Construction and Distribution Problems for
Irreducible Trinomials over Finite Fields [1]

by
Ian F. Blake, Shuhong Gao and Robert J. Lambert [2]

Abstract

Various aspects of the construction, distribution and factorization of polynomials over a finite field have been widely investigated in the recent literature. The present work is limited to studying certain questions on the distribution of irreducible trinomials over F_2. All such irreducible trinomials of degree less than 5,000 have been determined as a basis of the study. The results indicate some distribution anomalies that are not well explained by existing theory. Primitive trinomials are of particular interest in the generation of random numbers for simulation studies, but they do not always exist for a given degree n over F_2. We explore the existence of trinomials that have degrees slightly bigger than the given degree and contain a primitive polynomial of the given degree as a factor. Such trinomials may be used as an alternative for primitive trinomials.

[1] This work was supported by a grant from the Information Technology Research Centre, a Centre of Excellence of the Province of Ontario

[2] Ian F. Blake and Robert J. Lambert are with the Department of Electrical and Computer Engineering of the University of Waterloo. Shuhong Gao is with the Department of Computer Science of the University of Toronto

1. Introduction.

The subject of irreducible polynomials over a finite field has been of considerable interest in the recent literature with numerous construction techniques, as well as irreducibility testing and factorization techniques, devised. This work examines certain questions of irreducible trinomials (polynomials with three nonzero coefficients) over the finite field with two elements, F_2. Such polynomials are of interest and use in a variety of coding and cryptographic applications.

The question of interest in this work concerns the frequency with which irreducible trinomials arise and their distribution as a function of degree. The study is largely experimental and uses the set of all irreducible trinomials of degrees up to $5,000$ over F_2 prepared for this purpose. While no definitive results on the distribution questions raised are obtained, some interesting observations are made which might be amenable to mathematical analysis.

The next section discusses some general absolute, composition and recursive type of constructions for irreducible polynomials that have appeared in the literature. Results more specifically related to irreducible trinomials are considered in section 3. The experimental results are discussed from a distribution perspective with some interesting questions raised.

Primitive trinomials are of particular interest in the generation of random numbers for simulation studies. However, they do not always exist for a given degree n over F_2. There may be some advantage to use a trinomial which has degree slightly bigger than n and has a primitive polynomial of degree n as a factor. In section 4, we explore the existence of such trinomials. In particular, we describe a class of trinomials that arise in designing efficient parallel algorithms. We also present some computational results of the existence of these trinomials.

2. Composition and recursive constructions for irreducible polynomials.

The authors recently ([1],[3]) studied some constructive problems associated with irreducible trinomials over F_2. A variety of absolute, composition and recursive construction techniques for irreducible polynomials were considered there. A few of these are recalled here, not so much that they directly involve the construction of irreducible trinomials but that they indicate techniques that might be pursued for this problem. The selection of techniques reported on here is by no means exhaustive. The book [1] is used as a convenient reference for the constructions and the reader is referred to there for the original references.

As an example of an absolute construction, consider the following for irreducible binomials.

Theorem 1. ([1], p.40) Let $a \in F_q^*$ be an element of order e. Then the binomial $x^t - a$ is irreducible in $F_q[x]$ if and only if the integer t satisfies the following conditions:

(i) gcd $(t, (q-1)/e) = 1$,
(ii) each prime factor of t divides e, and
(iii) if $4|t$ then $4|(q-1)$.

The following corollary to this theorem is of interest.

Corollary. ([1], p.40) Let r be a prime factor of $q-1$ and $a \in F_q$ have order e such that r does not divide $(q-1)/e$. Assume that $q \equiv 1 \bmod 4$ if $r = 2$. Then for any integer $k \geq 0$,

$$x^{r^k} - a$$

is irreducible over F_q.

The construction is interesting in that an infinite family of irreducible binomials is constructed over a fixed field, from some initial conditions.

The following gives a simple result on an absolute construction of an irreducible trinomial.

Theorem 2. ([1], p. 42) The trinomial $x^p - x - b,\ b \in F_q$ where q is a prime power p^m, is irreducible over F_q if and only if $Tr_{q|p}(b) \neq 0$, where $Tr_{q|p}(.)$ is the trace function of F_q over F_p.

Many of the absolute constructions for irreducible polynomials are for polynomials over $F_q,\ q > 2$ which limit their interest for the present study, although the previous Corollary was of particular interest.

As an example of a recursive construction consider the following due to Varshamov. Denote by $I_{n,q}[x]$ the set of irreducible polynomials of degree n over F_q.

Theorem 3. ([1], pp. 51-53) Let $q = 2^m$ and $f(x) = \sum_{i=0}^{n} c_i x^i \in I_{n,q}[x]$. Suppose $Tr_{q|2}(c_{n-1}/c_n) \neq 0$ and define the polynomials

$$a_0(x) = x, \quad b_0(x) = 1$$

$$a_{k+1}(x) = a_k(x) b_k(x)$$

$$b_{k+1}(x) = a_k^2(x) + b_k^2(x)$$

for $k \geq 0$. Then

$$f_k(x) = (b_k(x))^n f(a_k(x)/b_k(x))$$

is irreducible over F_q of degree $n2^k$ for all $k \geq 0$.

Direct consequences of this theorem include the fact that for any integer $k \geq 0,\ a_k(x) + b_k(x)$ is irreducible over F_2 of degree 2^k, a somewhat surprising result. Also if $q = 2$ and the $f(x)$ of the theorem is monic with $c_1 c_{n-1} \neq 0$ then the polynomial

$$\sum_{i=0}^{n} c_i a_k^i(x) b_k^{n-i}(x) \in I_{n2^k,2}[x]$$

for all $k \geq 0$.

A number of interesting recursive type of constructions appear in the literature. However, they tend not to lead to irreducible trinomials and their interest for this work is limited.

More important for the present study are composition constructions and perhaps the most important here is the following one due to Cohen.

Theorem 4. ([1], p. 44) Let $f(x),\ g(x) \in F_q[x]$ and $P(x) = \sum_{i=0}^{n} c_i x^i \in I_{n,q}[x]$. Then

$$P(f/g) = g^n(x) P(f(x)/g(x)) = \sum_{i=0}^{n} c_i f^i(x) g^{n-i}(x)$$

is reducible over F_q iff $f(x) - \lambda g(x)$ is irreducible over F_{q^n} for some zero $\lambda \in F_{q^n}$ of $P(x)$.

It might appear that the construction is difficult to apply as one has to go to the extension field F_{q^n}, however, in many cases this is not a problem. For example, it can be shown that if $q = 2^n,\ P(x) = \sum_0^n c_i x^i \in I_{n,q}[x]$ then

$$x^n P(x + x^{-1}) \in I_{2n,q}[x] \ \text{ iff } \ Tr_{q|2}(c_1/c_0) \neq 0$$

Additionally, if $P(x) \in I_{n,q}[x]$ then for $a,b,c,d \in F_q$ such that $ad-bc \neq 0$ then $(cx+d)^n P((ax+b)/(cx+d)) \in I_{n,q}[x]$.

Of more direct relevance to this study is the conclusion from the previous theorem that for $t \in Z_+$, $P(x) \in I_{n,q}[x]$ of exponent e then

$$P(x^t) \in I_{nt,q}[x] \quad \text{iff} \quad \begin{array}{ll} i) & \gcd(t, \frac{q^n-1}{e}) = 1, \\ ii) & p \text{ prime, } p|t \text{ implies } p|e, \text{ and} \\ iii) & 4|t \text{ implies } 4|(q^n-1). \end{array}$$

Denote by $T_{n,k}(x)$ the trinomial $x^n + x^k + 1$. The above construction is of particular interest here since if $P(x)$ is an irreducible trinomial, then under the above circumstances $P(x^t)$ will be also. It can shown from the above that if $P(x) \in I_{n,q}[x]$ with exponent e such that if r is a prime factor of e such that r does not divide $(q^n-1)/e$ and if we assume that $q^n \equiv 1 \bmod 4$ if $r=2$, then $P(x^{r^k})$ is irreducible over F_q for every $k \geq 1$. Again, if $P(x)$ is an irreducible trinomial, then under the above conditions, an infinite family of irreducible trinomials is constructed.

An interesting direct consequence of this is that, since x^2+x+1 has exponent 3 then $x^{2t}+x^t+1$ is irreducible over F_2 if and only if t is a power of 3. Since every self-reciprocal ($f(x) = x^n f(x^{-1})$ where f is of degree n) trinomial is of the form $x^{2t}+x^t+1$, we see that all irreducible self-reciprocal trinomials over F_2 are of the form $x^{2\cdot 3^k} + x^{3^k} + 1$.

3. Distribution problems for irreducible trinomials.

A surprising amount of information has been collected about irreducible trinomials in the literature. Some of this has been noted in [3]. Our concern in this section will be to consider certain questions on the distribution of irreducible trinomials with degree. To this end, all irreducible trinomials of degrees less than $5,000$, as well as those between $9,800$ and $10,000$, were determined.

Consider first the following argument. There are precisely $n-1$ trinomials of degree n. Approximately $1/n$th of all polynomials are irreducible. By making certain assumptions of independence, one might argue that on average, the expected number of irreducible trinomials of degree n is one. The argument seems not to be correct, even from an approximate point of view. Notice that if $T_{n,k}(x) \in I_{n,2}[x]$ then $T_{n,n-k}(x) \in I_{n,2}[x]$ also, which will skew the results. There are $3,021$ irreducible trinomials of degree less than $1,000$, including self reciprocal and reciprocal polynomials, giving an average of approximately 3 irreducible trinomials per degree. This ratio holds remarkably constant as the degrees become larger: there are $15,139$ irreducible trinomials of degree less than $5,000$. A sharper estimate for this average number of irreducible trinomials as a function of degree, by more detailed arguments, would be of interest. Perhaps noteworthy is the appearance that the number does not seem to change as the degree increases, based on the limited evidence observed. Mathematical evidence that this is the case would be of interest.

Perhaps the strongest theoretical result available for the determination of irreducible trinomials is Swan's theorem.

Theorem 5 ([6]). $T_{n,k}(x)$ has an even number of irreducible factors if and only if

(i) n is even, k is odd, $n \neq 2k$ and $nk/2 \equiv 0$ or $1 \bmod 4$,

(ii) n is odd, k is even not dividing $2n$ and $n \equiv \pm 3 \bmod 8$,

(iii) n is odd, k is even, $k|2n$ and $n \equiv \pm 1 \bmod 8$.

If n and k are both odd then the tests can be applied to $T_{n,n-k}(x)$.

This is a powerful result with many interesting consequences. If the theorem is in fact a "strong" result, then the distribution of trinomials has a strong dependence on the degree modulo 8. For example, by part (i) of the theorem, there can be no irreducible trinomial of degree n over F_2 if $n \equiv 0 \mod 8$. By a simple argument it can be seen that $T_{n,1}(x)$ and $T_{n,2}(x)$ cannot both be irreducible simultaneously when $n > 3$. Also, it can be concluded that to find all irreducible trinomials of degree $n \equiv \pm 3 \mod 8$ it is sufficient to check if $T_{n,2d}(x)$ is irreducible for each divisor d of n such that $n/d \equiv \pm 3 \mod 8$.

In [3], a table of all integers $\leq 30,000$ such that $T_{n,1}(x)$ is irreducible over F_2 is reproduced. Also a table of all integers $\leq 60,000$ such that $T_{n,2}(x)$ is irreducible is given. This table leads to the conjecture, supported by the data for degrees up to $5,000$ that, for $n > 21$, if $T_{n,2}(x)$ is irreducible over F_2 then $T_{n,k}(x)$ is reducible for all $k \neq 2,\ n-2$.

Recall that primes of the form $2^p - 1$ are referred to as Mersenne primes and p a Mersenne exponent. The irreducibility over F_2 of $T_{p,k}(x)$ where p is a Mersenne exponent up to $216,091$ has been determined [3].

To examine the distribution of irreducible trinomials over F_2, Swan's theorem suggests consideration of these modulo 8. It has been noted that none can exist of degree $n \equiv 0$ modulo 8. Table 1 shows the number of values of n modulo 8, in the range indicated for which there is at least one irreducible trinomial over F_2. The relative abundance of such integers when $n \equiv \pm 1 \mod 8$ is of interest, as is the relative scarcity of them for $n \equiv \pm 3 \mod 8$. As well, the numbers seem relatively constant as n increases. The row for the range of degrees, $9,800 - 10,000$ was added to see if there was any effect noticeable at that range. The sparse data added seems consistent with that for lower degrees, although no conclusion is possible.

Range	1	2	3	4	5	6	7	Total
1–200	24	19	6	22	4	20	24	119
201–400	24	20	0	24	2	15	23	108
401–600	25	14	0	22	0	20	23	104
601–800	24	20	1	21	0	18	24	108
801–1000	24	17	1	22	2	16	24	106
1001–1200	23	18	0	19	2	19	24	105
1201–1400	25	15	0	22	0	19	24	105
1401–1600	25	16	0	23	0	19	24	107
1601–1800	24	13	0	21	0	14	24	96
1801–2000	24	11	0	18	0	19	25	97
2001–2200	25	17	0	19	0	17	24	102
2201–2400	25	15	1	23	0	15	24	103
2401–2600	24	14	0	21	1	16	22	98
2601–2800	23	17	1	21	0	13	25	100
2801–3000	25	16	0	21	0	13	24	99
3001–3200	25	13	0	25	0	16	23	102
3201–3400	23	12	0	21	0	19	24	99
3401–3600	23	13	0	23	0	16	24	99
3601–3800	25	16	0	21	0	16	24	102
3801–4000	25	15	0	21	0	16	24	101
4001–4200	23	17	0	21	1	18	25	105
4201–4400	22	18	0	22	0	18	25	105
4401–4600	23	19	0	22	2	17	23	106
4601–4800	24	15	0	23	0	14	24	100
4801–5000	24	14	0	19	1	19	24	101
9801–10,000	23	13	0	21	0	16	23	96

Table 1. The number of values of n in the range indicated for which there exists at least one irreducible trinomial over F_2.

Table 2 gives the total number of irreducible of degrees in the range shown, where $k \leq n/2$. Again, while the entries exhibit somewhat random behaviour, there is no discernible pattern of increase or decrease with degree.

Range	1	2	3	4	5	6	7	Total
1–200	73	27	7	73	5	30	82	297
201–400	92	36	0	74	2	25	76	305
401–600	85	26	0	71	0	35	71	288
601–800	87	30	1	73	0	34	94	319
801–1000	81	31	1	77	2	29	83	304
1001–1200	87	28	0	67	3	36	84	305
1201–1400	79	29	0	74	0	29	86	297
1401–1600	92	29	0	75	0	41	98	335
1601–1800	93	22	0	66	0	26	71	278
1801–2000	82	21	0	58	0	33	97	291
2001–2200	86	28	0	75	0	27	108	324
2201–2400	96	29	1	77	0	23	83	309
2401–2600	79	26	0	84	1	31	73	294
2601–2800	87	27	1	85	0	23	104	327
2801–3000	69	29	0	59	0	16	83	256
3001–3200	99	23	0	74	0	29	85	310
3201–3400	79	29	0	77	0	37	88	310
3401–3600	83	28	0	74	0	32	84	301
3601–3800	92	23	0	86	0	28	91	320
3801–4000	88	25	0	75	0	29	90	307
4001–4200	82	32	0	57	1	37	73	282
4201–4400	75	34	0	72	0	35	96	312
4401–4600	89	36	0	66	2	34	85	312
4601–4800	101	32	0	84	0	20	71	308
4801–5000	75	25	0	67	1	30	84	282
9801–10,000	71	31	0	76	0	33	102	313

Table 2. The total number of irreducible trinomials $T_{n,k}(x)$ in the range indicated, $k \le n/2$.

To further emphasize the dependence of the quantities considered as a function of degree modulo 8, Table 3 summarizes the results.

n mod 8	Number
0	0
1	602
2	394
3	10
4	537
5	15
6	422
7	598
	2578

Table 3. The number of $n \leq 5,000$ modulo 8, such that there exists at least one irreducible trinomial of degree n.

4. Primitive trinomials and a related problem.

Primitive trinomials are of particular interest in the generation of random numbers for simulation studies. Recently, they are used in designing efficient parallel algorithms on hypercube computers by Aiello and Leighton [2] (see also [4]). However, primitive trinomials do not always exist for a given degree n over F_2. In such case, one may use a trinomial which contains a primitive polynomial of degree n as a factor, as demonstrated by Tromp, Zhang and Zhao [5] where they generalized Aiello and Leighton's construction.

In particular, Tromp, Zhang and Zhao ask the following question: Given an integer n, when are there integers m, k such that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1)$ is a primitive polynomial of degree n over F_2? (The gcd is computed over F_2.) They computed a list of (smallest) such m and k for n up to 171 and verified that the answer is yes for these n. They conjecture that the answer is always yes. Their conjecture may be formulated as follows.

Conjecture. For every primitive polynomial f of degree n over F_2, there are integers $1 \leq k < m < 2^n - 1$ such that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1) = f$.

We extend Tromp et al's computation for n up to 500. The results are listed in Table 4, where for each $n \leq 500$, we give the smallest integers $m > k$ such that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1)$ is a primitive polynomial of degree n over F_2. As a special case, Table 4 contains primitive trinomials over F_2. It is interesting to note that m is very close to n, and in fact is always less than $2n$ except for $n = 24$. This fact was observed by L. Zhang for $n \leq 171$. It is tempting to conjecture that there is a constant c such that for every integer n there are integers $k < m \leq cn$ such that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1)$ is a primitive polynomial of degree n over F_2.

In random number generation, one may only require that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1)$ contain a primitive factor of degree n over F_2. In such case, the smallest m should be much smaller. For comparison, we select the entries n, m, k in Table 4 such that m is big compared to n, say $m - n > 20$. For each of these n, we compute the smallest m' and k' such that $\gcd(x^{m'} + x^{k'} + 1, x^{2^n-1} + 1)$ contains a primitive factor of degree n over F_2. The results are tabulated in Table 5. We see from Table 5 that the gap, $m' - n$, is much smaller than $m - n$.

n	m	k	n	m	k	n	m	k	n	m	k	n	m	k
2	2	1	42	51	7	82	85	19	122	128	15	162	166	27
3	3	1	43	53	2	83	85	14	123	123	2	163	171	70
4	4	1	44	52	15	84	84	13	124	124	37	164	189	68
5	5	2	45	59	12	85	93	28	125	128	3	165	173	42
6	6	1	46	58	9	86	91	22	126	141	70	166	186	53
7	7	1	47	47	5	87	87	13	127	127	1	167	167	6
8	13	1	48	70	27	88	154	37	128	131	50	168	179	38
9	9	4	49	49	9	89	89	38	129	129	5	169	169	34
10	10	3	50	54	7	90	111	28	130	130	3	170	170	23
11	11	2	51	53	4	91	99	13	131	138	61	171	173	10
12	19	6	52	52	3	92	103	39	132	132	29	172	172	7
13	16	3	53	61	28	93	93	2	133	136	43	173	176	5
14	17	2	54	93	23	94	94	21	134	134	57	174	174	13
15	15	1	55	55	24	95	95	11	135	135	11	175	175	6
16	29	6	56	67	31	96	123	1	136	139	30	176	179	27
17	17	3	57	57	7	97	97	6	137	137	21	177	177	8
18	18	7	58	58	19	98	98	11	138	183	23	178	178	87
19	22	3	59	61	26	99	101	13	139	142	3	179	181	14
20	20	3	60	60	1	100	100	37	140	140	29	180	289	75
21	21	2	61	66	17	101	103	2	141	148	71	181	188	51
22	22	1	62	77	30	102	115	3	142	142	21	182	207	17
23	23	5	63	63	1	103	103	9	143	147	1	183	183	56
24	55	6	64	74	21	104	109	9	144	159	14	184	187	67
25	25	3	65	65	18	105	105	16	145	145	52	185	185	24
26	29	12	66	83	20	106	106	15	146	149	6	186	191	2
27	29	1	67	76	29	107	109	8	147	149	19	187	194	45
28	28	3	68	68	9	108	108	31	148	148	27	188	199	12
29	29	2	69	75	23	109	118	21	149	151	2	189	197	20
30	41	12	70	82	15	110	117	19	150	150	53	190	194	33
31	31	3	71	71	6	111	111	10	151	151	3	191	191	9
32	59	29	72	93	7	112	133	1	152	155	38	192	213	101
33	33	13	73	73	25	113	113	9	153	153	1	193	193	15
34	37	6	74	80	39	114	118	7	154	157	22	194	194	87
35	35	2	75	77	4	115	125	6	155	158	75	195	197	25
36	36	11	76	88	43	116	136	1	156	188	59	196	209	42
37	43	4	77	80	9	117	123	31	157	164	25	197	200	69
38	42	1	78	89	2	118	118	33	158	167	54	198	198	65
39	39	4	79	79	9	119	119	8	159	159	31	199	199	34
40	43	3	80	83	23	120	174	31	160	177	19	200	221	35
41	41	3	81	81	4	121	121	18	161	161	18	201	201	14

n	m	k	n	m	k	n	m	k	n	m	k	n	m	k
202	202	55	242	249	62	282	282	35	322	322	67	362	362	63
203	216	89	243	245	52	283	286	51	323	325	41	363	365	169
204	213	7	244	253	78	284	284	119	324	337	72	364	364	67
205	211	39	245	247	2	285	291	122	325	328	151	365	368	89
206	220	67	246	253	9	286	286	69	326	331	25	366	366	29
207	207	43	247	247	82	287	287	71	327	327	34	367	367	21
208	219	95	248	253	100	288	369	173	328	331	52	368	378	173
209	209	6	249	249	86	289	289	21	329	329	50	369	369	91
210	259	31	250	250	103	290	293	114	330	351	70	370	370	139
211	214	103	251	253	74	291	293	133	331	344	69	371	373	56
212	212	105	252	252	67	292	292	97	332	332	123	372	385	61
213	219	4	253	258	97	293	295	2	333	333	2	373	376	85
214	219	86	254	268	121	294	294	61	334	339	115	374	396	167
215	215	23	255	255	52	295	295	48	335	341	20	375	375	16
216	245	27	256	282	115	296	301	15	336	380	159	376	381	157
217	217	45	257	257	12	297	297	5	337	337	55	377	377	41
218	218	11	258	258	83	298	313	48	338	341	32	378	378	43
219	221	1	259	264	103	299	301	5	339	341	13	379	382	187
220	254	35	260	316	37	300	300	7	340	349	75	380	380	47
221	236	77	261	266	17	301	307	78	341	351	124	381	389	99
222	227	6	262	266	89	302	302	41	342	342	125	382	382	81
223	223	33	263	263	93	303	307	28	343	343	75	383	383	90
224	229	30	264	295	42	304	307	46	344	347	153	384	397	184
225	225	32	265	265	42	305	305	102	345	345	22	385	385	6
226	229	99	266	266	47	306	320	131	346	349	72	386	386	83
227	229	77	267	269	88	307	312	119	347	349	173	387	392	59
228	238	43	268	268	25	308	319	103	348	403	165	388	400	141
229	232	61	269	274	47	309	319	113	349	355	177	389	394	193
230	243	13	270	270	53	310	317	120	350	350	53	390	390	89
231	231	26	271	271	58	311	319	139	351	351	34	391	391	28
232	235	69	272	275	101	312	453	56	352	355	78	392	395	71
233	233	74	273	273	23	313	313	79	353	353	69	393	393	7
234	234	31	274	274	67	314	314	15	354	358	127	394	394	135
235	249	7	275	278	99	315	317	127	355	366	173	395	406	187
236	236	5	276	329	102	316	316	135	356	371	38	396	396	25
237	259	67	277	283	12	317	320	113	357	365	32	397	402	13
238	243	28	278	278	5	318	325	81	358	365	132	398	407	203
239	239	36	279	279	5	319	319	36	359	359	68	399	399	86
240	269	14	280	323	3	320	431	213	360	379	141	400	459	89
241	241	70	281	281	93	321	321	31	361	369	64	401	401	152

n	m	k	n	m	k	n	m	k	n	m	k	n	m	k
402	410	149	422	422	149	442	461	177	462	462	73	482	485	108
403	408	127	423	423	25	443	453	68	463	463	93	483	488	59
404	404	189	424	446	155	444	519	203	464	469	142	484	484	105
405	419	42	425	425	12	445	457	66	465	465	59	485	492	181
406	406	157	426	435	46	446	446	105	466	472	19	486	491	90
407	407	71	427	432	5	447	447	73	467	469	29	487	487	94
408	421	133	428	428	105	448	451	78	468	488	147	488	491	180
409	409	87	429	435	146	449	449	134	469	477	109	489	489	83
410	414	107	430	444	55	450	450	79	470	470	149	490	490	219
411	419	174	431	431	120	451	458	139	471	471	1	491	493	224
412	412	147	432	457	186	452	463	108	472	493	235	492	550	171
413	416	9	433	433	33	453	464	5	473	475	17	493	496	37
414	469	64	434	445	102	454	472	235	474	474	191	494	494	137
415	415	102	435	437	61	455	455	38	475	485	21	495	495	76
416	422	15	436	436	165	456	473	185	476	476	15	496	506	81
417	417	107	437	443	12	457	457	16	477	485	149	497	497	78
418	421	40	438	438	65	458	458	203	478	478	121	498	519	11
419	421	176	439	439	49	459	461	202	479	479	104	499	515	137
420	451	45	440	443	146	460	460	61	480	491	197	500	515	246
421	429	14	441	441	31	461	464	27	481	481	138			

Table 4. List of smallest m and k for $n \leq 500$
such that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1)$ is primitive of degree n over F_2.

n	m	m'	k	k'	n	m	m'	k	k'
24	55	36	6	17	256	282	272	115	45
32	59	40	29	3	260	316	262	37	11
48	70	58	27	17	264	295	279	42	22
54	93	68	23	27	276	329	281	102	31
72	93	88	7	23	280	323	298	3	95
88	154	96	37	19	288	369	291	173	89
90	111	93	28	10	312	453	327	56	56
96	123	98	1	25	320	431	325	213	24
112	133	122	1	39	330	351	333	70	13
120	174	122	31	25	336	380	344	159	35
138	183	141	23	5	348	403	350	165	163
156	188	166	59	1	374	396	376	167	5
164	189	187	68	32	400	459	407	89	25
180	289	185	75	58	414	469	428	64	67
182	207	193	17	59	420	451	428	45	159
192	213	195	101	53	424	446	441	155	43
200	221	205	35	42	432	457	435	186	152
210	259	251	31	42	444	519	449	203	157
216	245	233	27	71	472	493	479	235	151
220	254	224	35	101	492	550	498	171	37
237	259	240	67	41	498	519	519	11	11
240	269	243	14	46					

Table 5. List of smallest m, k, m', and k' for $n \leq 500$
such that $\gcd(x^m + x^k + 1, x^{2^n-1} + 1)$ is primitive of degree n over F_2
and $\gcd(x^{m'} + x^{k'} + 1, x^{2^n-1} + 1)$ has a primitive factor of degree n over F_2.

In the remainder of this section, we prove that if the above conjecture is true for some primitive polynomial f then it is true for all primitive polynomials of the same degree.

Theorem 6. If the above conjecture is true for some primitive polynomial f then it is true for all primitive polynomials of the same degree.

Proof. Suppose that f is of degree n such that

$$\gcd(x^i + x^j + 1, x^{2^n-1} + 1) = f, \tag{1}$$

and α a root of f. Let g be any primitive polynomial of degree n over F_2 and β a root of it. Then $\beta = \alpha^u$ for some integer u with $\gcd(u, 2^n - 1) = 1$, as both α and β are primitive elements in F_{2^n}. Let v be an integer such that $uv \equiv 1 \mod 2^n - 1$. Then $\alpha = \beta^v$. We prove that

$$\gcd(x^{vi} + x^{vj} + 1, x^{2^n-1} + 1) = g. \tag{2}$$

First note that

$$\beta^{vi} + \beta^{vj} + 1 = \alpha^{uvi} + \alpha^{uvj} + 1 = \alpha^i + \alpha^j + 1 = 0,$$

that is, β is a root of $x^{vi}+x^{vj}+1$. We see that $g|(x^{vi}+x^{vj}+1)$. It suffices to prove that $(x^{vi}+x^{vj}+1)/g$ has no roots in F_{2^n}. We consider the roots of $x^{vi} + x^{vj} + 1$ and $x^i + x^j + 1$ in some extension field of F_2. Since $f = \prod_{k=0}^{n-1}(x - \alpha^{2^k})$, (1) implies that

$$x^i + x^j + 1 = \prod_{k=0}^{n-1}(x - \alpha^{2^k}) \prod_{\gamma}(x - \gamma)$$

where every γ in the second product is not in F_{2^n}. Hence

$$x^{vi} + x^{vj} + 1 = \prod_{k=0}^{n-1}(x^v - \alpha^{2^k}) \prod_{\gamma}(x^v - \gamma).$$

Obviously, every root of $x^v - \gamma$ is not in F_{2^n} when γ is not in F_{2^n}. The only roots of $x^{vi} + x^{vj} + 1$ that are in F_{2^n} come from $x^v - \alpha^{2^k}$, $0 \le k \le n-1$. Let η be a primitive v-th root of unity over F_2. Then

$$x^v - \alpha^{2^k} = x^v - \beta^{v2^k} = \prod_{\ell=0}^{v-1}(x - \beta^{2^k}\eta^\ell).$$

Since $\gcd(v, 2^n - 1) = 1$, $\eta^\ell \in F_{2^n}$ iff $v|\ell$. This means that $\beta^{2^k}\eta^\ell \notin F_{2^n}$ for $1 \le \ell \le v-1$. Hence $x^v - \alpha^{2^k}$ has only one root, i.e. β^{2^k} in F_{2^n} for $1 \le k \le n-1$. As $g = \prod_{k=0}^{n-1}(x - \beta^{2^k})$, we see that $(x^{vi} + x^{vj} + 1)/g$ has no roots in F_{2^n} and thus (2) holds. This completes the proof.

5. Comments.

The distribution of irreducible trinomials as a function of degree might initially be modeled as random. The results of Section 3 indicate a stronger number theoretic influence on this distribution than might be suspected. The random point of view, as noted, might suggest an average of one irreducible trinomial per degree, but the limited experimental evidence suggests an average of at least three. For at least half of the degrees less than 5000, at least one irreducible trinomial exists with a total number (including reciprocals and self reciprocals) of more than 15,000. Thus the greater prevalence of these polynomials than expected appears to persist for higher degrees.

The distribution of the irreducible trinomials with degree n, when n is regarded modulo 8, as suggested by Swan's theorem, was particularly revealing. The results indicate some strong number theoretic considerations underlying the distribution, as opposed to a purely random phenomena. In particular, the relative paucity of polynomials for $n \equiv \pm 3 \bmod 8$ might be a question of interest for further analytical consideration. By contrast, irreducible trinomials of degrees $n \equiv \pm 1$ modulo 8, nearly always exist. Additionally it might be of interest to consider whether Swan's theorem might be strengthened in any way and if the distribution, say, modulo 16, might be further revealing.

The conjectures noted in the section 3 seem reasonable from the experimental evidence available. It would be of comfort to have theoretical confirmation for them.

Primitive trinomials over F_2 are desirable in applications, but they dot not always exist. It may be suitable to use trinomials that have degree slightly bigger than the desired degree and contain a primitive factor of the desired degree over F_2. Our computation shows that such trinomials always exist. Again, it would be of interest to have a mathematical explanation of these phenomena.

Acknowledgement. The authors would like to thank L. Zhang for his useful comments and for sharing some of his ideas with us.

References

[1] *Applications of Finite Fields*, A.J. Menezes ed., Boston: Kluwer Academic Publishers, 1993.

[2] W. Aiello and T. Leighton. Coding theory, hypercube embeddings, and fault tolerance, in *Proc. of the 3rd Annual ACM Symposium on Parallel Algorithms and Architectures*, pp. 125–136, 1991.

[3] I.F. Blake, S. Gao and R.J. Lambert. Constructive problems for irreducible polynomials over finite fields, in Lecture Notes in Computer Science, vol. 793, Springer-Verlag, A. Gulliver and N. Secord editors, pp. 1-23, 1994.

[4] T. Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays · Trees · Hypercubes*, Morgan Kaufmann, San Matec, California, 1992.

[5] J. Tromp, L. Zhang and Y. Zhao. Small weight bases for Hamming codes, 1994. Preprint.

[6] R.G. Swan. Factorization of polynomials over finite fields, *Pac. J. Math.*, **12** (1962) pp. 1099-1106.