1 states that

$$\phi_{\mathcal{A}}(x)F_{\mathcal{A}}(x) = 1 \quad \text{in } \mathbb{F}_2[x].$$

In *Congruence Properties of Binary Partition Functions*, Anders, Dennison, Lansing, and Reznick studied the behavior of $f_{\mathcal{A}}(n)$ mod 2. Theorem 1.1 states that

$$\phi_{\mathcal{A}}(x)F_{\mathcal{A}}(x) = 1 \quad \text{in } \mathbb{F}_2[x].$$

We can make similar definitions for an infinite set $\mathcal{A}$ containing 0, and the above result still applies. This relates our work to that of a paper by Cooper, Eichhorn, and O'Bryant.

Return to the Stern Sequence

n	$f_{\{0,1,2\}}(n)$	$s(n)$	n	$f_{\{0,1,2\}}(n)$	$s(n)$
0	1	0	9	3	4
1	1	1	10	5	3
2	2	1	11	2	5
3	1	2	12	5	2
4	3	1	13	3	5
5	2	3	14	4	3
6	3	2	15	1	4
7	1	3	16	5	1
8	4	1			

Stern noticed in 1858 that the parity of $s(n)$ is periodic with period 3, and Reznick proved in 1989 that $s(n) = f_{\{0,1,2\}}(n-1)$.

Example

Note that $\phi_{\{0,1,2\},}(x) = 1 + x + x^2$, and applying the theorem, we see that in $\mathbb{F}_2[x]$

$$\begin{aligned} F_{\{0,1,2\}}(x) &= \frac{1}{1 + x + x^2} \\ &= (1 + x)/(1 + x^3) \\ &= (1 + x)(1 + x^3 + x^6 + \cdots) \\ &= 1 + x + x^3 + x^4 + x^6 + x^7 + \cdots \end{aligned}$$

Another Example

Dennison observed in her thesis that if $\mathcal{A} = \{0, 1, 3\}$, $f_{\mathcal{A}}(n)$ is periodic with period 7 and each period has four odd terms. Specifically, $f_{\mathcal{A}}(n)$ is odd when $n \equiv 0, 1, 2, 4 \pmod 7$.

Another Example

Dennison observed in her thesis that if $\mathcal{A} = \{0, 1, 3\}$, $f_{\mathcal{A}}(n)$ is periodic with period 7 and each period has four odd terms. Specifically, $f_{\mathcal{A}}(n)$ is odd when $n \equiv 0, 1, 2, 4 \pmod 7$.

Using our main theorem, we see

$$F_{\{0,1,3\}}(x) = \frac{1}{1 + x + x^3} = \frac{1 + x + x^2 + x^4}{1 + x^7}.$$

Similarly, Dennison noted that if $\mathcal{A} = \{0, 2, 3\}$, $f_{\mathcal{A}}(n)$ is periodic with period 7 and each period has four odd terms, which occur when $n \equiv 0, 2, 3, 4 \pmod 7$.

Similarly, Dennison noted that if $\mathcal{A} = \{0, 2, 3\}$, $f_{\mathcal{A}}(n)$ is periodic with period 7 and each period has four odd terms, which occur when $n \equiv 0, 2, 3, 4 \pmod 7$.

Again, we can use our main theorem to see that

$$F_{\{0,2,3\}}(x) = \frac{1}{1 + x^2 + x^3} = \frac{1 + x^2 + x^3 + x^4}{1 + x^7}.$$

Definitions and Observations

- Since $\mathcal{A}$ is finite, $\phi_{\mathcal{A}}(x)$ is a polynomial in $\mathbb{F}_2[x]$.

Definitions and Observations

- Since $\mathcal{A}$ is finite, $\phi_{\mathcal{A}}(x)$ is a polynomial in $\mathbb{F}_2[x]$.
- For any polynomial $p(x) \in \mathbb{F}_2[x]$, let

$$\ell(p) = \text{length}(p) = \text{ number of terms in } p.$$

Definitions and Observations

- Since $\mathcal{A}$ is finite, $\phi_{\mathcal{A}}(x)$ is a polynomial in $\mathbb{F}_2[x]$.
- For any polynomial $p(x) \in \mathbb{F}_2[x]$, let

$$\ell(p) = \text{length}(p) = \text{ number of terms in } p.$$

- Let $D = D(\phi_{\mathcal{A}})$ denote the *order* of $\phi_{\mathcal{A}}$, the smallest integer D such that $\phi_{\mathcal{A}}(x) \mid 1 + x^D$. Such a D is known to exist, and if $\phi_{\mathcal{A}}$ is irreducible, $D \mid 2^{\deg(\phi_{\mathcal{A}})} - 1$.

Definitions and Observations

- Since $\mathcal{A}$ is finite, $\phi_{\mathcal{A}}(x)$ is a polynomial in $\mathbb{F}_2[x]$.
- For any polynomial $p(x) \in \mathbb{F}_2[x]$, let

$$\ell(p) = \text{length}(p) = \text{ number of terms in } p.$$

- Let $D = D(\phi_{\mathcal{A}})$ denote the *order* of $\phi_{\mathcal{A}}$, the smallest integer D such that $\phi_{\mathcal{A}}(x) \mid 1 + x^D$. Such a D is known to exist, and if $\phi_{\mathcal{A}}$ is irreducible, $D \mid 2^{\deg(\phi_{\mathcal{A}})} - 1$.
- Define $\phi^*_{\mathcal{A}}(x)$ by $\phi_{\mathcal{A}}(x)\phi^*_{\mathcal{A}}(x) = 1 + x^D$.

An Example from Our Paper

Let $\mathcal{A} = \{0, 1, 4, 9\}$. In $\mathbb{F}_2[x]$,

$$\phi_{\mathcal{A}} = 1 + x + x^4 + x^9 = (1 + x)^4(1 + x + x^2)(1 + x^2 + x^3).$$

An Example from Our Paper

Let $\mathcal{A} = \{0, 1, 4, 9\}$. In $\mathbb{F}_2[x]$,

$$\phi_{\mathcal{A}} = 1 + x + x^4 + x^9 = (1 + x)^4(1 + x + x^2)(1 + x^2 + x^3).$$

Quick computations show that the period of $\phi_{\mathcal{A}}$ is 84. Recall that this means $\phi_{\mathcal{A}}\phi_{\mathcal{A}}^* = 1 + x^{84}$. Further computations show that $\phi_{\mathcal{A}}^*$ has 41 terms with exponents in the set $\{0, 1, 2, 3, \ldots, 70, 75\}$.

We have

$$F_{\mathcal{A}}(x) = \frac{1}{\phi_{\mathcal{A}}(x)} = \frac{\phi^*_{\mathcal{A}}(x)}{1 + x^D} \quad \text{in } \mathbb{F}_2[x]. \tag{1}$$

We have

$$F_{\mathcal{A}}(x) = \frac{1}{\phi_{\mathcal{A}}(x)} = \frac{\phi^*_{\mathcal{A}}(x)}{1 + x^D} \quad \text{in } \mathbb{F}_2[x]. \tag{1}$$

If $\phi^*_{\mathcal{A}}(x) = \sum_{i=1}^{r} x^{b_i}$, where $0 = b_1 < \cdots < b_r = D - \max \mathcal{A}$, then

$$f_{\mathcal{A}}(n) \equiv 1 \bmod 2 \iff n \equiv b_i \bmod D \quad \text{for some } i.$$

We have

$$F_{\mathcal{A}}(x) = \frac{1}{\phi_{\mathcal{A}}(x)} = \frac{\phi^*_{\mathcal{A}}(x)}{1+x^D} \quad \text{in } \mathbb{F}_2[x]. \tag{1}$$

If $\phi^*_{\mathcal{A}}(x) = \sum_{i=1}^{r} x^{b_i}$, where $0 = b_1 < \cdots < b_r = D - \max \mathcal{A}$, then

$$f_{\mathcal{A}}(n) \equiv 1 \bmod 2 \iff n \equiv b_i \bmod D \quad \text{for some } i.$$

In any block of D consecutive integers,

$$\#\{n : f_{\mathcal{A}}(n) \text{ is odd}\} = \ell(\phi^*_{\mathcal{A}}) = \beta_1(\phi_{\mathcal{A}})$$
$$\#\{n : f_{\mathcal{A}}(n) \text{ is even}\} = D - \ell(\phi^*_{\mathcal{A}}) = \beta_0(\phi_{\mathcal{A}}).$$

In *Reciprocals of Binary Power Series*, which appeared in *International Journal of Number Theory* in 2006, Cooper, Eichhorn, and O'Bryant considered the fraction $\ell(\phi_{\mathcal{A}}^*)/D$, as we did in our paper. Here I instead consider the ordered pair

$$\beta(\phi_{\mathcal{A}}) := (\beta_1(\phi_{\mathcal{A}}), \beta_0(\phi_{\mathcal{A}}))\,,$$

which gives more detailed information than reduced fractions.

The first coordinate represents the number of times $f_{\mathcal{A}}(n)$ is odd in a minimal period, and the second coordinate represents the number of times $f_{\mathcal{A}}(n)$ is even in a minimal period.

Definition

Cooper, Eichhorn, and O'Bryant showed by direct computation that $\beta_1(f) \leq \beta_0(f) + 1$ when $\deg(f) < 8$.

Definition

Cooper, Eichhorn, and O'Bryant showed by direct computation that $\beta_1(f) \leq \beta_0(f) + 1$ when $\deg(f) < 8$.

This is not, however, always the case. Let

$$f(x) = 1 + x + x^5 + x^9 + x^{10}.$$

Then $\text{order}(f) = 33$ and $\beta(f) = (18, 15)$, so $\beta_1(f) > \beta_0(f) + 1$.

Definition

Cooper, Eichhorn, and O'Bryant showed by direct computation that $\beta_1(f) \leq \beta_0(f) + 1$ when $\deg(f) < 8$.

This is not, however, always the case. Let

$$f(x) = 1 + x + x^5 + x^9 + x^{10}.$$

Then $\text{order}(f) = 33$ and $\beta(f) = (18, 15)$, so $\beta_1(f) > \beta_0(f) + 1$.

We call a polynomial $f(x)$ *robust* if $\beta_1(f) > \beta_0(f) + 1$. This is equivalent to saying that $\beta_1(f) > (D + 1)/2$, where D is the order of $f(x)$.

They also posed the problem of describing

$$\mathcal{K} := \left\{ \frac{\beta_1(f)}{\beta_0(f) + \beta_1(f)} : f(x) \text{ is a polynomial} \right\}.$$

They also posed the problem of describing

$$\mathcal{K} := \left\{ \frac{\beta_1(f)}{\beta_0(f) + \beta_1(f)} : f(x) \text{ is a polynomial} \right\}.$$

Since $f(x) = 1 + x^D$ has order D and $\beta_1(f) = \ell\left(f^*(x)\right) = 1$, we see $\inf \mathcal{K} = 0$. I will exhibit two sequences $\{f_n\}$ of polynomials such that

$$\lim_{n\to\infty} \frac{\beta_1\left(f_n\right)}{\beta_0(f_n) + \beta_1(f_n)} = 1,$$

thus proving that $\sup \mathcal{K} = 1$.

Reciprocal Polynomials

Definition

For a polynomial $f(x)$ of degree n, the *reciprocal polynomial* of $f(x)$ is $f_{(R)}(x) := x^n f(1/x)$.

Reciprocal Polynomials

Definition

For a polynomial $f(x)$ of degree n, the *reciprocal polynomial* of $f(x)$ is $f_{(R)}(x) := x^n f(1/x)$.

If $f(x) = 1 + x^{a_2} + \cdots + x^{a_{n-1}} + x^{a_n}$, then
$f_{(R)}(x) = 1 + x^{a_n - a_{n-1}} + \cdots + x^{a_n - a_2} + x^{a_n}$.

Reciprocal Polynomials

Definition

For a polynomial $f(x)$ of degree n, the *reciprocal polynomial* of $f(x)$ is $f_{(R)}(x) := x^n f(1/x)$.

If $f(x) = 1 + x^{a_2} + \cdots + x^{a_{n-1}} + x^{a_n}$, then
$f_{(R)}(x) = 1 + x^{a_n - a_{n-1}} + \cdots + x^{a_n - a_2} + x^{a_n}$.

If $\text{order}(f(x)) = D$, then $\text{order}\left(f_{(R)}(x)\right) = D$. Thus $\beta(f(x)) = \beta\left(f_{(R)}(x)\right)$, and the robustness of $f(x)$ is equivalent to the robustness of $f_{(R)}(x)$.

Main Theorem

Theorem

Fix $r \geq 3$.

(i) *The order of* $f_{r,1}(x) := 1 + x + x^{2^r-1} + x^{2^r+1}$ *divides* $4^r - 1$.

(ii) $\beta_1(f_{r,1}) = 4^r - 3^r$

(iii) *Hence* $\beta(f_{r,1}) = (4^r - 3^r, 3^r - 1)$ *and* $f_{r,1}(x)$ *is robust.*

Example

Consider $f_{3,1}(x) = 1 + x + x^7 + x^9$.

Example

Consider $f_{3,1}(x) = 1 + x + x^7 + x^9$.

- order $(f_{3,1}(x)) = 4^3 - 1 = 63$

Example

Consider $f_{3,1}(x) = 1 + x + x^7 + x^9$.

- order $(f_{3,1}(x)) = 4^3 - 1 = 63$
- $\beta_1 (f_{3,1}) = 4^3 - 3^3 = 37$

Example

Consider $f_{3,1}(x) = 1 + x + x^7 + x^9$.

- order $(f_{3,1}(x)) = 4^3 - 1 = 63$
- $\beta_1(f_{3,1}) = 4^3 - 3^3 = 37$
- $\beta(f_{3,1}) = (37, 26)$

Example

Consider $f_{3,1}(x) = 1 + x + x^7 + x^9$.

- order $(f_{3,1}(x)) = 4^3 - 1 = 63$
- $\beta_1(f_{3,1}) = 4^3 - 3^3 = 37$
- $\beta(f_{3,1}) = (37, 26)$

$$f^*_{3,1} = \frac{1 + x^{63}}{f_{3,1}} = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{10}$$
$$+ x^{11} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20}$$
$$+ x^{22} + x^{24} + x^{25} + x^{26} + x^{27} + x^{32} + x^{33} + x^{34}$$
$$+ x^{36} + x^{37} + x^{38} + x^{40} + x^{41} + x^{44} + x^{45} + x^{48}$$
$$+ x^{50} + x^{52} + x^{54}$$

Proof

Define

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{4^r-2^r}.$$

By a lemma,

$$\left(1 + x^{2^r-1} + x^{2^r}\right) g_{r,1}(x) = 1 + x^{4^r-1}.$$

Because

$$g_{r,1}(1) = \prod_{j=0}^{r-1} (1+1+1) + 1 = 0,$$

we know $(1+x) \mid g_{r,1}(x)$.

Because

$$g_{r,1}(1) = \prod_{j=0}^{r-1} (1+1+1) + 1 = 0,$$

we know $(1+x) \mid g_{r,1}(x)$.

Write $(1+x)h_{r,1}(x) = g_{r,1}(x)$, so

$$\left(1 + x^{2^r-1} + x^{2^r}\right)(1+x)h_{r,1}(x) = 1 + x^{4^r-1}.$$

Because

$$g_{r,1}(1) = \prod_{j=0}^{r-1} (1+1+1) + 1 = 0,$$

we know $(1+x) \mid g_{r,1}(x)$.

Write $(1+x)h_{r,1}(x) = g_{r,1}(x)$, so

$$\left(1 + x^{2^r-1} + x^{2^r}\right)(1+x)h_{r,1}(x) = 1 + x^{4^r-1}.$$

Since $f_{r,1}(x) = 1 + x + x^{2^r-1} + x^{2^r+1} = (1+x)\left(1 + x^{2^r-1} + x^{2^r}\right)$, we see that $f_{r,1}(x) \mid \left(1 + x^{4^r-1}\right)$ and

$$f_{r,1}h_{r,1} = 1 + x^{4^r-1}.$$

Rewrite

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{4^r-2^r}$$

to obtain

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j}(1 + x^{2^j})\right) + x^{4^r-2^r}.$$

Expand the product and rewrite, using $1 + x^{2^j} = (1+x)^{2^j}$, to obtain

$$\begin{aligned} g_{r,1}(x) &= 1 + x^{4^r - 2^r} + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^n \\ &= (1+x)\left(\frac{1+x^{4^r-2^r}}{1+x} + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}\right) \\ &= (1+x)\left(\sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}\right). \end{aligned}$$

Ultimately, $(\beta_1(f_{r,1}), \beta_0(f_{r,1})) = (4^r - 3^r, 3^r - 1)$.

Corollary

The reciprocal polynomials $f_{(R),r,1} = 1 + x^2 + x^{2^r} + x^{2^r+1}$ *are robust with order dividing* $4^r - 1$.

Corollary

The reciprocal polynomials $f_{(R),r,1} = 1 + x^2 + x^{2^r} + x^{2^r+1}$ *are robust with order dividing* $4^r - 1$.

Example

Consider $f_{(R),3,1}(x) = 1 + x^2 + x^8 + x^9$.

- order $f_{(R),3,1} = 4^3 - 1 = 63$
- $\beta\left(f_{(R),3,1}\right) = (37, 26)$

Theorem

Fix $r \geq 3$.

(i) *The order of $f_{r,2}(x) := 1 + x + x^{2^r} + x^{2^r+2}$ divides $4^r + 2^r + 1$.*

(ii) $\beta_1(f_{r,2}) = 4^r - 3^r + 2^r$

(iii) $\beta(f_{r,2}) = (4^r - 3^r + 2^r, 3^r + 1)$ *and $f_{r,2}(x)$ is robust.*

Example

Consider $f_{3,2}(x) = 1 + x + x^8 + x^{10}$.

Example

Consider $f_{3,2}(x) = 1 + x + x^8 + x^{10}$.

- order $(f_{3,2}(x)) = 4^3 + 2^3 + 1 = 73$

Example

Consider $f_{3,2}(x) = 1 + x + x^8 + x^{10}$.

- order $(f_{3,2}(x)) = 4^3 + 2^3 + 1 = 73$
- $\beta_1 (f_{3,2}) = 4^3 - 3^3 + 2^3 = 45$

Example

Consider $f_{3,2}(x) = 1 + x + x^8 + x^{10}$.

- order $(f_{3,2}(x)) = 4^3 + 2^3 + 1 = 73$
- $\beta_1(f_{3,2}) = 4^3 - 3^3 + 2^3 = 45$
- $\beta(f_{3,2}) = (45, 28)$

Example

Consider $f_{3,2}(x) = 1 + x + x^8 + x^{10}$.

- order $(f_{3,2}(x)) = 4^3 + 2^3 + 1 = 73$
- $\beta_1(f_{3,2}) = 4^3 - 3^3 + 2^3 = 45$
- $\beta(f_{3,2}) = (45, 28)$

$$
\begin{aligned}
f_{3,2}^* = 1 &+ x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^9 \\
&+ x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{18} \\
&+ x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{25} + x^{27} \\
&+ x^{28} + x^{29} + x^{30} + x^{31} + x^{36} + x^{37} + x^{38} \\
&+ x^{39} + x^{41} + x^{42} + x^{43} + x^{45} + x^{46} + x^{47} \\
&+ x^{50} + x^{51} + x^{54} + x^{55} + x^{57} + x^{59} + x^{61} + x^{63}
\end{aligned}
$$

Corollary

The reciprocal polynomials $f_{(R),r,2}(x) = 1 + x^2 + x^{2^r+1} + x^{2^r+2}$ *are robust with order dividing* $4^r + 2^r + 1$.

Corollary

The reciprocal polynomials $f_{(R),r,2}(x) = 1 + x^2 + x^{2^r+1} + x^{2^r+2}$ *are robust with order dividing* $4^r + 2^r + 1$.

Example

Consider $f_{(R),3,2}(x) = 1 + x^2 + x^9 + x^{10}$.

- order $f_{(R),3,2} = 73$
- $\beta\left(f_{(R),3,2}\right) = (45, 28)$

Acknowledgements

- The presenter acknowledges support from National Science Foundation grant DMS 08-38434 "EMSW21-MCTP: Research Experience for Graduate Students".
- The presenter also wishes to thank Professor Bruce Reznick for his time, ideas, and encouragement.

Lemma

If $f(x), g(x), h(x) \in \mathbb{F}_2[x]$ *satisfy* $f(x)g(x) = 1 + x^N$ *and* $f(x)h(x) = 1 + x^M$, *where* $N < M$, *then* $\ell(g(x))/N = \ell(h(x))/M$. *In particular, if* $\ell(g(x))/N$ *is in lowest terms, then* N *is the order of* $f(x)$.

Lemma

If $f(x), g(x), h(x) \in \mathbb{F}_2[x]$ *satisfy* $f(x)g(x) = 1 + x^N$ *and* $f(x)h(x) = 1 + x^M$, *where* $N < M$, *then* $\ell(g(x))/N = \ell(h(x))/M$. *In particular, if* $\ell(g(x))/N$ *is in lowest terms, then* N *is the order of* $f(x)$.

Definition

For a non-negative integer k, let $b(k)$ denote the number of 1's in the standard binary representation of k.

Lemma

If $f(x), g(x), h(x) \in \mathbb{F}_2[x]$ satisfy $f(x)g(x) = 1 + x^N$ and $f(x)h(x) = 1 + x^M$, where $N < M$, then $\ell(g(x))/N = \ell(h(x))/M$. In particular, if $\ell(g(x))/N$ is in lowest terms, then N is the order of $f(x)$.

Definition

For a non-negative integer k, let $b(k)$ denote the number of 1's in the standard binary representation of k.

Lemma

For $r \geq 2$,

$$\sum_{k=0}^{2^r-2} 2^{b(k)} = 3^r - 2^r.$$

Lemma

For any polynomial $f(x) \in \mathbb{F}_2(x)$, $f(x^2) = (f(x))^2$, *so* $f(x^{2^m}) = f(x)^{2^m}$.

Lemma

For any polynomial $f(x) \in \mathbb{F}_2(x)$, $f(x^2) = (f(x))^2$, so $f(x^{2^m}) = f(x)^{2^m}$.

Lemma

For $a, b \in \mathbb{N}$,

$$(1 + x^a + x^b) \prod_{j=0}^{m-1} \left(1 + x^{2^j a} + x^{2^j b}\right) = 1 + x^{2^m a} + x^{2^m b}.$$

Lemma

For any polynomial $f(x) \in \mathbb{F}_2(x)$, $f(x^2) = (f(x))^2$, so $f(x^{2^m}) = f(x)^{2^m}$.

Lemma

For $a, b \in \mathbb{N}$,

$$(1 + x^a + x^b) \prod_{j=0}^{m-1} \left(1 + x^{2^j a} + x^{2^j b}\right) = 1 + x^{2^m a} + x^{2^m b}.$$

Lemma

For $1 \leq r \in \mathbb{N}$,

$$\left(1 + x^{2^r-1} + x^{2^r}\right) \left(\prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{2^{2r}-2^r}\right) = 1 + x^{2^{2r}-1}.$$

Proof

Define

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{4^r-2^r}. \qquad (2)$$

By the fourth lemma,

$$\left(1 + x^{2^r-1} + x^{2^r}\right) g_{r,1}(x) = 1 + x^{4^r-1}.$$

Because

$$g_{r,1}(1) = \prod_{j=0}^{r-1} (1+1+1) + 1 \equiv 0 \pmod 2,$$

we know $(1+x) \mid g_{r,1}(x)$.

Because

$$g_{r,1}(1) = \prod_{j=0}^{r-1} (1+1+1) + 1 \equiv 0 \pmod 2,$$

we know $(1+x) \mid g_{r,1}(x)$.

Write $(1+x)h_{r,1}(x) = g_{r,1}(x)$, so

$$\left(1 + x^{2^r-1} + x^{2^r}\right)(1+x)h_{r,1}(x) = 1 + x^{4^r-1}.$$

Because

$$g_{r,1}(1) = \prod_{j=0}^{r-1} (1+1+1) + 1 \equiv 0 \pmod 2,$$

we know $(1+x) \mid g_{r,1}(x)$.

Write $(1+x)h_{r,1}(x) = g_{r,1}(x)$, so

$$\left(1 + x^{2^r-1} + x^{2^r}\right)(1+x)h_{r,1}(x) = 1 + x^{4^r-1}.$$

Since $f_{r,1}(x) = 1 + x + x^{2^r-1} + x^{2^r+1} = (1+x)\left(1 + x^{2^r-1} + x^{2^r}\right)$, we see that $f_{r,1}(x) \mid \left(1 + x^{4^r-1}\right)$.

Rewrite

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{4^r-2^r}$$

to obtain

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j}(1 + x^{2^j})\right) + x^{4^r-2^r}.$$

Expand the product and rewrite, using $1 + x^{2^j} = (1 + x)^{2^j}$, to obtain

$$\begin{aligned} g_{r,1}(x) &= 1 + x^{4^r - 2^r} + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^n \\ &= (1+x)\left(\frac{1 + x^{4^r-2^r}}{1+x} + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}\right) \\ &= (1+x)\left(\sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}\right). \end{aligned}$$

Then

$$h_{r,1}(x) = \sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}.$$

Then

$$h_{r,1}(x) = \sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}.$$

Let

$$S_{r,1}(x) := \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1},$$

which is a polynomial of degree $4^r - 2^r - 1$.

Then

$$h_{r,1}(x) = \sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}.$$

Let

$$S_{r,1}(x) := \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1},$$

which is a polynomial of degree $4^r - 2^r - 1$. By the second lemma,

$$\ell(S_{r,1}(x)) = \sum_{j=1}^{2^r-1} 2^{b(j-1)} = \sum_{k=0}^{2^r-2} 2^{b(k)} = 3^r - 2^r,$$

and $S_{r,1}(x)$ has $4^r - 2^r - (3^r - 2^r) = 4^r - 3^r$ terms with coefficient zero.

To construct $h_{r,1}(x)$, we add $\sum_{j=0}^{4^r-2^r-1} x^j$. Note that the degree of this sum is equal to the degree of $S_{r,1}(x)$.

This addition has the effect of reversing the 0's and 1's, so $\ell(h_{r,1}(x)) = 4^r - 3^r$ and $h_{r,1}(x)$ has $3^r - 2^r$ terms with coefficient 0.

Because the order of $f_{r,1}(x)$ divides $4^r - 1$, we consider $h_{r,1}(x)$ as a polynomial of degree $4^r - 2$, where the additional terms have coefficient 0. When viewed this way, $h_{r,1}(x)$ has $3^r - 1$ terms with coefficient 0.

Hence $(\beta_1(f_{r,1}), \beta_0(f_{r,1})) = (4^r - 3^r, 3^r - 1)$.