On the Number of Trace-One Elements in Polynomial Bases for $\mathbb{F}_{2^n}$

Omran Ahmadi and Alfred Menezes

Department of Combinatorics & Optimization
University of Waterloo, Canada
{oahmadid,ajmeneze}@uwaterloo.ca

May 13, 2004; updated on July 14, 2004

Abstract. This paper investigates the number of trace-one elements in a polynomial basis for $\mathbb{F}_{2^n}$. A polynomial basis with a small number of trace-one elements is desirable because it results in an efficient and low-cost implementation of the trace function. We focus on the case where the reduction polynomial is a trinomial or a pentanomial, in which case field multiplication can also be efficiently implemented.

1 Introduction

Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_2$. Then $\mathbb{F}_2[x]/(f)$ is a finite field of order 2^n, denoted $\mathbb{F}_{2^n}$, and $f(x)$ is called the *reduction polynomial* for this representation of $\mathbb{F}_{2^n}$. The element $\alpha = x$ is a root of f in $\mathbb{F}_{2^n}$, and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, called a *polynomial basis*. Multiplication of field elements represented with respect to a polynomial basis is faster if the reduction polynomial has a small number of non-zero coefficients (e.g., see Section 2.3.5 of [9]). If $f(x)$ has only three non-zero coefficients then $f(x)$ is called a *trinomial* and the corresponding polynomial basis is called a *trinomial basis*. Similarly, if $f(x)$ has only five non-zero coefficients then $f(x)$ is called a *pentanomial* and the corresponding polynomial basis is called a *pentanomial basis*. Trinomial and pentanomial bases are frequently used in elliptic curve cryptographic systems (e.g., see [1, 2, 5]).

Suppose now that $a \in \mathbb{F}_{2^n}$ has polynomial basis representation $a = \sum_{j=0}^{n-1} a_j \alpha^j$, where each $a_j \in \mathbb{F}_2$. The *trace* of a is

$$\begin{aligned}\mathrm{Tr}(a) &= \sum_{i=0}^{n-1} a^{2^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} a_j \alpha^j \right)^{2^i} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_j (\alpha^j)^{2^i} \\ &= \sum_{j=0}^{n-1} a_j \sum_{i=0}^{n-1} (\alpha^j)^{2^i} = \sum_{j=0}^{n-1} a_j \,\mathrm{Tr}(\alpha^j).\end{aligned}$$

Thus, $\mathrm{Tr}(a)$ can be computed by adding modulo 2 those coefficients a_j for which $\mathrm{Tr}(\alpha^j) = 1$. This operation is faster in software if the number of basis elements

α^j for which $\mathrm{Tr}(\alpha^j) = 1$ is small. Also, the circuit to implement this operation in hardware is simpler if the number of trace-one basis elements is small. For example, if $\mathrm{Tr}(\alpha^j) = 0$ for $1 \le j \le n-1$ and $\mathrm{Tr}(\alpha^0) = 1$, then $\mathrm{Tr}(a) = a_0$; in this case, the trace function is especially easy to evaluate. A fast and low-cost implementation of the trace operation is beneficial, for example, when halving a point on an elliptic curve over $\mathbb{F}_{2^n}$ (see [10, 13, 6]), or when generating pseudorandom sequences using elliptic curves [7] or the Welch-Gong transformation sequence generator [8]. Thus it is of interest to find irreducible trinomials and pentanomials whose corresponding bases have the smallest possible number of trace-one elements.

It is well known that every finite field $\mathbb{F}_{2^n}$ has a *normal basis* $N = \{\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{n-1}}\}$. The element α of such a basis must satisfy $\mathrm{Tr}(\alpha) = 1$ (since otherwise the elements of N are linearly dependent over $\mathbb{F}_2$), and hence all basis elements have trace one. Adding α to $n-k$ other basis elements yields a new basis for $\mathbb{F}_{2^n}$ in which exactly k elements have trace one. Hence, for each $k \in [1, n]$, there exists a basis for $\mathbb{F}_{2^n}$ in which exactly k elements have trace one. A natural question, which we will also pursue in this paper, is whether there exists a polynomial basis with this property.

The remainder of this paper is organized as follows. The traces of elements of trinomial and pentanomial bases are determined in §2. Some observations about the traces of elements of general polynomial bases are presented in §3. In §4, we generalize some of our results to finite fields of any characteristic. We draw our conclusions in §5.

2 Irreducible Trinomials and Pentanomials

We first determine the traces of the elements of a trinomial basis.

Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ be an irreducible polynomial of degree n over $\mathbb{F}_2$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$. Then it is well known that the roots of $f(x)$ in $\mathbb{F}_{2^n}$ are precisely $x_i = \alpha^{2^i}$ for $0 \le i \le n-1$. Now define

$$s_k = \mathrm{Tr}(\alpha^k) \quad \text{for} \quad 0 \le k \le n-1. \tag{1}$$

Then we have $f(x) = \prod_{i=0}^{n-1}(x - x_i)$ and $s_k = \sum_{i=0}^{n-1} x_i^k$. Thus the coefficients a_i are the elementary symmetric polynomials of x_i, and s_k are the power sums. By Newton's identity [11, Theorem 1.75],

$$s_k + s_{k-1}a_1 + s_{k-2}a_2 + \cdots + s_1 a_{k-1} + k a_k = 0 \tag{2}$$

for $1 \le k < n$.

Theorem 1 Let $f(x) = x^n + x^{n-m} + 1$ be an irreducible polynomial over $\mathbb{F}_2$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$. Then for $0 \le k \le n-1$ we have

$$\mathrm{Tr}(\alpha^k) = \begin{cases} n \bmod 2, & \text{if } k = 0, \\ 0, & \text{if } m \not| k, \\ m \bmod 2, & \text{otherwise.} \end{cases}$$

Proof. We apply (2) with $a_m = a_n = 1$ and $a_k = 0$ for $k \neq m, n$. We find $s_k = 0$ for $1 \leq k < m$ and $s_m + m = 0$; thus $s_m = (m \bmod 2)$. For $m + 1 \leq k < n$, (2) implies $s_k + s_{k-m} = 0$, and the result follows. □

The following result is an immediate consequence of Theorem 1.

Corollary 2 Let $f(x) = x^n + x^{n-m} + 1$ be an irreducible polynomial over $\mathbb{F}_2$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$.

(i) If m is even (and hence n is odd), then all elements of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ except for 1 have trace zero.
(ii) If m is odd, then exactly $\lfloor (n-1)/m \rfloor$ of the basis elements $\{\alpha, \ldots, \alpha^{n-1}\}$ have trace one.
(iii) If $m = 1$ and n is odd, then all elements of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ have trace one.

Notice that if $x^n + x^{n-m} + 1$ is irreducible over $\mathbb{F}_2$ then so is its reciprocal $x^n + x^m + 1$. If n is even then both m and $n - m$ must be odd. If we let $l = \max(m, n-m)$, then $l \geq \frac{n}{2}$ and we can conclude from Theorem 1 that exactly one element of the polynomial basis corresponding to $x^n + x^{n-l} + 1$ has trace one. If n is odd then one of m and $n - m$ must be even; let l be this number. Then by Corollary 2(i), exactly one element of the polynomial basis corresponding to $x^n + x^{n-l} + 1$ has trace one. This proves the following result.

Theorem 3 Suppose that there exists an irreducible trinomial of degree n over $\mathbb{F}_2$. Then there exists a trinomial basis for $\mathbb{F}_{2^n}$ exactly one of whose elements has trace one.

For each $n \in [2, 1000]$ for which an irreducible trinomial of degree n exists, Table 1 lists one such polynomial whose corresponding basis has exactly one trace-one element.

Next, we determine the traces of elements of some pentanomial bases.

Theorem 4 Let $f(x) = x^n + x^{n-m_1} + x^{n-m_2} + x^{n-m_3} + 1$ be an irreducible polynomial over $\mathbb{F}_2$ with $m_3 > m_2 > m_1 > \frac{n}{2}$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$. Then for $0 \leq k \leq n-1$ we have

$$\mathrm{Tr}(\alpha^k) = \begin{cases} n \bmod 2, & \text{if } k = 0, \\ k \bmod 2, & \text{if } k \in \{m_1, m_2, m_3\}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We apply (2) with $a_{m_1} = a_{m_2} = a_{m_3} = a_n = 1$ and $a_k = 0$ for other $k \in [1, n-1]$. We see that $s_k = 0$ for $1 \leq k < m_1$ and $s_{m_1} + m_1 = 0$; thus $s_{m_1} = (m_1 \bmod 2)$. For $m_1 < k < m_2$, we have $s_k + s_{k-m_1} = 0$. But since $n > k > m_1 > n/2$, we have $k - m_1 < m_1$. Hence $s_{k-m_1} = 0$ which yields $s_k = 0$. Similar arguments show that $s_{m_2} = (m_2 \bmod 2)$, $s_{m_3} = (m_3 \bmod 2)$, and $s_k = 0$ for $m_2 < k < m_3$ and $m_2 < k < n$. □

n	m	n	m	n	m	n	m	n	m	n	m	n	m	n	m	n	m	n	m
2	1	90	27	183	127	284	53	388	159	490	219	599	389	697	267	804	75	900	1
3	1	92	21	185	41	286	69	390	9	492	7	601	201	698	215	806	21	902	21
4	1	93	91	186	11	287	71	391	31	494	17	602	215	700	75	807	7	903	35
5	3	94	21	191	9	289	21	393	7	495	89	604	105	702	37	809	15	905	117
6	1	95	11	193	15	292	37	394	135	497	269	606	165	705	17	810	159	906	123
7	1	97	33	194	87	294	33	396	25	498	155	607	105	708	15	812	29	908	143
9	1	98	11	196	3	295	123	399	49	500	27	609	31	711	319	814	21	911	533
10	3	100	15	198	9	297	5	401	231	503	3	610	127	713	41	815	333	913	91
11	9	102	29	199	67	300	5	402	171	505	331	612	81	714	23	817	187	916	183
12	3	103	9	201	17	302	41	404	65	506	23	614	45	716	183	818	119	918	77
14	5	105	7	202	55	303	1	406	141	508	9	615	211	718	165	820	123	919	141
15	1	106	15	204	27	305	203	407	71	510	69	617	417	719	257	822	17	921	221
17	3	108	17	207	43	308	15	409	87	511	15	618	295	721	9	823	9	924	31
18	3	110	33	209	45	310	93	412	147	513	85	620	9	722	231	825	787	926	365
20	3	111	49	210	7	313	79	414	13	514	67	622	297	724	207	826	255	927	403
21	7	113	9	212	105	314	15	415	163	516	21	623	87	726	5	828	189	930	31
22	1	118	33	214	73	316	63	417	107	518	33	625	133	727	217	831	49	932	177
23	5	119	81	215	23	318	45	418	199	519	79	626	251	729	253	833	149	935	417
25	3	121	91	217	45	319	129	420	7	521	353	628	223	730	147	834	15	937	217
28	1	123	121	218	11	321	31	422	149	522	39	631	307	732	343	838	61	938	207
29	27	124	19	220	7	322	67	423	25	524	167	633	101	735	49	839	327	942	45
30	1	126	21	223	33	324	51	425	21	526	97	634	39	737	5	841	309	943	493
31	3	127	1	225	97	327	175	426	63	527	47	636	217	738	347	842	47	945	77
33	13	129	5	228	113	329	275	428	105	529	157	639	95	740	135	844	105	948	189
34	7	130	3	231	91	330	99	431	231	532	1	641	11	742	85	845	843	951	391
35	33	132	17	233	159	332	89	433	33	534	161	642	119	743	209	846	105	953	435
36	9	134	57	234	31	333	331	436	165	537	443	646	249	745	333	847	153	954	131
39	25	135	11	236	5	337	55	438	65	538	195	647	5	746	351	849	253	956	305
41	3	137	21	238	73	340	45	439	49	540	9	649	37	748	19	850	111	959	143
42	7	140	15	239	81	342	125	441	7	543	203	650	3	750	309	852	159	961	393
44	5	142	21	241	171	343	75	444	81	545	423	651	637	751	187	855	29	964	103
46	1	145	69	242	95	345	37	446	105	550	193	652	93	753	595	857	119	966	201
47	5	146	71	244	111	346	63	447	73	551	135	654	33	754	19	858	207	967	567
49	9	147	49	247	145	348	103	449	167	553	39	655	463	756	45	860	35	969	31
52	3	148	27	249	35	350	53	450	47	556	153	657	73	758	233	861	847	972	7
54	9	150	53	250	103	351	55	455	381	558	73	658	55	759	109	862	349	975	19
55	7	151	3	252	15	353	69	457	61	559	349	660	11	761	3	865	1	977	15
57	7	153	1	253	207	354	99	458	203	561	71	662	21	762	83	866	75	979	801
58	19	154	15	255	173	358	57	460	19	564	163	663	107	767	513	868	145	982	177
60	1	155	93	257	41	359	117	462	73	566	153	665	33	769	447	870	301	983	641
62	29	156	9	258	71	362	63	463	93	567	143	668	147	772	7	871	493	985	763
63	1	159	31	260	15	364	9	465	31	569	77	670	153	774	185	873	521	986	3
65	33	161	39	263	93	366	29	468	27	570	67	671	15	775	93	876	149	988	121
66	3	162	27	265	127	367	21	470	9	574	13	673	183	777	29	879	11	990	161
68	9	166	37	266	47	369	91	471	1	575	317	676	31	778	375	881	489	991	39
71	9	167	35	268	25	370	139	473	273	577	25	679	463	780	13	882	99	993	367
73	25	169	57	270	53	372	111	474	191	580	237	682	171	782	329	884	173	994	223
74	35	170	11	271	201	375	149	476	9	582	85	684	209	783	71	887	147	996	65
76	21	172	1	273	23	377	41	478	121	583	453	686	197	785	191	889	127	998	101
79	9	174	13	274	67	378	43	479	105	585	121	687	13	791	251	890	183	999	59
81	35	175	57	276	63	380	47	481	201	588	35	689	87	793	253	892	31		
84	5	177	89	278	5	382	81	484	105	590	93	690	79	794	143	894	173		
86	21	178	31	279	5	383	135	486	81	593	119	692	299	798	53	895	883		
87	13	180	3	281	93	385	51	487	127	594	19	694	169	799	25	897	113		
89	51	182	81	282	35	386	83	489	83	596	273	695	177	801	217	898	207		

Table 1. For each $n \in [2, 1000]$ for which an irreducible trinomial exists, one such polynomial $x^n + x^m + 1$ is listed whose corresponding basis has exactly one trace-one element.

Theorems 1 and 4 can be used to prove the existence for all finite fields $\mathbb{F}_{2^n}$, $n \in [2, 10000]$, of polynomial bases with a small number of trace-one elements.

Lemma 5 For each $n \in [2, 10000]$ there exists a trinomial or pentanomial basis for $\mathbb{F}_{2^n}$ having at most four elements of trace one.

Proof. If for some n there exists an irreducible trinomial of degree n, then by Theorem 3 there exists a trinomial basis for $\mathbb{F}_{2^n}$ exactly one of whose elements has trace one. Seroussi [14] (see also [3]) lists for each $n \in [2, 10000]$ an irreducible trinomial of degree n (if one exists) or an irreducible pentanomial $x^n + x^{m_1} + x^{m_2} + x^{m_3} + 1$ where $m_1 > m_2 > m_3$. All the pentanomials satisfy the condition $m_1 < \frac{n}{2}$ except for $x^8 + x^4 + x^3 + x + 1$ whose polynomial basis has two trace-one elements. The result now follows from Theorem 4. □

We verified by computer search that for each $n \in [6, 4000]$ there exists an irreducible pentanomial of degree n over $\mathbb{F}_2$ whose corresponding pentanomial basis has exactly one element of trace one. (There is no irreducible pentanomial of degree 4 or 5 with this property.) The tables in the Appendix list one such irreducible pentanomial for each $n \in [6, 809]$. Proving that such pentanomials exist for all $n \geq 6$ is certainly difficult since it remains open to prove the existence of an irreducible pentanomial of degree n over $\mathbb{F}_2$ for all $n \geq 4$. Nevertheless, the results of our search motivate the following conjecture.

Conjecture 6 Let $n \geq 6$, and suppose that there exists an irreducible pentanomial of degree n over $\mathbb{F}_2$. Then there exists a pentanomial basis for $\mathbb{F}_{2^n}$ exactly one of whose elements has trace one.

A classification of the number of trace-one elements in general pentanomial bases seems harder. Let $x^n + x^{n-m_1} + x^{n-m_2} + x^{n-m_3} + 1$ be irreducible over $\mathbb{F}_2$ with $m_3 > m_2 > m_1$ (and without the restriction $m_1 > \frac{n}{2}$). A proof similar to that of Theorem 4 shows that if m_1, m_2, m_3 are even then all elements of the corresponding pentanomial basis except 1 have trace zero (cf. Theorem 8). Suppose now that m_1, m_2 are even and m_3 is odd. (Similar statements can be made for the other cases where at least one of $\{m_1, m_2, m_3\}$ is odd.) Similar to the proof of Theorem 4 we have $\mathrm{Tr}(\alpha^k) = 0$ for $1 \leq k < m_3$ and $\mathrm{Tr}(\alpha^{m_3}) = 1$. Also, equation (2) can be written as $s_k = s_{k-m_1} + s_{k-m_2} + s_{k-m_3}$ for $k > m_3$. This equation gives a fast method for computing the traces of basis elements.

Let S_n be the set of integers $t \in [1, n]$ for which $\mathbb{F}_{2^n}$ has a pentanomial basis exactly t of whose elements have trace one. Since $\mathrm{Tr}(1) = (n \bmod 2)$, we have $n \notin S_n$ if n is even. An interesting problem is to determine the odd integers n for which $S_n = [1, n]$, and the even integers n for which $S_n = [1, n-1]$. It is well known that there are approximately $\frac{2^n}{n}$ irreducible polynomials of degree n over $\mathbb{F}_2$; see [12, Lemma 2]. There are exactly $3 \cdot 2^{n-2}$ binary polynomials of degree n that have a zero constant term or have an even number of non-zero terms (and so are reducible). Thus, the probability that a random degree-n binary polynomial having an odd number of non-zero terms and non-zero constant term is irreducible is approximately $\frac{4}{n}$. If the proportion of irreducibles

among pentanomials is also $\frac{4}{n}$, then the expected number of irreducible binary pentanomials is approximately $\frac{4}{n}\binom{n-1}{3} \approx \frac{2n^2}{3}$. Consequently, for large n we expect that there are many irreducible binary pentanomials and so it would be reasonable to conjecture that $S_n = [1, n]$ (or $S_n = [1, n-1]$). Table 2 provides some evidence that this conjecture is likely to be false. For example, there are exactly 2734 irreducible binary pentanomials of degree 77. However, none of the corresponding polynomial bases have exactly 48, 54, 55, 57, 59, 60, 61, 62, 65 or 73 elements of trace one.

n	T_n	n	T_n	n	T_n
4	{1,2}	36	$\emptyset$	68	{49,53,55}
5	{1,3}	37	{37}	69	{51,53,57,58,62,63,69}
6	{2}	38	{28}	70	$\emptyset$
7	{3}	39	{30}	71	{51}
8	$\emptyset$	40	{28,30}	72	{55,56,57,63,71}
9	$\emptyset$	41	$\emptyset$	73	{56,59,60,73}
10	$\emptyset$	42	{32,33}	74	{53,56,72,73}
11	$\emptyset$	43	{37}	75	{56,58,59,62,64}
12	{5}	44	$\emptyset$	76	$\emptyset$
13	$\emptyset$	45	{33,34,35}	77	{48,54,55,57,59,60,61,62,65,73}
14	$\emptyset$	46	{39}	78	{56,57,70}
15	$\emptyset$	47	{40}	79	{59}
16	{13,15}	48	{33,34,38,41,47}	80	{53,58,63,71,79}
17	$\emptyset$	49	$\emptyset$	81	{68}
18	{14}	50	{38}	82	{61,62,64,66,80,81}
19	{15, 19}	51	{43,51}	83	{63,68,83}
20	$\emptyset$	52	{38}	84	$\emptyset$
21	{17,19,21}	53	{51,53}	85	{63,65,73,85}
22	$\emptyset$	54	{46}	86	{67,70}
23	$\emptyset$	55	{42}	87	$\emptyset$
24	{23}	56	{47,49,55}	88	{69,87}
25	{20}	57	{42,46}	89	$\emptyset$
26	{21}	58	{44,53}	90	{63,67,68}
27	{21}	59	{48,52}	91	{74,78,91}
28	$\emptyset$	60	{54}	92	{68}
29	{27}	61	{58,61}	93	{67,68,73,93}
30	$\emptyset$	62	{49,52,55}	94	{71,79}
31	$\emptyset$	63	$\emptyset$	95	{75,82}
32	$\emptyset$	64	{51,55,59,63}	96	{65,71,72,73,85,95}
33	$\emptyset$	65	$\emptyset$	97	$\emptyset$
34	{24}	66	{59}	98	{57,67,76,77,85,92}
35	$\emptyset$	67	{67}	99	{77,84,99}

Table 2. Listing of T_n for each $4 \leq n \leq 99$. Here, T_n is the set of integers $t \in [1, n-1]$ ($t \in [1, n]$ if n is odd) for which $\mathbb{F}_{2^n}$ does not have a pentanomial basis exactly t of whose elements have trace one.

3 Irreducible Polynomials of Arbitrary Weight

Theorem 4 can be generalized to polynomials of arbitrary weight.

Theorem 7 Let $f(x) = x^n + x^{n-m_1} + x^{n-m_2} + \cdots + x^{n-m_l} + 1$ be an irreducible polynomial over $\mathbb{F}_2$ with $m_l > \cdots > m_2 > m_1 > \frac{n}{2}$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$. Then for $0 \leq k \leq n-1$ we have

$$\mathrm{Tr}(\alpha^k) = \begin{cases} n \bmod 2, & \text{if } k = 0, \\ k \bmod 2, & \text{if } k \in \{m_1, m_2, \ldots, m_l\}, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 4 implies that if m_1, m_2, m_3 are even (and hence n is odd), then all elements of the polynomial basis corresponding to the irreducible polynomial $x^n + x^{n-m_1} + x^{n-m_2} + x^{n-m_3} + 1$ have trace zero except for the element 1. The following results characterize, for the cases of odd and even n, the polynomial bases of $\mathbb{F}_{2^n}$ that have the minimum possible number of trace-one elements.

Theorem 8 Let n be odd and let $f(x) = x^n + x^{n-m_1} + x^{n-m_2} + \cdots + x^{n-m_l} + 1$ be an irreducible polynomial over $\mathbb{F}_2$. Let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$, and let $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Then B has only one trace-one element if and only if m_i is even for all $1 \leq i \leq l$.

Proof. Suppose that B has only one trace-one element; this element must be 1 since n is odd. Assume that at least one of the m_i's is odd, and let m_j be the smallest such number. From equation (2) we see that $s_k = 0$ for all $k < m_j$. Now for $k = m_j$ equation (2) becomes $s_{m_j} + m_j = 0$. But since m_j is odd this means that $s_{m_j} = 1$, which is a contradiction.
Conversely, suppose that each m_i is even. Then for $k < m_1$, equation (2) is $s_k = 0$. For $k = m_1$, equation (2) is $s_{m_1} + m_1 = 0$ which yields $s_{m_1} = 0$ since m_1 is even. Similar arguments show that $s_k = 0$ for all $k > m_1$. □

Theorem 9 Let n be even and let $f(x) = x^n + x^{n-m_1} + x^{n-m_2} + \cdots + x^{n-m_l} + 1$ be an irreducible polynomial over $\mathbb{F}_2$. Let $M = \{m_1, m_2, \ldots, m_l\}$ and let p be the smallest odd number in M. Define $M + p = \{m_1 + p, \ldots, m_l + p\}$ and $N(M+p) = \{k \in M + p \mid k < n\}$. Then the polynomial basis corresponding to $f(x)$ has exactly one trace-one element if and only if $p > 1$ and

$$N(M+p) = \{k \in M \mid k > p \text{ and } k \text{ is odd}\}. \tag{3}$$

Proof. First we prove the sufficiency part. Using equation (2), we see that $s_k = 0$ if $k < p$ and $s_p = 1$. We show by induction that $s_k = 0$ for $k > p$. Equation (2) for $k = p+1$ is $s_{p+1} + s_p a_1 + (p+1)a_{p+1} = 0$. Since p is odd and $p > 1$, we have $a_1 = 0$ and $p + 1 \equiv 0 \pmod 2$; hence $s_{p+1} = 0$. Suppose that for $k > p$ we have $s_i = 0$ for all $i < k$ with $i \neq p$. Then we have $s_k + s_p a_{k-p} + k a_k = 0$. If k is even then we have $s_k + a_{k-p} = 0$. But $k - p$ is odd and from (3) we have $k - p \notin M$. Hence $a_{k-p} = 0$ yielding $s_k = 0$. On the other hand if k is odd, then we have

$s_k + a_{k-p} + a_k = 0$. Now if $a_k = 1$, then from (3) we have $k - p \in M$ and hence $a_{k-p} = 1$. This yields $s_k = 0$. If $a_k = 0$, then from (3) we have $k - p \notin M$ and hence $a_{k-p} = 0$, which in turn implies that $s_k = 0$.
It remains to prove necessity. If $p = 1$ then from (2) we have $s_1 = 1$ and $s_2 = 1$; hence we must have $p > 1$. Again we have $s_k = 0$ for $k < p$, and $s_p = 1$ and $s_{p+1} = 0$. Now let $k > p$. Then $s_k = 0$ and from (2) we must have $a_{k-p} + ka_k = 0$. If k is odd then we have $a_{k-p} + a_k = 0$. This means that $k \in M$ iff $k - p \in M$, which in turn means that $k \in M$ iff $k \in M + p$. Now if k is even then we have $a_{k-p} = 0$. This means that the odd number $k - p$ is not in M, or equivalently that $k \notin M + p$. This completes the proof. □

The next result, whose proof we omit, characterizes the irreducible polynomials for which all elements (except possibly 1) of the corresponding polynomial basis have trace one. One example of such a polynomial is $x^{101} + x^{100} + x^{39} + x^{38} + x^{23} + x^{22} + 1$.

Theorem 10 Let $f(x) = x^n + x^{n-m_1} + x^{n-m_2} + \cdots + x^{n-m_l} + 1$ be an irreducible polynomial over $\mathbb{F}_2$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$. Then $\mathrm{Tr}(\alpha^k) = 1$ for all $1 \leq k \leq n-1$ if and only if the following conditions are satisfied:

(i) $m_1 = 1$,
(ii) $m_{j+1} = m_j + 1$ for $j = 2, 4, 6, \ldots, l-1$, and
(iii) $m_2 \equiv m_4 \equiv m_6 \equiv \cdots \equiv m_{l-1} \equiv 0 \pmod 2$.

Let $n \in [2, 6]$, and let $t \in [1, n]$ if n is odd and $t \in [1, n-1]$ if n is even. It can easily be verified that $\mathbb{F}_{2^n}$ has a polynomial basis exactly t of whose elements have trace one, except for the following values of (n, t): $(3, 2)$, $(4, 2)$, $(5, 3)$, $(6, 2)$. We verified by computer search that for each $n \in [7, 100]$ and each $t \in [1, n-1]$ ($t \in [1, n]$ if n is odd), $\mathbb{F}_{2^n}$ has a heptanomial basis exactly t of whose elements have trace one. This motivates the following conjecture.

Conjecture 11 Let $n \geq 7$, and let $t \in [1, n]$ if n is odd and $t \in [1, n-1]$ if n is even. Then $\mathbb{F}_{2^n}$ has a polynomial basis exactly t of whose elements have trace one.

4 Generalizations to arbitrary finite fields

If $a \in \mathbb{F}_{q^n}$, then the trace of a relative to $\mathbb{F}_q$ is $\mathrm{Tr}(a) = \sum_{i=0}^{n-1} a^{q^i}$. Theorems 1, 7 and 8 can be readily generalized to finite fields of any characteristic p. We state these results here and omit their proofs. We do not know of any (natural) generalizations of Theorems 9 and 10.

Theorem 12 Let $f(x) = x^n + ax^{n-m} + b$ be an irreducible polynomial over $\mathbb{F}_q = \mathbb{F}_{p^r}$, and let α be a root of $f(x)$ in $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f)$. Then for $0 \leq k \leq n-1$

we have

$$\mathrm{Tr}(\alpha^k) = \begin{cases} n \bmod p, & \text{if } k = 0, \\ 0, & \text{if } m \not| k, \\ (-a)^{k/m} m, & \text{otherwise.} \end{cases}$$

Theorem 13 Let $f(x) = x^n + a_{m_1} x^{n-m_1} + a_{m_2} x^{n-m_2} + \cdots + a_{m_l} x^{n-m_l} + a_n$ be an irreducible polynomial over $\mathbb{F}_q = \mathbb{F}_{p^r}$ with $m_l > \cdots > m_2 > m_1 > \frac{n}{2}$, and let α be a root of $f(x)$ in $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f)$. Then for $0 \le k \le n-1$ we have

$$\mathrm{Tr}(\alpha^k) = \begin{cases} n \bmod p, & \text{if } k = 0, \\ -k a_k, & \text{if } k \in \{m_1, m_2, \ldots, m_l\}, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 14 Suppose that $n \not\equiv 0 \pmod p$, and let $f(x) = x^n + a_{m_1} x^{n-m_1} + a_{m_2} x^{n-m_2} + \cdots + a_{m_l} x^{n-m_l} + a_n$ be an irreducible polynomial over $\mathbb{F}_q = \mathbb{F}_{p^r}$. Let α be a root of $f(x)$ in $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f)$, and let $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Then B has only one element of nonzero trace if and only if $m_i \equiv 0 \pmod p$ for all $1 \le i \le l$.

5 Conclusions

We derived simple expressions for the number of trace-one elements in trinomial and pentanomial bases. These expressions allowed us to conclude that for each $n \in [2, 10000]$ there exists a trinomial or polynomial basis for $\mathbb{F}_{2^n}$ having at most four trace-one elements. We also characterized the irreducible polynomials having the minimum and maximum possible number of trace-one elements. An outstanding open problem is to determine whether for any $n \ge 7$ and $t \in [1, n-1]$ ($t \in [1, n]$ if n is odd) there exists a polynomial basis for $\mathbb{F}_{2^n}$ having exactly t trace-one elements.

6 Acknowledgements

We thank Ian Blake, Guang Gong, and the anonymous referees for their very helpful comments.

References

1. ANSI X9.62, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, American National Standards Institute, 1999.
2. ANSI X9.63, *Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*, American National Standards Institute, 2001.
3. I. Blake, S. Gao and R. Lambert, "Constructive problems for irreducible polynomials over finite fields", *Information Theory and Applications*, Lecture Notes in Computer Science 793 (1994), 1-23.

4. A. Bluher, "A Swan-like Theorem", preprint, 2004.
5. FIPS 186-2, "Digital Signature Standard (DSS)", Federal Information Processing Standards Publication 186-2, National Institute of Standards and Technology, 2000.
6. K. Fong, D. Hankerson, J. López and A. Menezes, "Field inversion and point halving revisited", *IEEE Transactions on Computers*, 53 (2004), 1047-1059.
7. G. Gong, T. Berson and D. Stinson, "Elliptic curve pseudorandom sequence generators", *Selected Areas in Cryptography—SAC '99*, Lecture Notes in Computer Science 1758 (2000), 34-48.
8. G. Gong and A. Youssef, "Cryptographic properties of the Welch-Gong transformation sequence generators", *IEEE Transactions on Information Theory*, 48 (2002), 2837-2846.
9. D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2003.
10. E. Knudsen, "Elliptic scalar multiplication using point halving", *Advances in Cryptology—ASIACRYPT '99*, Lecture Notes in Computer Science 1716 (1999), 135-149.
11. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1984.
12. M. Rabin, "Probabilistic algorithms in finite fields", *SIAM Journal on Computing*, 9 (1980), 273-280.
13. R. Schroeppel, "Elliptic curve point halving wins big", 2nd Midwest Arithmetical Geometry in Cryptography Workshop, Urbana, Illinois, November 2000.
14. G. Seroussi, "Table of low-weight binary irreducible polynomials", Hewlett-Packard Technical Report HPL-98-135, 1998.

A Table of irreducible pentanomials

The following tables list for each $n \in [6, 809]$ an irreducible pentanomial $f(x) = x^n + x^{m_1} + x^{m_2} + x^{m_3} + 1$ over $\mathbb{F}_2$ whose corresponding polynomial basis has exactly one element of trace one. Among all such polynomials, the one listed is that for which (a) m_1 is the smallest possible; (b) for this particular value of m_1, m_2 is the largest possible and $< m_1$; and (c) for these particular values of m_1 and m_2, m_3 is the largest possible and $< m_2$. This selection criteria (hopefully) ensures that the middle order terms x^{m_1}, x^{m_2}, x^{m_3} are all of relatively low degree and are close to each other, which in turns facilitates efficient multiplication of polynomials modulo $f(x)$ (e.g., see Section 2.3.5 of [9]). Observe that $m_1 \approx \frac{n}{3}$ if $n \equiv 3, 5 \pmod 8$, and $m_1 \ll \frac{n}{3}$ otherwise. This phenomenon was recently explained by Bluher [4] who proved that the polynomial $f(x) = x^n + \sum_{i \text{ odd}, i < n/3} a_i x^i \in \mathbb{F}_2[x]$ is reducible when $n \equiv \pm 3 \pmod 8$ (cf. Theorem 8).

n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3
6	4	3	1	73	7	3	1	140	6	4	1	207	9	7	3	274	16	15	8	341	119	111	107
7	5	3	1	74	6	2	1	141	47	45	21	208	15	10	4	275	97	89	51	342	14	5	4
8	4	3	2	75	25	23	19	142	12	4	1	209	11	9	1	276	10	8	1	343	13	7	3
9	7	5	1	76	5	4	2	143	9	5	1	210	11	8	4	277	95	91	33	344	11	10	6
10	4	3	2	77	31	17	15	144	7	4	2	211	73	69	49	278	8	6	5	345	11	5	1
11	5	3	1	78	10	9	4	145	13	9	1	212	10	8	3	279	15	13	1	346	14	13	6
12	4	2	1	79	13	3	1	146	7	6	4	213	71	69	59	280	10	9	6	347	117	113	107
13	7	3	1	80	9	4	2	147	49	45	27	214	5	4	2	281	11	5	3	348	8	7	4
14	6	5	2	81	9	3	1	148	12	10	9	215	13	5	1	282	6	3	2	349	119	111	53
15	9	7	3	82	9	6	4	149	51	47	35	216	13	10	6	283	97	93	79	350	6	5	2
16	6	4	1	83	29	25	21	150	5	4	2	217	11	5	3	284	8	6	5	351	11	7	1
17	7	5	1	84	6	5	2	151	15	9	1	218	12	2	1	285	95	93	29	352	22	17	6
18	6	3	2	85	31	27	21	152	6	3	2	219	73	71	59	286	12	8	5	353	15	13	11
19	9	7	5	86	6	5	2	153	9	3	1	220	11	8	6	287	17	11	9	354	12	4	3
20	4	2	1	87	7	5	1	154	10	9	6	221	75	71	21	288	21	10	6	355	121	117	57
21	9	7	1	88	7	6	2	155	53	49	25	222	5	4	2	289	15	13	3	356	12	11	8
22	6	5	2	89	9	7	5	156	10	8	5	223	9	3	1	290	18	17	16	357	119	117	27
23	5	3	1	90	7	6	4	157	55	53	47	224	12	7	2	291	97	95	89	358	14	8	7
24	7	4	2	91	33	25	19	158	8	6	5	225	15	7	1	292	11	8	6	359	9	7	1
25	9	7	3	92	6	5	4	159	15	13	3	226	12	5	2	293	99	95	9	360	15	6	2
26	6	3	2	93	31	29	25	160	14	3	2	227	77	73	43	294	16	13	6	361	11	7	3
27	9	7	3	94	8	6	5	161	21	19	7	228	8	2	1	295	9	5	1	362	14	11	6
28	6	4	1	95	7	5	3	162	8	7	4	229	79	75	39	296	14	5	2	363	121	119	59
29	15	13	5	96	10	9	6	163	57	49	29	230	8	7	6	297	7	3	1	364	10	7	4
30	6	4	1	97	9	7	5	164	10	8	7	231	9	7	1	298	11	8	6	365	127	119	99
31	7	5	3	98	8	7	4	165	55	51	13	232	9	4	2	299	101	97	15	366	8	6	5
32	7	6	2	99	33	31	25	166	10	3	2	233	13	11	3	300	7	6	4	367	17	9	1
33	7	5	1	100	6	5	2	167	17	9	1	234	14	11	10	301	103	99	59	368	24	21	14
34	6	2	1	101	35	33	31	168	16	9	6	235	81	77	25	302	16	14	1	369	17	5	3
35	13	11	9	102	8	5	2	169	13	3	1	236	10	9	2	303	17	15	11	370	14	9	4
36	5	4	2	103	13	9	3	170	6	3	2	237	79	77	25	304	15	4	2	371	125	121	93
37	15	11	5	104	12	3	2	171	57	55	45	238	6	4	1	305	9	5	1	372	8	7	2
38	8	7	6	105	13	7	1	172	12	10	5	239	15	13	5	306	20	18	15	373	127	123	45
39	7	5	1	106	9	4	2	173	59	55	43	240	12	5	2	307	105	97	57	374	8	6	5
40	9	6	4	107	37	33	23	174	10	6	3	241	19	15	7	308	12	10	5	375	23	15	11
41	7	3	1	108	6	4	1	175	13	7	1	242	11	8	6	309	103	99	73	376	10	3	2
42	8	7	2	109	43	41	23	176	11	6	2	243	81	79	15	310	14	9	2	377	15	5	3
43	17	13	11	110	6	4	1	177	13	7	5	244	10	9	2	311	7	5	3	378	9	6	4
44	6	5	2	111	11	9	5	178	8	7	2	245	83	79	51	312	32	25	10	379	129	125	77
45	15	11	9	112	11	10	2	179	61	57	49	246	11	8	2	313	7	3	1	380	14	6	3
46	6	4	3	113	7	5	1	180	6	4	3	247	15	7	3	314	15	14	8	381	127	125	101
47	7	3	1	114	12	10	3	181	63	57	55	248	15	14	10	315	105	103	19	382	17	16	12
48	8	5	2	115	41	33	19	182	8	7	6	249	19	17	1	316	10	8	3	383	9	7	5
49	9	3	1	116	4	2	1	183	15	7	1	250	15	10	6	317	107	103	45	384	12	3	2
50	4	3	2	117	39	35	17	184	10	5	2	251	89	81	79	318	8	6	5	385	19	11	3
51	17	11	9	118	6	5	2	185	13	5	3	252	10	8	1	319	13	3	1	386	10	6	5
52	6	5	4	119	9	7	5	186	9	8	6	253	87	83	61	320	8	3	2	387	129	125	113
53	19	17	15	120	9	6	2	187	65	63	61	254	14	6	5	321	13	7	5	388	18	16	3
54	8	6	3	121	13	7	3	188	6	5	2	255	15	7	3	322	18	17	16	389	135	127	85
55	13	7	1	122	6	2	1	189	63	59	17	256	10	5	2	323	109	105	53	390	12	4	1
56	7	4	2	123	41	39	35	190	8	7	6	257	17	5	3	324	4	2	1	391	15	13	1
57	9	7	1	124	10	9	8	191	11	9	3	258	9	6	4	325	111	107	89	392	13	10	6
58	6	5	4	125	43	39	31	192	12	9	6	259	89	85	17	326	11	10	6	393	17	13	1
59	21	19	17	126	7	4	2	193	13	9	3	260	6	5	4	327	13	11	7	394	8	7	2
60	5	4	2	127	7	3	1	194	4	3	2	261	87	85	19	328	14	3	2	395	133	129	113
61	23	15	13	128	11	10	6	195	65	59	51	262	9	8	4	329	15	13	1	396	7	6	4
62	8	7	6	129	13	7	3	196	12	11	8	263	11	9	5	330	8	7	2	397	135	131	65
63	9	3	1	130	14	12	11	197	67	63	53	264	9	6	2	331	113	109	89	398	7	6	2
64	4	3	2	131	45	41	33	198	14	8	1	265	17	15	11	332	6	2	1	399	17	9	3
65	11	9	3	132	8	5	4	199	17	11	7	266	6	3	2	333	111	109	105	400	15	12	10
66	4	2	1	133	47	43	3	200	11	8	2	267	89	87	81	334	13	8	2	401	19	15	1
67	25	21	7	134	8	4	1	201	9	7	1	268	10	4	1	335	15	13	1	402	12	11	8
68	10	9	8	135	9	5	3	202	7	6	4	269	91	87	77	336	15	14	2	403	137	133	131
69	23	17	15	136	8	3	2	203	69	67	65	270	5	4	2	337	25	21	11	404	7	6	4
70	8	5	4	137	13	9	5	204	5	4	2	271	21	11	1	338	6	3	2	405	135	133	129
71	5	3	1	138	9	8	6	205	71	67	59	272	9	6	2	339	113	111	89	406	8	3	2
72	10	9	6	139	53	49	41	206	14	13	10	273	11	5	3	340	12	8	5	407	9	7	5

n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3	n	m_1	m_2	m_3
408	10	5	2	475	161	157	111	542	8	6	1	609	23	11	3	676	10	7	4	743	21	19	11
409	7	5	3	476	10	8	1	543	11	7	5	610	11	10	8	677	227	223	139	744	38	27	18
410	10	4	3	477	159	157	93	544	26	7	2	611	205	201	31	678	20	8	1	745	19	13	1
411	137	135	113	478	6	4	1	545	19	17	9	612	14	13	8	679	21	19	9	746	12	7	4
412	14	8	3	479	19	11	7	546	8	7	2	613	211	209	191	680	32	11	2	747	249	247	75
413	139	135	25	480	26	21	6	547	185	181	29	614	17	12	6	681	11	9	3	748	18	10	5
414	16	7	2	481	11	7	3	548	16	9	8	615	11	5	1	682	14	12	11	749	255	251	239
415	13	5	3	482	10	7	2	549	183	181	141	616	19	14	2	683	229	225	203	750	14	13	8
416	15	14	2	483	161	157	83	550	21	20	2	617	11	3	1	684	16	11	4	751	11	9	1
417	13	3	1	484	14	12	11	551	11	7	3	618	11	8	4	685	231	223	47	752	25	18	14
418	16	7	6	485	163	159	145	552	20	5	2	619	209	201	29	686	10	9	4	753	23	15	11
419	145	131	129	486	14	8	5	553	21	19	9	620	14	7	4	687	19	17	11	754	19	14	12
420	13	10	8	487	13	11	5	554	10	8	7	621	207	205	3	688	19	14	6	755	253	249	67
421	143	139	21	488	20	11	2	555	185	183	3	622	16	10	1	689	21	19	7	756	14	10	7
422	10	6	1	489	17	11	1	556	14	12	5	623	13	9	5	690	12	10	7	757	255	247	111
423	9	5	3	490	16	8	3	557	187	183	181	624	18	5	2	691	237	217	195	758	18	17	10
424	10	9	6	491	165	161	137	558	16	13	2	625	19	13	1	692	14	6	5	759	17	11	1
425	13	5	1	492	6	4	1	559	13	9	1	626	18	15	8	693	231	229	223	760	26	13	2
426	14	12	11	493	167	163	123	560	16	3	2	627	209	207	27	694	19	10	4	761	7	3	1
427	145	137	101	494	16	7	2	561	11	9	3	628	12	11	2	695	13	9	5	762	15	12	4
428	14	10	3	495	15	9	1	562	11	4	2	629	211	207	35	696	23	10	2	763	257	253	87
429	143	141	63	496	16	5	2	563	189	185	177	630	7	4	2	697	19	17	11	764	12	11	6
430	14	6	1	497	23	15	9	564	15	14	8	631	21	9	7	698	10	9	8	765	255	253	243
431	5	3	1	498	10	9	6	565	191	187	173	632	21	14	4	699	233	231	173	766	23	6	2
432	14	5	2	499	169	165	57	566	6	5	2	633	25	11	7	700	6	5	2	767	19	17	7
433	11	5	3	500	10	6	1	567	13	11	5	634	12	10	5	701	235	231	175	768	21	8	2
434	18	15	14	501	167	159	129	568	25	18	14	635	213	209	193	702	22	13	6	769	17	13	5
435	145	141	93	502	8	5	4	569	13	7	3	636	13	8	4	703	19	13	9	770	14	5	2
436	6	5	4	503	9	5	1	570	18	12	7	637	215	207	179	704	8	3	2	771	257	253	97
437	147	143	113	504	15	14	6	571	193	189	179	638	13	12	2	705	25	9	3	772	8	6	5
438	14	13	8	505	23	17	7	572	12	9	8	639	19	7	1	706	12	11	8	773	259	255	151
439	13	11	9	506	16	15	4	573	191	189	149	640	14	3	2	707	237	233	135	774	16	14	7
440	8	3	2	507	169	167	133	574	14	9	2	641	19	5	1	708	5	4	2	775	9	5	1
441	17	15	9	508	8	6	5	575	17	15	7	642	10	9	6	709	241	239	231	776	16	7	2
442	12	4	3	509	171	167	121	576	15	14	2	643	217	213	85	710	13	12	4	777	23	19	13
443	153	145	133	510	6	4	1	577	17	15	1	644	12	11	10	711	13	7	5	778	22	17	12
444	12	11	2	511	15	7	1	578	23	22	16	645	215	211	185	712	23	12	2	779	261	257	35
445	151	147	133	512	8	5	2	579	193	191	169	646	17	12	8	713	17	15	9	780	10	9	4
446	11	6	2	513	13	11	5	580	6	4	1	647	15	13	5	714	13	10	6	781	263	259	21
447	11	5	3	514	11	8	6	581	195	191	89	648	33	24	14	715	241	237	129	782	12	8	1
448	11	6	4	515	173	169	129	582	12	9	6	649	11	5	1	716	10	6	5	783	11	5	3
449	11	9	3	516	14	2	1	583	23	9	5	650	18	15	6	717	239	235	65	784	20	3	2
450	14	7	2	517	175	171	17	584	17	14	6	651	217	215	209	718	6	4	1	785	17	9	3
451	153	149	25	518	14	10	7	585	25	17	5	652	13	12	4	719	21	15	3	786	12	10	3
452	6	5	4	519	17	5	1	586	14	2	1	653	219	215	203	720	9	6	4	787	265	261	179
453	151	147	97	520	19	8	6	587	197	193	177	654	13	8	2	721	17	11	3	788	20	18	3
454	8	6	1	521	15	11	9	588	14	12	9	655	17	15	5	722	16	10	3	789	263	261	173
455	15	7	1	522	21	20	6	589	199	195	171	656	19	18	10	723	241	239	199	790	18	15	10
456	18	9	6	523	177	169	159	590	12	9	2	657	19	15	9	724	16	10	1	791	19	13	11
457	15	7	1	524	17	12	2	591	19	9	3	658	12	10	7	725	243	239	171	792	35	24	2
458	16	8	3	525	175	173	161	592	28	27	6	659	221	217	181	726	11	6	2	793	13	9	5
459	153	149	29	526	14	7	6	593	13	3	1	660	10	8	5	727	15	9	3	794	19	18	16
460	13	10	4	527	9	7	1	594	11	10	8	661	223	219	133	728	4	3	2	795	265	263	157
461	155	151	75	528	11	6	2	595	201	197	53	662	12	6	3	729	9	7	1	796	15	6	4
462	15	12	2	529	13	5	3	596	6	5	4	663	15	3	1	730	16	15	4	797	267	263	171
463	21	5	1	530	12	10	7	597	199	197	173	664	15	4	2	731	245	241	121	798	20	17	16
464	25	14	10	531	177	173	141	598	8	6	1	665	19	11	3	732	7	6	4	799	21	19	3
465	15	7	3	532	10	4	3	599	11	7	1	666	10	7	2	733	247	239	45	800	12	7	2
466	14	11	6	533	183	175	173	600	24	21	14	667	225	221	121	734	11	6	2	801	9	7	1
467	161	153	107	534	11	10	2	601	19	5	3	668	10	6	1	735	21	15	7	802	20	12	7
468	14	5	4	535	9	7	3	602	6	3	2	669	223	219	49	736	13	8	6	803	273	265	263
469	159	151	113	536	18	7	2	603	201	195	131	670	19	18	2	737	25	21	7	804	12	8	5
470	9	8	2	537	17	13	5	604	15	6	4	671	17	15	3	738	22	7	6	805	271	267	219
471	21	19	9	538	13	10	6	605	203	199	127	672	12	5	2	739	249	245	233	806	16	13	6
472	30	27	18	539	181	177	19	606	16	8	5	673	23	21	1	740	4	2	1	807	15	7	1
473	21	19	5	540	14	7	4	607	15	3	1	674	20	18	7	741	247	243	241	808	14	3	2
474	12	10	3	541	183	175	145	608	20	9	2	675	225	223	189	742	12	4	1	809	13	11	3