

# Distribution of Irreducible Polynomials over $F_2$

Kenneth H. Hicks<sup>1</sup>, Gary L. Mullen<sup>2</sup>, and Ikuro Sato<sup>1</sup>

<sup>1</sup> Department of Physics, Ohio University, Athens OH 45701

<sup>2</sup> Department of Mathematics, The Pennsylvania State University,  
University Park PA 16802, *email:mullen@math.psu.edu*

**Abstract.** Using a polynomial analogue of the wheel sieve, we discuss the distribution of irreducible polynomials over  $F_2$ . In particular, we provide considerable numerical evidence that in analogue to integer arithmetic progressions, irreducible polynomials over  $F_2$  are binomially distributed in the progressions of the wheel sieve. We also present numerical evidence that the irreducibles of fixed degree are binomially distributed by weight. Also briefly discussed is the distribution of self-reciprocal irreducible polynomials. A number of conjectures are raised.

## 1 Introduction

Let  $F_q$  denote the finite field of order  $q$  where  $q$  is a prime number, and let  $F_q[x]$  denote the ring of all polynomials over  $F_q$  in the variable  $x$ . It is well known that the ring  $Z$  of integers and the polynomial ring  $F_q[x]$  share a number of common properties. For example, the ring  $Z$  has unique factorization into primes while the ring  $F_q[x]$  has unique factorization into irreducible polynomials. Moreover, in each case there are an infinite number of prime elements. In  $Z$ , this is simply Euclid's Theorem that there are infinitely many primes. In the polynomial setting, this result follows from the fact that for each degree  $d \geq 1$ , there is an irreducible polynomial of degree  $d$  over  $F_q$ , see [6] page 93.

Dirichlet's Theorem on primes in an arithmetic progression provides a refinement of Euclid's theorem to the effect that if  $(a, b) = 1$ , then there are infinitely many primes in the progression  $an + b$  as  $n$  runs through the set of positive integers. In the polynomial ring setting, the analogous result was first proved by Kornblum [5] and states that if  $(A(x), B(x)) = 1$ , then the progression  $A(x)Y + B(x)$  contains infinitely many irreducible polynomials as  $Y$  varies through the elements of  $F_q[x]$ .

While a computer sieve study of the distribution of irreducible polynomials could be conducted for fields of prime or even prime power order, throughout the remainder of this paper we will focus only on the case where  $q = 2$ . How does one order the polynomials in  $F_q[x]$ ? Corresponding to the polynomial  $f(x) = a_n x^n + \cdots + a_1 x + a_0$ , we may naturally associate the integer  $I_f = a_n 2^n + \cdots + a_1 2 + a_0$ . Since each  $a_i \in F_2$  and hence may be assumed to be either zero or one, this is of course simply the base 2 representation of

the integer  $I_f$ . We will often say things like  $N_1(x) < N_2(x)$ , meaning that subject to the above ordering, the polynomial  $N_1(x)$  occurs before  $N_2(x)$ . While this is an small abuse of the notation, the meaning should be clear from the context.

The wheel sieve for integers was first described by Pritchard [7] as a sublinear algorithm for computer prime number sieve routines. In [3], this technique was used to study the distribution of primes in sets of arithmetic progressions of the form  $a + nm_k$  where, if  $p_i$  denotes the  $i$ -th prime, the multiplier  $m_k$  is the  $k$ -th *primorial* number  $p_1 \cdot p_2 \cdot \dots \cdot p_k$  and  $a < m_{k-1}$  is any number relatively prime to  $m_k$ . The heuristics in [3] show that the primes are distributed binomially among the arithmetic progressions  $a + nm_k$ , using a binomial probability given by the asymptotic value from Dirichlet's Theorem.

In Section 2 we discuss a polynomial version of the wheel sieve, and in Section 3 we consider the distribution of irreducibles in arithmetic progressions. Section 4 is devoted to a discussion of irreducibles by weight. We close with Section 5, which provides a brief discussion of the distribution of self-reciprocal irreducible polynomials.

## 2 The Polynomial Wheel Sieve

For an integer  $k \geq 1$ , let  $M_k(x) = P_1(x) \cdots P_k(x)$  be the product of the first  $k$  monic irreducibles in  $F_q[x]$ . The polynomial  $M_k(x)$  corresponds to the  $k$ -th primorial number  $p_1 \cdots p_k$ , and will be called the  $k$ -th *primorial polynomial*. For each value of  $k \geq 1$ , the wheel sieve generates a sequence of polynomials, using an interactive process with polynomials from the previous cycle as seeds.

**Definition 1.** For a fixed prime  $p_i$ , let  $W_1 = \{1, 2, \dots, p_i - 1, x\}$  be the set of initial polynomials. Given  $W_k$ , let  $S_k = \{S \in W_k \mid P_k(x) \nmid S\}$  be the set after sieving the set  $W_k$  by the irreducible  $P_k$ . Then  $W_{k+1} = \{S(x) + N(x)M_k(x) \mid S(x) \in S_k, \deg(N) < \deg(P_k)\}$  and  $N(x)$  runs through all polynomials  $< P_k$ .

Let  $\mathbf{W}_k$  be the matrix containing the set  $W_k$ , with  $q^{\deg(P_k)}$  columns. The first column is the set  $S_{k-1}$ , ordered increasingly. And the remaining columns as we move from left to right, contain successive multiples of the primorial polynomial  $M_{k-1}(x)$  added to the first polynomial in column 1.

**Example 1:** Let  $q = 2$ . The first four irreducible polynomials over  $F_2$  are  $P_1(x) = x$ ,  $P_2(x) = x + 1$ ,  $P_3(x) = x^2 + x + 1$ ,  $P_4(x) = x^3 + x + 1$ , and the first three primorial polynomials are  $M_1(x) = x$ ,  $M_2(x) = x^2 + x$ ,  $M_3(x) = x^4 + x$ . Then we have the trivial case

$$W_1 = \{1, x\}, S_1 = \{1\}.$$

Continuing we have

$$W_2 = \{1, x + 1\}, S_2 = \{1\},$$

and

$$W_3 = \{1, x^2 + x + 1, x^3 + x^2 + 1, x^3 + x + 1\}, S_3 = \{1, x^3 + x^2 + 1, x^3 + x + 1\}$$

or using a more compact notation, where the polynomial  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  is abbreviated in the form  $a_n a_{n-1} \dots a_0$ , we have  $S_3 = \{1, 1101, 1011\}$ .

For the next case,

$$\mathbf{W}_4 = \begin{pmatrix} 1 & 10011 & 100101 & 110111 & 1001001 & 1011011 & 1101101 & 1111111 \\ 1011 & 11001 & 101111 & 111101 & 1000011 & 1010001 & 1100111 & 1110101 \\ 1101 & 11111 & 101001 & 111011 & 1000101 & 1010111 & 1100001 & 1110011 \end{pmatrix}$$

and

$$S_4 = \left\{ \begin{array}{cccccccc} 1 & 10011 & 100101 & 110111 & 1001001 & 1011011 & 1101101 & \\ & 11001 & 101111 & 111101 & 1000011 & 1010001 & 1100111 & 1110101 \\ 1101 & 11111 & 101001 & 111011 & & 1010111 & 1100001 & 1110011 \end{array} \right\}$$

**Remark.** An alternative definition of  $S_k$  might be helpful. Since each polynomial in  $S_k$  is relatively prime to  $M_k(x)$ , one could also say  $S_k = \{f \in F_q[x] \mid \deg(f) < \deg(M_k), \gcd(f, M_k) = 1\}$ .

As indicated on page 122 of [6], there is a function  $\Phi_q$  defined for nonzero polynomials  $f$  in  $F_q[x]$  which counts the number of polynomials in  $F_q[x]$  that are of smaller degree than the degree of  $f$  and which are relatively prime to  $f$ . Lemma 3.69 of [6] provides some of the basic properties of this function, and shows that this function has many of the properties of the Euler function  $\phi$  from elementary number theory. The function  $\Phi_q$  is multiplicative and if  $f \in F_q[x]$  has degree  $n \geq 1$ , then  $\Phi_q(f) = q^n(1 - q^{-n_1}) \dots (1 - q^{-n_r})$ , where the  $n_i$  are the degrees of the distinct monic irreducible polynomials appearing in the canonical factorization of  $f$  in  $F_q[x]$ . This formula can be rewritten to appear to look more like the formula for the usual Euler  $\phi$  function. In particular, if  $f = P_1^{e_1} \dots P_r^{e_r}$  where each  $P_i$  is irreducible, then

$$\Phi_q(f) = \prod_{i=1}^r (q^{n_i e_i} - q^{n_i(e_i-1)}) \quad .$$

**Lemma 1.** *The number of elements in  $S_k$  is*

$$\#S_k = \Phi_q(M_k(x)) = \prod_{i=1}^k (q^{n_i} - 1)$$

where  $n_i$  is the degree of  $P_i(x)$ .

*Proof.* This is a trivial result of the definition of  $\Phi_q(f)$ .

### 3 Irreducibles in Arithmetic Progressions

The wheel sieve provides a natural framework to study the distribution of irreducible polynomials in sets of arithmetic progressions. Following the notation of Hayes [2], let  $H$  be a polynomial over a finite field of  $q$  elements and  $A$  be a polynomial prime to  $H$ . If  $\pi(r; H, A)$  is the number of irreducibles of degree  $r$  which are congruent to  $A \pmod{H}$ , then a theorem of Artin states

$$\pi(r; H, A) \sim \frac{1}{\Phi_q(H)} \cdot \frac{q^r}{r} \quad (1)$$

with an error term that is  $\mathcal{O}(q^{r\nu}/r)$  for some  $\nu < 1$ , see [2]. We note that the fraction  $q^r/r$  is an asymptotic expression for  $N_q(r)$ , where  $N_q(r) = (1/r) \sum_{d|r} \mu(d) q^{r/d}$  is the number of monic irreducibles of degree  $r$  over  $F_q$ , see [6].

If  $M_2(n)$  denotes the number of irreducibles over  $F_2$  of degree at most  $n$ , then  $M_2(n)$  can be written as the double sum

$$M_2(n) = \sum_{m=1}^n \frac{1}{m} \sum_{d|m} \mu(d) 2^{m/d}.$$

The asymptotic number of irreducibles in the set  $S_k$ , after sieving, is given by  $M_2(n)$  where  $n$  is the largest degree of any polynomial in  $S_k$ .

Starting with  $n = 1$ , the first few values of  $M_2(n)$  are given by 2, 3, 5, 8, 14, 23, 41, 71,  $\dots$ . A simplified formula or recurrence for  $M_2(n)$  would be of interest. A related question is to determine  $P_i(x)$ , the  $i$ -th irreducible over  $F_2$ , subject to the ordering from Section 1.

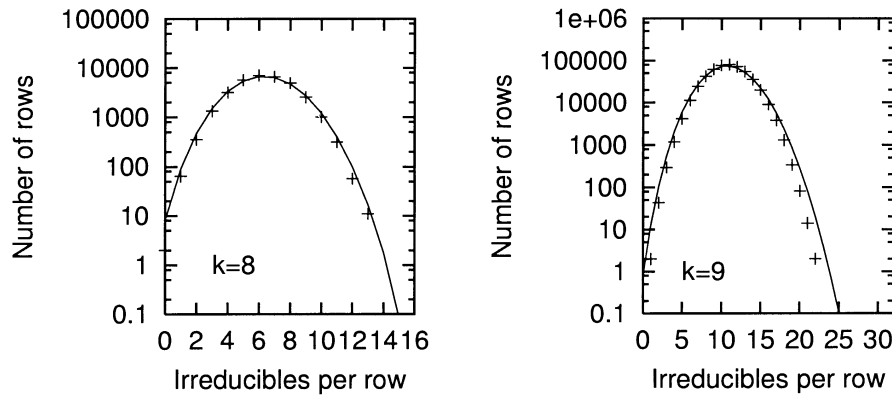
We are interested in studying heuristics of  $\pi(r; H, A)$  and in particular in comparing the error term with the distribution obtained for the polynomial arithmetic progressions of the wheel sieve, where  $H = M_k(x)$  and  $A$  is taken from the set  $S_{k-1}$ .

#### 3.1 Heuristics of the Distribution of Irreducibles in $S_k$

A computer program was written for  $q = 2$  that calculates the elements of the set  $S_k$  ordered as in the example for  $\mathbf{W}_4$ . We chose  $q = 2$  because the polynomials can be represented by a string of zeros and ones, as shown for  $\mathbf{W}_4$ . Each polynomial in  $S_k$  was tested for irreducibility using simple bit manipulations such as bit shifts and XOR (exclusive or) operations on the binary string representing the polynomial. The computer output was checked extensively against published tables of irreducible polynomials [6].

The results are given in Table 1 and Figure 1. The numbers given are the distribution of irreducible polynomials found in each “row” of the polynomial arithmetic progressions given in Definition 1. In Example 1, the rows corresponding to the arithmetic progressions are seen clearly for  $\mathbf{W}_4$ . The

number of irreducibles in each row is easily counted for  $k = 4$ : in Example 1,  $S_4$  has one row has 6 irreducibles and two rows have 7 irreducibles. Similarly, for  $k = 5$ , there are 11 rows having 6 irreducibles each (see Table 1).



**Fig. 1.** The count of rows with the given number of irreducible polynomials in the matrix  $\mathbf{W}_k$  for given  $k$ . The curve is the prediction from Conjecture 1.

### 3.2 Computational Heuristics Compared to Estimates

The frequency distribution of irreducible polynomials per row in  $W_k$  is shown in Figure 1 for  $k = 8$  and  $k = 9$ . When shown in a semi-log plot, this distribution has a parabolic shape which is characteristic of a binomial distribution and so we make

**Definition 2.** A binomial distribution in the parameter  $p$  is given by the terms of the expansion  $(p + (1 - p))^n$ . The mean value of this distribution is  $\mu = np$  and the standard deviation is  $\sigma = \sqrt{np(1 - p)}$ .

The solid lines in Figure 1 are calculated using the values of  $p$  and  $n$  given in the conjecture below. The values of  $p$  and  $n$  give a mean value  $\mu$  for the binomial distribution that, for large  $k$ , approaches the asymptotic value in (1). The value of  $n$  is equal to the number of columns in the matrix representation of  $S_k$ . Note that the solid lines are calculated and *not* fit to the data. Based upon the data, it is natural to make

*Conjecture 1.* The irreducible polynomials in the progressions given in Definition 1 are distributed so as to asymptotically approach a binomial distribution in the parameter  $p = (\Phi_q(M_k(x)))^{-1}(q^r/r)$ , where  $q = 2$  and  $r$  is the degree of  $M_k(x)$ , and a value of  $n = 2^{\deg(P_i)} - 1$ , where  $P_i(x)$  is the  $i$ -th irreducible polynomial over  $F_2$ .

**Table 1.** Number of rows with  $N$  irreducible polynomials for a given value of  $k$ .

N	$k$				
	5	6	7	8	9
0	0	0	0	2	0
1	0	0	0	64	2
2	0	0	8	355	43
3	0	0	10	1326	294
4	1	0	69	3153	1185
5	5	1	164	5648	4141
6	11	0	353	7057	11166
7	4	15	522	6615	24189
8	0	32	468	4936	42129
9	0	24	347	2526	61697
10	0	39	193	1011	76230
11	0	32	60	314	80045
12	0	4	10	57	71195
13	0	0	1	11	54293
14	0	0	0	0	35215
15	0	0	0	0	19696
16	0	0	0	0	9039
17	0	0	0	0	3817
18	0	0	0	0	1310
19	0	0	0	0	341
20	0	0	0	0	82
21	0	0	0	0	14
22	0	0	0	0	2

Based on this conjecture, the error term in the distribution of irreducibles is easily computed, based on the standard deviation  $\sigma$  of the binomial distribution. The heuristics from the binomial distribution can be compared directly with the error term in (1). The error term given just below (1) has an unknown value of  $\nu$  whereas the binomial distribution has all parameters known. For a large number of trials, the binomial distribution may be approximated by a gaussian, with distribution as a function of row  $j$ ,

$$D(j) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(j-\mu)^2/2\sigma^2}$$

where  $\mu$  and  $\sigma$  are given in Definition 2. When  $D(j) = 1$  then the asymptotic estimate in Conjecture 1 is bounded. This occurs when  $j - \mu = \pm\sigma\sqrt{\log(2\pi\sigma^2)}$ . Now  $\mu$  is the location of the peak of the distribution, as given by (1), so the error term is asymptotically  $\mathcal{O}(\sigma\sqrt{\log\sigma^2})$ . Using the definition of  $\sigma$ , we see that the error term estimated from Conjecture 1 is  $\mathcal{O}(\sqrt{(q^r/r)\log(q^r/r)})$ . This estimate for the error term is consistent with the heuristics, as shown in Figure 1, but is dependent on Conjecture 1.

## 4 Distribution of Irreducibles by Weight

Let  $W(n, m)$  denote the number of binary irreducibles of degree  $n$  and weight  $m$ , i.e. with  $m$  nonzero coefficients. While we are unable to provide a formula, or even a conjecture, for  $W(n, m)$ , we now provide numerical evidence that the irreducibles of degree  $n$  and weight  $m$  are binomially distributed. We note that any irreducible must have constant term 1, and have odd weight, otherwise it is divisible by  $x$  or  $x + 1$ .

The data for  $W(n, m)$  are given in Table 2, for  $n$  up to 26, corresponding to the largest degree in cycle  $k = 9$  of the wheel sieve. The weights appear to be binomially distributed, in this case with binomial probability  $p = 1/2$ . Naively, this is what one might expect from the combinatorics if the weights are randomly chosen. More formally, we make

*Conjecture 2.* The irreducible polynomials of degree  $n$  over  $F_2$  are binomially distributed by weight.

From the data in Table 2, it seems that for fixed  $m$ ,  $W(n, m)$  is an increasing function of  $n$ , except for  $m = 3$  and  $m = 5$ . An interesting question to ask is whether  $W(n, 3) > 0$ , for “almost all”  $n$  when  $n$  is large. If one makes a conjecture that the weights follow a binomial distribution, then the weight for the trinomials is easily calculated for monic polynomials over  $F_2$  and a binomial probability  $p = 1/2$  as,

$$2 \left( \frac{1}{2} \right)^{n-3} \binom{2^n}{n} = \frac{16}{n}, \quad (2)$$

which decreases asymptotically to zero. This would imply that the probability of monic trinomials vanishes as one considers all irreducibles of large degree. Note that (2) does not rule out irreducible trinomials of large degree, but says that the probability of finding one would be vanishingly small for large  $n$  if the binomial distribution is an accurate representation of the distribution.

It is difficult to say whether (2) is accurate, because the ends of the weight distribution have small numbers of counts for  $W(n, m)$  and thus the statistical errors become significant. For a purely random process with a large number of Bernoulli trials, the distribution follows a Gaussian distribution. Figure 2 shows the data for  $W(n, m)$  plotted along with a Gaussian distribution. The amplitude for the gaussian is calculated from  $N_2(n)$ , the exact number of irreducibles of degree  $n$  over  $F_2$ . The peak of the gaussian is calculated from  $(n + 3)/2$  for given degree  $n$ . The standard deviation of the distribution is given by  $\sqrt{(n - 3)pq}$  where  $p = q = 0.5$  for an equal probability Bernoulli trial. In other words, there are no free parameters in the Gaussian curve. The agreement between the data for  $W(n, m)$  and the Gaussian curve is remarkably good. However, without better heuristics, it is difficult to answer whether  $W(n, 3) > 0$  with finite probability for infinitely many values of  $n$ .

From [1] we know that  $W(2n, 3) > 0$  for infinitely many  $n$ . We now raise

**Table 2.** Weight distribution for irreducible polynomials  $W(n, m)$  where  $n$  is the degree and  $m$  is the number of non-zero coefficients.

n	m											
	3	5	7	9	11	13	15	17	19	21	23	25
2	1	0	0	0	0	0	0	0	0	0	0	0
3	2	0	0	0	0	0	0	0	0	0	0	0
4	2	1	0	0	0	0	0	0	0	0	0	0
5	2	4	0	0	0	0	0	0	0	0	0	0
6	3	6	0	0	0	0	0	0	0	0	0	0
7	4	10	4	0	0	0	0	0	0	0	0	0
8	0	17	13	0	0	0	0	0	0	0	0	0
9	4	22	28	2	0	0	0	0	0	0	0	0
10	2	38	44	14	1	0	0	0	0	0	0	0
11	2	46	84	52	2	0	0	0	0	0	0	0
12	4	54	152	110	14	1	0	0	0	0	0	0
13	0	66	236	264	60	4	0	0	0	0	0	0
14	2	73	357	500	214	15	0	0	0	0	0	0
15	6	98	546	898	546	82	6	0	0	0	0	0
16	0	94	734	1587	1304	337	24	0	0	0	0	0
17	6	152	1050	2674	2696	1006	122	4	0	0	0	0
18	5	124	1374	4316	5406	2745	531	30	1	0	0	0
19	0	158	1774	6696	10238	6766	1772	190	0	0	0	0
20	4	199	2325	9995	18405	15227	5368	815	39	0	0	0
21	4	184	2892	14988	31848	32144	14698	2888	212	0	0	0
22	2	226	3650	20993	53602	64163	36877	9928	1078	38	0	0
23	4	296	4660	29458	86626	122502	86528	29748	4606	286	8	0
24	0	202	5191	40861	136378	225569	190357	81708	17063	1509	32	0
25	4	406	6938	55202	208988	399576	399560	208542	55752	6880	324	4
26	0	328	8012	74404	314185	685607	799042	503547	166341	27390	1899	40

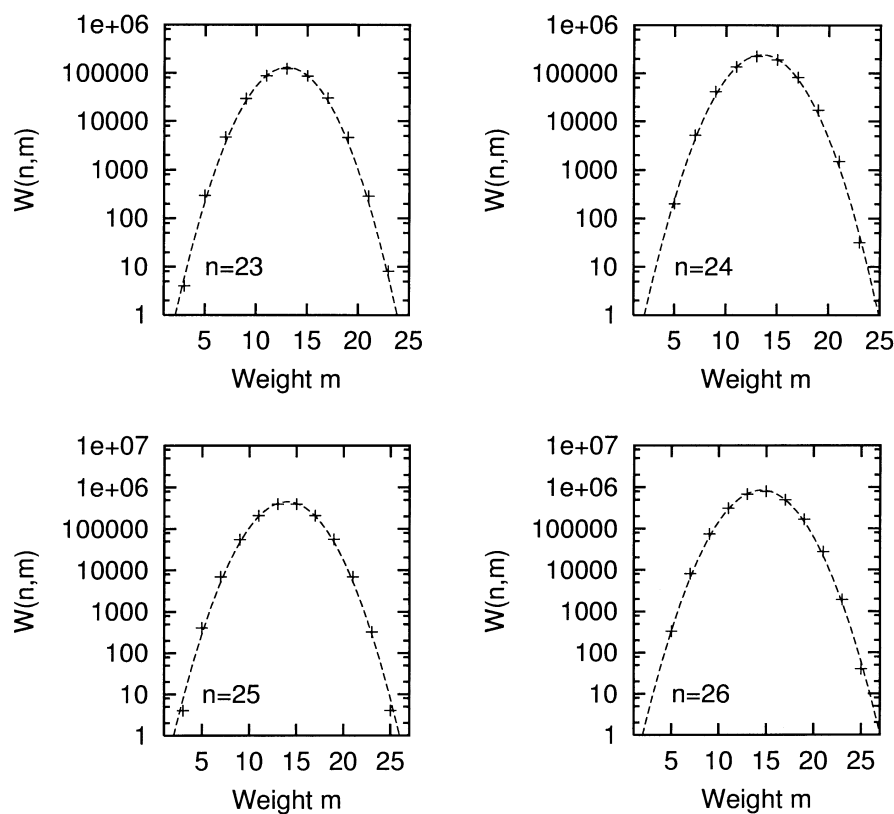
*Conjecture 3.* For fixed odd  $m \geq 3$ , there are infinitely many values of  $n \geq m - 1$  so that  $W(n, m) > 0$ .

## 5 Distribution of Self-reciprocal Irreducibles

If  $f(x)$  is a polynomial of degree  $n$ , then the *reciprocal* polynomial  $f^*(x)$  is defined by  $f^*(x) = x^n f(1/x)$ , and  $f(x)$  is said to be *self-reciprocal* if  $f(x) = f^*(x)$ . Self-reciprocal irreducibles of degree  $> 1$  must have even degree say  $2n$ , and it is easy to see that if  $f(x)$  is irreducible, so is  $f^*(x)$ . We refer to [4] section 2.7 for a discussion of self-reciprocal irreducibles, including a formula, see page 77, for the number  $si(n, 2)$  of self-reciprocal irreducibles of degree  $2n$  over  $F_2$ .

Let  $si(n, m, 2)$  be the number of self-reciprocal irreducibles of degree  $2n$  and weight  $m$  over  $F_2$ . The distribution of weights for self-reciprocal irreducibles of degree  $2n \leq 26$  is given in Table 3.





**Fig. 2.** The count of irreducible polynomials of degree  $n$  with a given weight  $m$ . The curve is the prediction from Conjecture 2.

**Table 3.** Distribution of weights for self-reciprocal irreducibles of degree  $2n$  with  $m$  non-zero coefficients.

$2n$	$m$											
	3	5	7	9	11	13	15	17	19	21	23	25
2	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0
6	1	0	0	0	0	0	0	0	0	0	0	0
8	0	1	1	0	0	0	0	0	0	0	0	0
10	0	2	0	0	1	0	0	0	0	0	0	0
12	0	0	2	2	0	1	0	0	0	0	0	0
14	0	1	3	2	2	1	0	0	0	0	0	0
16	0	2	2	3	4	5	0	0	0	0	0	0
18	1	0	2	6	8	7	3	0	1	0	0	0
20	0	3	1	11	11	11	10	3	1	0	0	0
22	0	0	4	15	20	19	17	10	8	0	0	0
24	0	0	7	17	22	37	41	24	15	5	2	0
26	0	2	2	14	39	77	62	63	35	16	5	0

We note from Table 3 for  $n \leq 13$  that  $si(n, 2)$  is a 0-1 linear combination of the values  $si(m, 2)$  for  $m < n$ . We ask whether this holds for all  $n \geq 1$ ?

It is already known [1] that  $si(n, 3, 2) > 0$  for infinitely many values of  $n$ , and we raise the following:

*Conjecture 4.* For fixed odd  $m \geq 3$  there are infinitely many values of  $2n > m$  such that  $si(n, m, 2) > 0$ .

From [1] the self-reciprocal polynomials of degree  $2n$  for which  $si(n, 3, 2) > 0$  are explicitly given in the form  $x^{2n} + x^n + 1$ , where  $n$  is any non-negative power of 3. It would be of interest to have an analogous explicit form for self-reciprocal irreducibles of degree  $2n$  and weight 5, and more generally of degree  $2n$  and weight  $m$ ; however this seems to be out of reach at the present.

## References

1. I.F. BLAKE, S. GAO, R.J. LAMBERT, *Construction and distribution problems for irreducible trinomials over finite fields*, Applications of Finite Fields, Edited by D. Gollmann, Clarendon Press, Oxford, 1996, 19-32.
2. D.R. HAYES, *The distribution of irreducibles in  $GF[q, x]$* , Trans. Amer. Math. Soc. 117(1965), 101-127.
3. K.H. HICKS AND I. SATO, *Heuristics of arithmetic progressions in the framework of the wheel sieve*, submitted for publication.
4. D. JUNGnickEL, *Finite Fields: Structure and Arithmetics*, Bibliographisches Inst. & F.A. Brockhaus AG, Mannheim, 1993.
5. H. KORNBLUM, *Über die Primfunktionen in einer arithmetischen Progression*, Math. Z. 5(1919), 100-111.
6. R. LIDL AND H. NIEDERREITER, Finite Fields, Cambridge Univ. Press, 1997.
7. P. PRITCHARD, *Explaining the wheel sieve*, Acta Informat. 17(1982), 477-485.

Finite Fields with Applications to Coding Theory,  
Cryptography and Related Areas  
Proceedings of the Sixth International Conference on  
Finite Fields and Applications, held at Oaxaca, México,  
May 21–25, 2001  
Mullen, G.L.; Stichtenoth, H.; Tapia-Recillas, H. (Eds.)  
2002, IX, 335 p., Hardcover  
ISBN: 978-3-540-43961-5