Much Odd Circular Enumeration

Cattell Miers Ruskey
Serra

WORKING PAPER – DO NOT DISTRIBUTE

March 3, 1998

Abstract

We derive a formua for the number of trace 1 irreducible polynomials over GF(2) of degree n, and show that this quantity is equal to the number of unlabelled Lyndon words of length n and to the number of some other naturally occuring classes of discrete structures.

Keywords: Irreducible polynomial, trace, Lyndon word, necklace.

The following expression occurs in a wide-variety of contexts.

$$L(n) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{n/d} \tag{1}$$

Less well-known, but occuring almost as often, is the following expression.

$$L_o(n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{n/d} \tag{2}$$

In this paper we discuss various classes of objects counted by $L_o(n)$. In some cases the enumeration is new, in others it was known previously but we provide new proofs. What is lacking in general, but which would be highly desirable, are natural bijections between the various classes of objects.

Theorem 1 *The following values are equinumerous.*

(A) $L_o(n)$

(B) The number of length n Lyndon words of odd density.

(C) *The self-complementary length $2n$ Lyndon words.*

(D) *The number of vortex-free tournaments on n vertices and with maximum cycle length.*

(E) *The number of full-cycles generated by the complementing circulating register.*

(F) *The number of unlabelled Lyndon words of length n.*

(G) *The number of degree n irreducible polynomials over GF(2) with trace 1.*

(H) *The number of degree n irreducible prolynomials over GF(2) of even index.*

(I) *The number of degree $2n$ self-reciprocal irreducible polynomials over GF(2).*

(J) *The number of degree $2n$ self-complementary irreducible polynomials over GF(2).*

(K) *The number of elements of $GF(n) \setminus \{0\}$ whose elements sum to 1 (or, more generally, to b, where $\gcd(b, n)$ is a power of 2).*

(L) *?? The number of unimodal N-sequences (cyclic permutations of $[n]$).*

Two other related sets of numbers are of interest.

$$N(n) = \frac{1}{n} \sum_{d|n} \phi(d) 2^{n/d} \tag{3}$$

$$N_o(n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \phi(d) 2^{n/d} \tag{4}$$

THEOREM 2 *The following values are equinumerous.*

(A') $N_o(n)$

(B') *The number of length n necklaces of odd density.*

(C') *The self-complementary length $2n$ necklaces.*

(D') *The number of vortex-free tournaments on n vertices.*

(E') *The number of cycles generated by the complementing circulating register.*

(F') *The number of unlabelled necklaces of length n and period d such that n/d is odd.*

(G') *The number of irreducible polynomials over GF(2) with trace 1 and degree d such that $n = dm$ for some odd m.*

(H') *The number of irreducible prolynomials over GF(2) of even index and degree d such that $n = dm$ for some odd m.*

(I') *The number self-reciprocal irreducible polynomials over GF(2) with degree* $2d$ *such that $n = dm$ for some odd m.*

(J') *The number of self-complementary irreducible polynomials over GF(2) with degree* $2d$ *such that $n = dm$ for some odd m.*

(K') *The number of subsets of* $GF(n) \setminus \{0\}$ *whose elements sum to* $0 (\mathrm{mod} n)$.

(L') *?? The number of unimodal N-sequences (cyclic permutations of* $[n]$*).*

I'm not really sure about G'-J'.

1 Lyndon words and necklaces

A *Lyndon* word of length n is a binary string of length n that is lexicographically smaller than all of its circular shifts. A *necklace* of length n is a binary string of length n that is lexicographically smaller or equal to all of its circular shifts. For example, the Lyndon words of length 5 are 00001, 00011, 00101, 00111, and 01111. The missing necklaces of length 5 are 00000 and 11111. It is well-known that the number of Lyndon words of length n is $L(n)$ and the number of necklaces is $N(n)$. The *complement* of a bitstring $\mathbf{b} = b_1 b_2 \cdots b_n$ is the bitstring obtained by complementing each bit, $\bar{\mathbf{b}} = \bar{b}_1 \bar{b}_2 \cdots \bar{b}_n$. A Lyndon word (or necklace) is *self-complementary* if $\bar{\mathbf{b}} = \mathbf{b}$.

An *unlabelled Lyndon word* is a Lyndon word that is also no greater than its complement, considered as a circular string. An *unlabelled necklace* is a necklace that is also no greater than its complement, considered as a circular string. For example 00011 is an unlabelled Lyndon word, but 00111 is not, since it is equivalent to 00011 under complement and rotation.

The number of unlabelled necklaces and Lyndon words was considered by Gilbert and Riordan [3]. They showed that the number of unlabelled necklaces is

$$N_u(n) = \frac{1}{2n} \sum_{d|n} \phi(d) 2^{n/d} + \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ even}}} \phi(d) 2^{n/d} = N(n) - N_o(n).$$

and that the number of unlabelled Lyndon words is

$$L_u(n) = \sum_{d|n} \mu(d) N_u(n/d).$$

Let $L(n,k)$ be the number of length n Lyndon words containing exactly k 1's. The following lemma was proven in Davison [2], here we provide a more "combinatorial" proof.

Lemma 1

$$\sum_{k=1}^{n-1} L(n,k)x^k = \frac{1}{n}\sum_{d|n}\mu(d)(1+x^d)^{n/d} \tag{5}$$

Proof: We first show that

$$(1+x)^n = \sum_{d|n} d\sum_{k=0}^{d} L(d,k)x^{kn/d} \tag{6}$$

and then apply Möbius inversion. To prove (6), consider the set of all functions from an n-set $[n]$ to a $(1+x)$-set, say $\{e\}+X$ where $|X|=x$. There are $(1+x)^n$ such functions, f. We can classify them according to (a) the period n/d (where $d \mid n$) of the binary string $\hat{f}(1)\hat{f}(2)\cdots\hat{f}(n)$, where $\hat{f}(i)$ is 0 if $f(i)$ is e and $\hat{f}(i)$ is 1 otherwise, and (b) the number of 1's, k, in $\hat{f}(1)\hat{f}(2)\cdots\hat{f}(d)$. There are $d \cdot L(d,k)$ such strings. In total there are kn/d positions containing elements of X and x choices for those elements. This shows that (6) is true for any number x. Since (6) is a polynomial equation of polynomials in x of degree n, it must be true for any real x.

To express the right hand side of (6) as a function only of d and not of n, we make the substitution of $y^{1/n}$ for x to obtain

$$(1+y^{1/n})^n = \sum_{d|n} d\sum_{k=0}^{d} L(d,k)y^{k/d} \tag{7}$$

We can now apply Möbius inversion to obtain

$$\sum_{k=0}^{n} L(n,k)y^{k/n} = n\sum_{d|n}\mu(d)(1+y^{d/n})^{n/d}.$$

A final re-substitution of x^n for y finishes the proof. ∎

Note that plugging $x=1$ into the equation of Lemma 1 gives the formula for the total number of Lyndon words of length n, namely $L(n)$. Of more interest to us is the case where $x=-1$, which yields

$$L_e(n) - L_o(n) = \frac{1}{n}\sum_{\substack{d|n \\ d \text{ even}}} \mu(d)2^{n/d}$$

Note that this difference is zero if n is odd. Subracting $(L_e(n) + L_o(n)) - (L_e(n) - L_o(n))$, we obtain

$$2 \cdot L_o(n) = L(n) - \frac{1}{n} \sum_{\substack{d|n \\ d \text{ even}}} \mu(d) 2^{n/d} = \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{n/d}.$$

This proves that (A) = (B).

Furthermore, something like the following is true... need to fix...

$$L_e(n) = \begin{cases} L_o(n/2) & \text{if } n \text{ even} \\ 0 & \text{if } n \text{ odd} \end{cases}$$

How do we count the self-complementary Lyndon words?

2 Vortex free tournaments and the complementing register

Knuth [6] considers the equivalence relation generated by

$$b_1 b_2 \cdots b_n \equiv b_2 \cdots b_n \bar{b}_1,$$

over the set of all binary strings of length n. The number of equivalence classes is shown to be equal to the number of vortex-free tournaments on n vertices.

$$\begin{array}{l} 010101 \to 101011 \to 010110 \to 101101 \to 011010 \to 110101 \to \\ 101010 \to 010100 \to 101001 \to 010010 \to 100101 \to 001010 \to \end{array}$$

The strings 000000, 100001, 001001, 011011 also give rise to equivalence classes containing 12 elements and the size of the equivalence class containing 110011 is 4.

Now consider the mapping f that sends two consecutive members of an equivalence class to their exclusive-or. For the class shown above $f(010101, 101011) = 111110$. Applied to other members of the class a circular rotation of 111110 results. This is true in general.

$$\begin{array}{l} (b_1 \oplus b_2)(b_2 \oplus b_3) \cdots (b_{n-1} \oplus b_n)(b_n \oplus \bar{b}_1) \\ (b_2 \oplus b_3) \cdots (b_{n-1} \oplus b_n)(b_n \oplus \bar{b}_1)(\bar{b}_1 \oplus \bar{b}_2) \end{array}$$

Since $\bar{x} \oplus \bar{y} = x \oplus y$, these strings are shifts of one another. Furthermore, they must contain an odd number of 1's since $b_1 \oplus b_2 \oplus b_2 \oplus b_3 \oplus \cdots \oplus b_{n-1} \oplus b_n \oplus b_n \oplus \bar{b}_1 = b_1 \oplus \bar{b}_1 = 1$).

The process is reversible, so long as a value for b_1 is specified. This proves one part of the theorems, namely (D) = (E) and (D') = (E'). The number of cycles generated by the complementing register was counted by Golomb [4] (equation (12) on page 173), showing that (A') = (E').

VFT	$\mathbf{N_o}(6)$	S(6)
000000	000001	000000
010101	011111	011100
100001	000111	001010
001001	001101	010001
011011	001011	000111
		0 1 2 3 4 5

3 Counting irreducible trace one polynomials

To compute the number degree n trace one polynomials over $GF(2)$ we are going to count an equivalent value, the number of trace one elements in $GF(2^n)$. We use $Tr_{n/k}(\alpha)$ to denote the trace of element $\alpha \in GF(2^n)$ relative to the subfield $GF(2^k)$, where k divides n. If $k = 1$ then we simply write $Tr_n(\alpha) = Tr_{n/1}(\alpha)$. The value of the trace is defined to be

$$Tr_{md/m}(\alpha) = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{m(d-1)}} \tag{8}$$

We will use the facts that the trace is linear, that $Tr_n(\alpha) \in GF(2)$, that $Tr_{md/m}(\alpha^{2^m}) = Tr_{md/m}(\alpha)$, and that $Tr_{md}(\alpha) = Tr_m(Tr_{md/m}(\alpha))$. These facts are part of Theorem 2.23 (pg. 52) of Lidl and Niederreiter [8].

Define $T_1(n)$ to be the number of trace 1 elements of GF(2^n) that are not in any subfield. Define $T_0(n)$ to be the number of trace 0 elements of GF(2^n) that are not in any subfield. Let $T(n) = T_1(n) + T_0(n)$ be the total number of elements of GF(2^n) that are not in any subfield.

Lemma 2

$$2^{n-1} = \sum_{\substack{d|n \\ d \text{ odd}}} T_1(d). \tag{9}$$

Proof: We count the number of trace one elements in $GF(2^n)$ in two different ways.

The quadradic $z^2 + z = \alpha$ has exactly two distinct solutions over $GF(2^n)$ if $Tr(\alpha) = 0$ (e.g., see McEliece [9] pg. 105). Thus there are at least as many trace 1 elements as trace 0 elements; in particular there is at least one. Let $\lambda \in GF(2^n)$ have trace one. For each element $\beta \in GF(2^n)$, the traces $Tr(\beta)$ and $Tr(\beta+\lambda) = Tr(\beta)+1$ are different. Therefore, there are 2^{n-1} trace one elements in $GF(2^n)$, giving us the left-hand side of (9).

Suppose that $\alpha \in GF(2^m)$ has trace one, $Tr_m(\alpha) = 1$. What is $Tr_{md}(\alpha)$? Compute

$$\begin{aligned}
Tr_{md}(\alpha) &= Tr_m(Tr_{md/m}(\alpha)) \\
&= Tr_m(\alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{m(d-1)}}) \\
&= Tr_m(\alpha) + Tr_m(\alpha^{2^m}) + Tr_m(\alpha^{2^{2m}}) + \cdots + Tr_m(\alpha^{2^{m(d-1)}}) \\
&= Tr_m(\alpha) + Tr_m(\alpha^{2^m}) + Tr_m((\alpha^{2^m})^{2^m}) + \cdots + Tr_m((\alpha^{2^{m(d-2)}})^{2^m}) \\
&= 1 + 1 + \cdots + 1 \qquad (d \text{ terms}) \\
&= d \qquad (\mathrm{mod} 2).
\end{aligned}$$

Thus the trace is even if d is even and is odd if d is odd. Furthermore, if $Tr_m(\alpha) = 0$ then $Tr_{md}(\alpha)$ is zero, no matter the parity of d. Thus, an element of trace one in $GF(2^n)$ has trace one in a subfield $GF(2^{n/d})$ if and only if d is odd. By summing all odd extensions we obtain the right-hand side of 9. ■

It is also worth noting that

$$2^m = \sum_{d|m} T(d) \tag{10}$$

Theorem 3 (Modified Möbius Inversion) *The following two statements are equivalent. (a) For all numbers n*

$$f(n) = \sum_{\substack{d|n \\ d \text{ odd}}} g(n/d).$$

(b) For all numbers n

$$g(n) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) f(n/d).$$

Applying the last theorem to (9) we obtain

$$T_1(n) = \frac{1}{2} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{n/d}. \tag{11}$$

Note that

$$\sum_{\substack{d|2n \\ d \text{ even}}} f(d) = \sum_{d|n} f(2d)$$

and

$$\mu(2d) = \begin{cases} 0 & \text{if } d \text{ even} \\ -\mu(d) & \text{if } d \text{ odd} \end{cases}.$$

If n is even then

$$
\begin{aligned}
2 \cdot T_0(n) &= 2 \cdot T(n) - 2 \cdot T_1(n) \\
&= 2 \sum_{d|n} \mu(d) 2^{n/d} - \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{n/d} \\
&= \sum_{d|n} \mu(d) 2^{n/d} + \sum_{\substack{d|n \\ d \text{ even}}} \mu(d) 2^{n/d} \\
&= T(n) + \sum_{d|(n/2)} \mu(2d) 2^{n/(2d)} \\
&= T(n) - \sum_{\substack{d|(n/2) \\ d \text{ odd}}} \mu(d) 2^{(n/2)/d} \\
&= T(n) - 2T_1(n/2)
\end{aligned}
$$

Subtracting $T_0(n)$ from both sides and re-arranging yields

$$T_1(n) = T_0(n) + 2T_1(n/2)$$

The number of irreducible polynomials over $GF(2)$ is $T(n)/n$ since the n conjugates $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ of an element of $GF(2^n)$ not contained in any subfield all have the same minimal polynomial. The number of trace 1 irreducible polynomials over $GF(2)$ is $T_1(n)/n$. The number of trace 0 irreducible polynomials over $GF(2)$ is $T_0(n)/n$. Note that $L(n) = T(n)/n$, $L_o(n) = T_1(n)/n$, and $L_e(n) = T_0(n)/n$, thereby proving one part of Theorem 1, namely (A) = (G).

4 Subsets summing to zero

Consider the set of all 2^{n-1} subsets of $\{1, 2, \ldots, n-1\}$. How many of these subsets sum to zero mod n? Call the answer $f(n)$. For example, $f(6) = 5$ since only the 6 subsets $\emptyset, \{1,2,3\}, \{2,4\}, \{1,5\}, \{3,4,5\}$ sum to 0 mod 6. We will show that $f(n) = N_o(n)$, repeating the development of Stanley [11] in Exercise 27, pg. 48 and its solution on pg. 59. We count the number of subsets of $\{0, 1, \ldots, n-1\}$ that sum to zero mod n. This count is twice $f(n)$ since every solution including 0 can be matched with a solution that doesn't include 0.

Let $P(x) = (1+x)(1+x^2)\cdots(1+x^n) = \sum_{k \geq 0} a_k x^k$. Observe that $2f(n) = \sum_j a_{jn}$. Let ζ be a primitive n-th root of unity. For any integer k

$$\sum_{j=1}^{n} \zeta^{jk} = \begin{cases} n, & \text{if } n|k \\ 0, & \text{otherwise} \end{cases}$$

Thus

$$\begin{aligned}\frac{1}{n}\sum_{j=1}^{n} P(\zeta^j) &= \frac{1}{n}\sum_{j=1}^{n}\sum_{k\geq 0} a_k \zeta^{jk} \\ &= \frac{1}{n}\sum_{k\geq 0}\sum_{j=1}^{n} a_k \zeta^{jk} \\ &= \sum_{j} a_{jn}\end{aligned}$$

If ζ^j is a primitive d-th root of unity (or equivalently, $dn = \gcd(j,n)$), then

$$x^d - 1 = (x-\zeta^j)(x-\zeta^{2j})\cdots(x-\zeta^{dj}) \tag{12}$$

Setting $x = -1$ in (12) gives

$$(1+\zeta^j)(1+\zeta^{2j})\cdots(1+\zeta^{dj}) = \begin{cases} 2 & \text{if } d \text{ odd} \\ 0 & \text{if } d \text{ even.}\end{cases}$$

Hence

$$P(\zeta^j) = \begin{cases} 2^{n/d} & \text{if } d \text{ odd} \\ 0 & \text{if } d \text{ even}\end{cases}$$

The proof of $f(n) = N_o(n)$ is finished by observing that there are $\phi(d)$ values $j \in [n]$ for which ζ^j is a primitive d-th root.

We now adapt the preceding argument to the case where the subsets sum to 1 mod n. Let $\mathcal{P}(d)$ denote the set of all $\phi(d)$ primitive d-th roots of unity.

The following lemma will prove useful.

Lemma 3 *For all numbers d,*

$$\sum_{\zeta\in\mathcal{P}(d)} \zeta = \sum_{\gcd(k,d)=1} \cos(2\pi k/d) = \mu(d).$$

For all numbers d,

$$\sum_{\zeta\in\mathcal{P}(d)} \zeta^2 = \sum_{\gcd(k,d)=1} \cos(4\pi k/d) = \begin{cases} \mu(d) & \textit{if } d \textit{ odd} \\ \mu(d/2) & \textit{if } d \textit{ even.}\end{cases}$$

Proof: To get the first part of the lemma, apply Möbius inversion to

$$\sum_{d|n}\sum_{\zeta\in\mathcal{P}(d)} \zeta = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1\end{cases}$$

∎

Now we want the coefficients x^k of $(P(x)-1)/x$ such that $n \mid k$.

$$\begin{aligned}
\frac{1}{n}\sum_{j=1}^{n}(P(\zeta^j)-1)/\zeta^j &= \frac{1}{n}\sum_{j=1}^{n}\zeta^{n-j}P(\zeta^j) - \frac{1}{n}\sum_{j=1}^{n}\zeta^{n-1} \\
&= \frac{1}{n}\sum_{\substack{d\mid n \\ d \text{ odd}}}\sum_{\zeta\in\mathcal{P}(d)}\zeta\cdot 2^{n/d} \\
&= 2L_o(n)
\end{aligned}$$

For the case where the sum is 2 mod n,

$$\frac{1}{n}\sum_{j=1}^{n}\frac{P(\zeta^j)-\zeta^j-1}{\zeta^{2j}} = \frac{1}{n}\sum_{\substack{d\mid n \\ d \text{ odd}}}\sum_{\zeta\in\mathcal{P}(d)}\zeta^2\cdot 2^{n/d}$$

5 Trace and subtrace

The trace of a polynomial of degree n is the coefficient of x^{n-1}. Define the *sub-trace* to be the coefficient of x^{n-2}. In this section we enumerate the number of irreducible polynomials over GF(2) with given trace and subtrace. Let $L(n,k)$ be the number of length n Lyndon words of density k. It is known that

$$L(n,k) = \frac{1}{n}\sum_{d\,\mid\,\gcd(n,k)}\mu(d)\binom{n/d}{k/d}. \tag{13}$$

A simple proof is obtained by writing the right hand side of 5 as

$$\frac{1}{n}\sum_{d\mid n}\mu(d)\sum_{p=0}^{n/d}\binom{n/d}{p}x^{dp}$$

and then extracting the coefficient of x^k.

For $S \subseteq \{0,1,\ldots,n\}$, let

$$e(S) = \sum_{k\in S}L(n,k).$$

Note that $e(\{0,1,\ldots,n\}) = L(n)$ and $e(\{k \mid k \text{ is odd }\}) = L_o(n)$.

Theorem 4 *The number of irreducible polynomials of degree n over $GF(2)$ with given trace and subtrace is covered by one of the following cases.*

- *The number of trace 0, subtrace 1 polynomials is* $e(\{k \mid (k+n) \equiv 0 \pmod 4\})$.

- *The number of trace 1, subtrace 0 polynomials is* $e(\{k \mid (k+n) \equiv 1 \pmod 4\})$.
- *The number of trace 0, subtrace 0 polynomials is* $e(\{k \mid (k+n) \equiv 2 \pmod 4\})$.
- *The number of trace 1, subtrace 1 polynomials is* $e(\{k \mid (k+n) \equiv 3 \pmod 4\})$.

Proof: Yet to be discovered! □

6 Self-complementary polynomials

Recall that a polynomial $p(x)$ is *self-complementary* if $p(x) = p(x+1)$. Any self-complementary irreducible polynomial must have even degree, as we shall see below in Theorem 6. We hope to prove the following theorem.

Theorem 5 *Let* $p(x) = a_0 + \cdots + a_{n-3}x^{n-3} + a_{n-2}x^{n-2} + a_{n-1}x^{n-1} + a_n x^n$ *be a self-complementary irreducible polynomial over GF(2) of degree* $n = 2m$. *Then the following table gives the values of* a_{n-3}, a_{n-2}, *and* a_{n-1} *depending on the value of* m *mod 4.*

$m \bmod 4$	a_{n-3}	a_{n-2}	a_{n-1}
0	*1*	*1*	*0*
1	*0*	*1*	*1*
2	*1*	*0*	*0*
3	*1*	*0*	*1*

Proof: Yet to be discovered! □

Not every self-complementary polynomial is irreducible. For example, $1+x^2+x^4$ is reducible and self-complementary. We can prove the following for self-complementary polynomials, not necessarily irreducible, over GF(2).

Theorem 6 *Let* $p(x) = a_0 + \cdots + a_{n-3}x^{n-3} + a_{n-2}x^{n-2} + a_{n-1}x^{n-1} + a_n x^n$ *be a self-complementary polynomial over GF(2) of degree* n. *Then*

- n *must be even, and*
- $\sum a_i = a_0 \pmod 2$, *and*
- $a_{n-1} = 0$ *if and only if* $4 \mid n$, *and*
-
  - *if* $n = 0 \bmod 8$, *then* $a_{n-3} = a_{n-2}$,
  - *if* $n = 2 \bmod 8$, *then* $a_{n-3} = 0$,

– *if* $n = 4 \bmod 8$*, then* $a_{n-3} = \overline{a_{n-2}}$*,*

– *if* $n = 6 \bmod 8$*, then* $a_{n-3} = 1$*.*

Proof: Let $p(x)$ be a polynomial of degree n over GF(2).

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

Then

$$\begin{aligned} p(x+1) &= c_n(x+1)^n + c_{n-1}(x+1)^{n-1} + \cdots + c_1(x+1) + c_0 1 \\ &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 1, \end{aligned}$$

where

$$a_i = \sum_{k=i}^{n} c_k \binom{k}{i} \pmod 2$$

Now suppose that $p(x) = p(x+1)$. Then $a_k = c_k$ for $k = 0, 1, \ldots, n$. Let's look at the values $k = n-1, n-2, n-3$, and $n-4$.

$$\begin{aligned} c_{n-1} &= \sum_{k=n-1}^{n} c_k \binom{k}{n-1} \pmod 2 \\ &= c_{n-1}\binom{n-1}{n-1} + c_n \binom{n}{n-1} \pmod 2 \\ &= c_{n-1} + n \pmod 2 \end{aligned}$$

This last equation implies that n must be even. For $k = n-2$ we have

$$\begin{aligned} c_{n-2} &= \sum_{k=n-2}^{n} c_k \binom{k}{n-2} \pmod 2 \\ &= c_{n-2}\binom{n-2}{n-2} + c_{n-1}\binom{n-1}{n-2} + c_n \binom{n}{n-2} \pmod 2 \\ &= c_{n-2} + c_{n-1} + \binom{n}{2} \pmod 2 \end{aligned}$$

Thus $c_{n-1} = \binom{n}{2} \bmod 2$, which means that $c_{n-1} = 0$ if and only if 4 divides n. This determines the trace. Now consider $k = n-3$.

$$
\begin{aligned}
c_{n-3} &= \sum_{k=n-3}^{n} c_k \binom{k}{n-3} \pmod 2 \\
&= c_{n-3}\binom{n-3}{n-3} + c_{n-2}\binom{n-2}{n-3} + c_{n-1}\binom{n-1}{n-3} + c_n\binom{n}{n-3} \pmod 2 \\
&= c_{n-3} + c_{n-1}\binom{n-1}{2} + \binom{n}{3} \pmod 2
\end{aligned}
$$

Blech! Unfortunately, this doesn't tell us anything about c_{n-2}. Note, for reference, however, that $\binom{n}{3} = 1 \pmod 2$ if and only if $n = 3 \pmod 4$.

$$
\begin{aligned}
c_{n-4} &= \sum_{k=n-4}^{n} c_k \binom{k}{n-4} \pmod 2 \\
&= c_{n-4}\binom{n-4}{n-4} + c_{n-3}\binom{n-3}{n-4} + c_{n-2}\binom{n-2}{n-4} + c_{n-1}\binom{n-1}{n-4} + c_n\binom{n}{n-4} \pmod 2 \\
&= c_{n-4} + c_{n-3} + c_{n-2}\binom{n-2}{2} + c_{n-1}\binom{n-1}{3} + \binom{n}{4} \pmod 2
\end{aligned}
$$

Using the fact that $\binom{n}{4}$ mod 2 is 1 if $n = 0, 1, 2, 3$ mod 8 and is 0 if $n = 4, 5, 6, 7$ mod 8, together with what we learned before yields the final result stated in the theorem. □

There are 4 degree 4 self-complementary polynomial over GF(2), namely 00101, 01001, 10101, 11001. Observe that if $a_0 + a_1x + \cdots + a_nx^n$ is self-complementary, then so is $\overline{a_0} + a_1x + \cdots + a_nx^n$. The 4 degree 6 self-complementary polynomials over GF(2) with $a_0 = 0$ are 0001111, 0011011, 0101011, 0111111.

LEMMA 4 *The polynomial $s(x) = s_0 + s_1x + \cdots + s_{2m}x^{2m}$, whose coefficients are specified below, is self-complementary. The low order first m coefficients are 0, that is $s_0 = s_1 = \cdots = s_{m-1} = 0$. For $k = 0, 1, \ldots, m$,*

$$
s_{m+k} = \binom{m}{k} \pmod 2
$$

PROOF: We need to show that

$$
\sum_{k=i}^{2m} \binom{m}{k-m}\binom{k}{i} \equiv \binom{m}{i-m} \pmod 2
$$

This follows at once from the fact that

$$\sum_{k=i}^{2m}(-1)^k \binom{m}{k-m}\binom{k}{i} = \binom{m}{i-m},$$

which follows as a result of identity (3.49) of Gound [5] which is repeated below.

$$\sum_{k=0}^{n}(-1)^k \binom{n}{k}\binom{x-k}{r} = \binom{x-n}{r-n}$$

□

The preceding lemma show that there is at least one self-complementary polynomial of any even degree; below we show exactly how many there are.

Theorem 7 *The number of self-complementary polynomials of degree* $2m$ *is* 2^m. *More generally, the number of self-complementary polynomials for which* $a_1 = a_2 = \cdots = a_k = 0$ *is* 2^{m-k-1}.

Proof:

Let $\mathbf{S}_n$ denote the set of all self-complementary polynomials of degree $2n$. Let $\mathbf{A}_n = \cup_{0 \le i \le n} \mathbf{S}_n$.

Note that if p and q are self-complementary polynomials, then so is $p+q$. In other words, $\mathbf{A}_n$ is a linear set.

We now show that if p is a degree $2n$ self-complementary poly, then $\mathbf{S}_n = p + \mathbf{A}_{n-1}$.

If $q \in p + \mathbf{A}_{n-1}$, then q is self-complementary, and $deg(q) = 2n$. Thus $\mathbf{S}_n \supseteq p + \mathbf{A}_{n-1}$. If $q \in \mathbf{S}_n$, then $r = q + p$ is self-complementary and has degree strictly less than $2n$, and so $r \in \mathbf{A}_{n-1}$. Thus $\mathbf{S}_n \subseteq p + \mathbf{A}_{n-1}$.

This says that any basis for $\mathbf{A}_n$ has one poly of each even degree (i.e. a basis for $\mathbf{A}_n$ is formed from a basis for $\mathbf{A}_{n-1}$ by throwing in a degree $2n$ poly). □

Some interesting(?) observations regarding irreducible self-complementary polynomials over GF(2) for particular values of n. Whether there is a general pattern is not known.

- If $n = 12$ then $a_7 = 0$.
- If $n = 14$ then $a_7 = 1$.
- If $n = 16$ then $a_7 = 1$.
- If $n = 18$ then $a_{11} = a_{13}$.
- If $n = 20$ then $a_{15} = 0$ and $a_{13} = a_{14}$.

- If $n = 22$ then $a_{15} = 0$ and $a_{13} = a_{14}$ and $a_{17} = \overline{a_{18}}$.
- If $n = 24$ then $a_{15} = 0$ and $a_{19} = 1$ and $a_{13} = a_{14}$.
- If $n = 26$ then $a_{15} = 0$ and $a_{13} = a_{14}$ and $a_{22} = a_{21} = \overline{a_{19}}$.
- If $n = 28$ then $a_{15} = a_{23} = 0$ and $a_{13} = \overline{a_{14}}$ and $a_{19} = a_{22} = \overline{a_{21}}$.
- If $n = 30$ then $a_{15} = a_{23} = 1$ and $a_{13} = \overline{a_{14}}$ and $a_{21} = \overline{a_{22}}$ and $a_{25} = \overline{a_{26}}$.

Here is an interesting conjecture. If $p(x)$ is a generating function then $< x^k > p(x)$ denotes the coefficient of x^k in $p(x)$. The minimal polynomial of a finite field element β is denoted $min_\beta(x)$.

THEOREM 8 *If β is the root of a self-complementary polynomial of degree $2m$, then*

$$\langle x^{2m-4} \rangle min_\beta(x) = f(m) + \langle x^{m-2} \rangle min_{\beta^2+\beta}(x) \bmod 2,$$

where f is a function from numbers to $\{0, 1\}$.

References

[1] L. Carlitz, *Some theorems on irreducible reciprocal polynomials over a finite field*, J. reine angew. Math., 227 (1967) 212-220.

[2] J.L. Davison, *Lyndon graphs are not Hamiltonian for n even*, J. Combinatorial Math. and Combinatorial Computing, 11 (1992) 109-112.

[3] E.N. Gilbert and J. Riordan, *Symmetry Types of Periodic Sequences*, Illinois J. Mathematics, 657-665.

[4] S.W. Golomb, *Shift Register Sequences*, Holden-Day, 1967.

[5] H.W. Gould, *Combinatorial Identities*, Morgantown Printing and Binding, 1972.

[6] D.E. Knuth, *Axioms and Hulls*, Lecture Notes in Computer Science #606, Springer-Verlag, 1992.

[7] D.E. Knuth, R.L. Graham, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.

[8] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[9] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[10] R.L. Miller, *Necklaces, symmetries, and self-reciprocal polynomials*, Discrete Math., 22 (1978) 25-33.

[11] R.P. Stanley, *Enumerative Combinatorics, Vol. I*, Wadsworth & Brooks/Cole, 1986.

n	a_n	b_n	nb_n	$T(n)$	$T_1(n)$	$T_0(n)$
1	2	0?	0			
2	1	0	0			
3	1	1	3			
4	2	0	0	12	8	4
5	3	2	10	30	15	15
6	5	2	12	54	30	24
7	9	4	28	126	63	63
8	16	8	64	240	128	112
9	28	13	117			
10	51	24	240			
11	93	48	528			
12	170	80	960			
13	315	160	2080			
14	585	288	4032			
15	1091	541	8115			
16	2048	1024	16384			

7 Extra goodies

The material in this section is not meant for publication. It is just some tables and notes that the referees may find useful.

8 Tables

Below are the binomial coefficients mod 2.

```
101010101010101
 11001100110011
  1000100010001
   111100001111
    10100000101
     1100000011
      100000001
       11111111
        1010101
         110011
          10001
           1111
```

$k \setminus n$	0	1	2	3	4	5	6	7	8	9			
0	1												
1	1	1											
2	1	2	1										
3	1	3	3	1									
4	1	4	6	4	1								
5	1	5	10	10	5	1							
6	1	6	15	20	15	6	1						
7	1	7	21	35	35	21	7	1					
8	1	8	28	56	70	56	28	8	1				
9	1	9	36	84	126	126	84	36	9	1			
10	1	10	45	120	210	252	210	120	45	10	1		
11	1	11	55	165	330	462	462	330	165	55	11	1	
12	1	12	66	220	495	792	924	792	495	220	66	12	1
13	1	13	78	286									

Table 1: Table of $C(n, k)$ (binomial coefficients).

```
101
 11
  1
```

9 Extending a classic result?

Let $\mathbf{I}_n(x)$ be the product of all irreducible polynomials of degree n. The formula for the number of irreducible polynomials comes from the fact that

$$x^{2^n} - x = \prod_{d|n} I_n(x). \tag{14}$$

Equation (2) suggests that it should be true that

$$x^{2^{m-1}} + \text{ lower order terms } = \prod_{\substack{d|n \\ d \text{ odd}}} X_n(x), \tag{15}$$

Where X is one of those classes of polynomials counted by $L(n)$. Is this, in fact, the case?

Observation: The only polynomial $f(x)$ for which $f(x) = f^*(x)$ and $f(x) = f(x+1)$ is $x^2 + x + 1$.

$k \setminus n$	1	2	3	4	5	6	7	8	9	10					
2	1														
3	1	1													
4	1	1	1												
5	1	2	2	1											
6	1	2	3	2	1										
7	1	3	5	5	3	1									
8	1	3	7	8	7	3	1								
9	1	4	9	14	14	9	4	1							
10	1	4	12	20	25	20	12	4	1						
11	1	5	15	30	42	42	30	15	5	1					
12	1	5	18	40	66	75	66	40	18	5	1				
13	1	6	22	55	99	132	132	99	55	22	6	1			
14	1	6	26	70	143	212	245	212	143	70	26	6	1		
15	1	7	30	91	200	333	429	429	333	200	91	30	7	1	
16	1	7	35	112	273	497	715	800	715	497	273	112	35	7	1

Table 2: Table of $L(n,k)$ (Lyndon words of density k).

9.1 Proof of Theorem 3

We will use the following two identities from [7] ((4.9) on pg. 105 and (4.55) on pg. 136).

$$\sum_{m|n}\sum_{k|m} a_{k,m} = \sum_{k|n}\sum_{m|(n/k)} a_{k,km} \tag{16}$$

$$\sum_{d|m}\mu(d) = \sum_{d|m}\mu(m/d) = [m=1] \tag{17}$$

Let $n = 2^k m$ where m is an odd number.

$$\begin{aligned}
\sum_{\substack{d|n \\ d \text{ odd}}} g(2^k m/d) &= \sum_{d|m}\sum_{\substack{c|(2^k m/d) \\ d \text{ odd}}} \mu(c) f(\frac{2^k m/d}{c}) \\
&= \sum_{d|m}\sum_{c|(m/d)} \mu(c) f(\frac{2^k m/d}{c}) \\
&= \sum_{c|m}\sum_{d|c} \mu(\frac{c}{d}) f(\frac{2^k m}{c}) \\
&= \sum_{c|m} f(\frac{2^k m}{c}) \sum_{d|c} \mu(\frac{c}{d})
\end{aligned}$$

n\k	0	1	2	3	4	5	6	7	8									
1	1																	
2	1	1																
3	2	1	1															
4	2	2	2	2														
5	4	3	3	3	3													
6	6	5	5	6	5	5												
7	10	9	9	9	9	9	9											
8	16	16	16	16	16	16	16	16										
9	30	28	28	29	28	28	29	28	28									
10	52	51	51	51	51	52	51	51	51	51								
11	94	93	93	93	93	93	93	93	93	93	93							
12	172	170	170	172	170	170	172	170	170	172	170	170						
13	316	315	315	315	315	315	315	315	315	315	315	315	315					
14	586	585	585	585	585	585	585	586	585	585	585	585	585	585				
15	1096	1091	1091	1094	1091	1092	1094	1091	1091	1094	1092	1091	1094	1091	1091			
16	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048	2048		
17	3856	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	3855	
18	7286	7280	7280	7285	7280	7280	7285	7280	7280	7286	7280	7280	7285	7280	7280	7285	7280	7280

Table 3: Number of subsets of 1,2,...,n-1 summing to k mod n.

$$
\begin{aligned}
&= \sum_{c|m} f(\frac{2^k m}{c})[c=1] \\
&= f(2^k m) = f(n).
\end{aligned}
$$

The verification in the other direction is very similar and is omitted.