Some Open Problems Arising from my Recent Finite Field Research

Gary L. Mullen

Penn State University

mullen@math.psu.edu

July 13, 2015

Let q be a prime power

Let F_q denote the finite field with q elements

E-perfect codes

F. Castro, H. Janwa, M, I. Rubio, Bull. ICA (2016)

Theorem

(Hamming bound) Let C be a t-error-correcting code of length n over F_q. Then

$$|C|\left[1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right]\leq q^n.$$

A code C is **perfect** if the code's parameters yield an equality in the Hamming bound.

The parameters of all perfect codes are known, and can be listed as follows:

The **trivial** perfect codes are

1. The zero vector $(0, \ldots, 0)$ of length n,
2. The entire vector space F_q^n
3. The binary repetition code of odd length n.

The non-trivial perfect codes must have the parameters $(n, M = q^k, 3)$ of the Hamming codes and the Golay codes (unique up to equivalence) whose parameters can be listed as follows:

1. The Hamming code $\left[\frac{q^m-1}{q-1}, n-m, 3\right]$ over F_q, where $m \geq 2$ is a positive integer;
2. The $[11, 6, 5]$ Golay code over F_3;
3. The $[23, 12, 7]$ Golay code over F_2.

Let C be a t-error-correcting code of length n over F_q.

Then,

$$|C| \left[1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t \right] \leq q^n.$$

A t-error correcting code C with parameters $(n, M, d), t = \lfloor \frac{d-1}{2} \rfloor$, is e-**perfect** if in the Hamming bound, equality is achieved when, on the right hand side, q^n is replaced by q^e.

An n-perfect code is a perfect code.

Conjecture

Let C be an (n, M, d) t-error correcting non-trivial e-perfect code over F_q. Then C must have one of the following sets of parameters:

1. $\left(\frac{q^m-1}{q-1}, q^{e-m}, 3\right)$, *with q a prime power and $m < e \leq n$, where $m \geq 2$;*
2. $(11, 3^{e-5}, 5)$, *with $q = 3$ and $5 < e \leq 11$;*
3. $(23, 2^{e-11}, 7)$, *with $q = 2$ and $11 < e \leq 23$;*
4. $(90, 2^{e-12}, 5)$, *with $q = 2$ and $12 < e \leq 89$.*

Problem

Prove this conjecture.

We can construct e-perfect codes with each of the parameters listed above, except for the case when $n = 90$ and $e = 89$.

As was the case for perfect codes, there could be many e-perfect codes with a given set of parameters.

R-closed subsets of Z_p

S. Huczynska, M, J. Yucas, JCT, A (2009)

Let G be a finite abelian group with $|G| = g$

Let S be a subset of G with $|S| = s$.

Definition

*Let $0 \leq r \leq s^2$. A set S is r-**closed** if, among the s^2 ordered pairs (a, b) with $a, b \in S$, there are exactly r pairs such that $a + b \in S$.*

The r-value of the r-closed set S is denoted by $r(S)$.

If S is a subgroup of G then S is s^2-closed

If S is a sum-free set then S is 0-closed.

For a given G, what (if anything) can be said about the spectrum of r-values of the subsets of G?

Motivated by the classical Cauchy-Davenport Theorem, we are particularly interested in the case when $G = Z_p$ under addition modulo the prime p.

For $G = Z_p$ we characterize the maximal and minimal possible r-values.

We make a conjecture (verified computationally for all primes $p \leq 23$) about the complete spectrum of r-values for any subset cardinality in Z_p and prove that, for any p, all conjectured r-values in the spectrum are attained when the subset cardinality is suitably small ($s < \frac{2p+2}{7}$).

Theorem

Let G be a finite abelian group of order g. Let s be a positive integer with $0 \leq s \leq g$, and let S be a subset of G of size s. Let T be the complement of S in G. Then

$$r(S) + r(T) = g^2 - 3gs + 3s^2.$$

Theorem (Cauchy-Davenport)

If A and B are non-empty subsets of Z_p then $|A+B| \geq \min(p, |A|+|B|-1)$.

Definition

For p be a prime, define

$$k[p] = \lfloor \frac{p+1}{3} \rfloor = \begin{cases} \frac{p-1}{3}, & p \equiv 1 \bmod 3 \\ \frac{p}{3}, & p \equiv 0 \bmod 3 \\ \frac{p+1}{3}, & p \equiv -1 \bmod 3 \end{cases}$$

Proposition

Let p be a prime. If $S \subseteq Z_p$ is 0-closed then $|S| \leq k[p]$.

Definition

Let p be an odd prime. For $0 \leq s \leq p$, define f_s and g_s as follows:

$$f_s = \begin{cases} 0 & s \leq k[p] \\ \frac{(3s-p)^2-1}{4} & s > k[p] \text{ and } s \text{ even} \\ \frac{(3s-p)^2}{4} & s > k[p] \text{ and } s \text{ odd} \end{cases}$$

$$g_s = \begin{cases} \frac{3s^2}{4} & s \leq p-k[p] \text{ and } s \text{ even} \\ \frac{3s^2+1}{4} & s \leq p-k[p] \text{ and } s \text{ odd} \\ p^2-3sp+3s^2 & s > p-k[p] \end{cases}$$

Note that $f_s + g_{p-s} = p^2 - 3sp + 3s^2$.

Proposition

Let $p > 11$. For $1 \leq s \leq 3$ and $p - 3 \leq s \leq p$, the r-values for subsets of Z_p of size s are precisely the integers in the interval $[f_s, g_s]$ with the following exceptions:

s	f_s	g_s	exceptions
1	0	1	—
2	0	3	2
3	0	7	4
p	p^2	p^2	—
$p-1$	p^2-3p+2	p^2-3p+3	—
$p-2$	p^2-6p+9	$p^2-6p+12$	$p^2-6p+10$
$p-3$	$p^2-9p+20$	$p^2-9p+27$	$p^2-9p+23$

Definition

If $4 \le s \le p-4$, *define* $V(s)$ *by*

$$V(s) = \begin{cases} 0 & \textit{if } s \le k[p] \\ \lceil \frac{p-s-3}{4} \rceil & \textit{if } s \ge \lfloor \frac{p+1}{2} \rfloor \\ \lceil \frac{3s-p-1}{4} \rceil & \textit{otherwise} \end{cases} .$$

Conjecture

For $p > 11$ and $4 \le s \le p-4$, there are $V(s)$ exceptional values at the low end of the interval $[f_s, g_s]$ and $V(p-s)$ exceptional values at the high end of the interval $[f_s, g_s]$. All other values in the interval can be obtained as r-values. The exceptions are given by:

$$f_s + 3i + 1 \text{ for } 0 \le i < V(s) \text{ if } s \equiv p \text{ mod } 2$$

$$f_s + 3i + 2 \text{ for } 0 \le i < V(s) \text{ if } s \not\equiv p \text{ mod } 2$$

$$g_s - 3i - 1 \text{ for } 0 \le i < V(p-s) \text{ if } s \text{ is even}$$

$$g_s - 3i - 2 \text{ for } 0 \le i < V(p-s) \text{ if } s \text{ is odd}$$

Verified computationally for all primes $p \le 23$ and all corresponding s $(4 \le s \le p-4)$.

Problem

Prove the conjecture

All conjectured r-values in the spectrum are attained when the subset cardinality is suitably small ($s < \frac{2p+2}{7}$).

Subfield Value Sets

W.-S. Chou, J. Gomez-Calderon, M, D. Panario, D. Thomson, Funct. Approx. Comment. Math. (2013)

Let F_{q^d} be a subfield of F_{q^e} so $d|e$

For $f \in F_{q^e}[x]$, **subfield value set** $V_f(q^e; q^d) = \{f(c) \in F_{q^d} | c \in F_{q^e}\}$

Theorem

$$|V_{x^n}(q^e; q^d)| = \frac{(n(q^d - 1), q^e - 1)}{(n, q^e - 1)} + 1$$

Dickson poly. deg. n, parameter $a \in F_q$

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

$D_n(x,0) = x^n$

Theorem

Chou, Gomez-Calderon, M, JNT, (1988)

$$|V_{D_n(x,a)}| = \frac{q-1}{2(n,q-1)} + \frac{q+1}{2(n,q+1)} + \alpha$$

α *usually 0.*

Theorem

q odd and $a \in F_{q^e}^*$ with $a^n \in F_{q^d}$, $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = 1$,

$$|V_{D_n(x,a)}(q^e; q^d)| = \frac{(q^e - 1, n(q^d - 1)) + (q^e - 1, n(q^d + 1))}{2(q^e - 1, n)}$$

$$+ \frac{(q^e + 1, n(q^d - 1)) + (q^e + 1, n(q^d + 1))}{2(q^e + 1, n)} - \frac{3 + (-1)^{n+1}}{2}$$

Problem

Find subfield value set $|V_{D_n(x,a)}(q^e; q^d)|$ when $a \in F_{q^e}^*$ and $a^n \notin F_{q^d}$

In order to have $D_n(c,a) = y^n + \frac{a^n}{y^n} \in F_{q^d}$ we need

$$(y^n + \frac{a^n}{y^n})^{q^d} = y^n + \frac{a^n}{y^n}.$$

If $a^n \in F_{q^d}$

$$(y^{n(q^d-1)} - 1)(y^{n(q^d+1)} - a^n) = 0.$$

Hypercubes of class r

J. Ethier, M, D. Panario, B. Stevens, D. Thomson, JCT, A (2011)

Definition

*Let d, n, r, t be integers, with $d > 0, n > 0, r > 0$ and $0 \leq t \leq d - r$. A (d, n, r, t)-***hypercube of dimension** d**, order** n**, class** r **and type** t *is an $n \times \cdots \times n$ (d times) array on n^r distinct symbols such that in every t-subarray (that is, fix t coordinates of the array and allow the remaining $d - t$ coordinates to vary) each of the n^r distinct symbols appears exactly n^{d-t-r} times.*
If $d \geq 2r$, two such hypercubes are **orthogonal** *if when superimposed, each of the n^{2r} possible distinct pairs occurs exactly n^{d-2r} times.*
A set $\mathcal{H}$ of such hypercubes is **mutually orthogonal** *if any two distinct hypercubes in $\mathcal{H}$ are orthogonal.*

A $(2, n, 1, 1)$ hypercube is a latin square order n.

If $r = 1$ we have latin hypercubes.

$$\begin{array}{ccc|ccc|ccc} 0 & 1 & 2 & 4 & 5 & 3 & 8 & 6 & 7 \\ 3 & 4 & 5 & 7 & 8 & 6 & 2 & 0 & 1 \\ 6 & 7 & 8 & 1 & 2 & 0 & 5 & 3 & 4 \end{array}$$

A hypercube of dimension 3, order 3, class 2, and type 1.

Theorem

The maximum number of mutually orthogonal hypercubes of dimension d, order n, type t, and class r is bounded above by

$$\frac{1}{n^r - 1}\left(n^d - 1 - \binom{d}{1}(n-1) - \binom{d}{2}(n-1)^2 - \cdots - \binom{d}{t}(n-1)^t\right).$$

Corollary

There are at most $n-1$ mutually orthogonal Latin squares of order n.

Theorem

Let q be a prime power. The number of $(2r, q, r, r)$-hypercubes is at least the number of linear MDS codes over F_q of length $2r$ and dimension r.

Theorem

There are at most $(n-1)^r$, $(2r, n, r, r)$ *mutually orthogonal hypercubes.*

Theorem

Let n *be a prime power. For any integer* $r < n$*, there is a set of* $n-1$ *mutually orthogonal* $(2r, n, r, r)$*-hypercubes.*

Theorem

Let $n = 2^{2k}$, $k \in \mathbb{N}$*. Then there is a complete set of* $(n-1)^2$ *mutually orthogonal hypercubes of dimension* 4*, order* n*, and class* 2*.*

D. Droz: If $r = 2$ and n is odd, there is complete set.

Hypercube problems

1. Construct a complete set of mutually orthogonal $(4, n, 2, 2)$-hypercubes when $n = 2^{2k+1}$.

   D. Droz: If $r = 2$, $n = 2^{2k+1}$ there are $(n-1)(n-2)$ MOHC. Are there $(n-1)^2$ MOHC?

2. Is the $(n-1)^r$ bound tight when $r > 2$? If so, construct a complete set of mutually orthogonal $(2r, n, r, r)$-hypercubes of class $r > 2$. If not, determine a tight upper bound and construct such a complete set.

   D. Droz: If $r \geq 1$ and $n \equiv 1 \pmod{r}$, there is complete set.

   D. Droz: If $n = p^{rk}$ there is a complete set.

3. Find constructions (other than the standard Kronecker product constructions) for sets of mutually orthogonal hypercubes when n is not a prime power. Such constructions will require a new method not based on finite fields.

4. What can be said when $d > 2r$?

k-Normal elements

S. Huczynska, M, D. Panario, D. Thomson, FFA (2013)

Let q be a prime power and $n \in \mathbb{N}$. An element $\alpha \in \mathbb{F}_{q^n}$ yields a **normal basis** for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $B = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; such an α is a **normal element** of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem

For $\alpha \in \mathbb{F}_{q^n}$, $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the polynomials $x^n - 1$ and $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ in $\mathbb{F}_{q^n}[x]$ are relatively prime.

Motivated by this, we make the

Definition

*Let $\alpha \in \mathbb{F}_{q^n}$. Denote by $g_\alpha(x)$ the polynomial $\sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i} \in \mathbb{F}_{q^n}[x]$. If $\gcd(x^n - 1, g_\alpha(x))$ over $\mathbb{F}_{q^n}$ has degree k (where $0 \leq k \leq n-1$), then α is a k-**normal** element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

A normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is 0-normal.

Definition

Let $f \in \mathbb{F}_q[x]$ be monic, the Euler Phi function for polynomials is given by $\Phi_q(f) = |(\mathbb{F}_q[x]/f\mathbb{F}_q[x])^*|$.

Theorem

The number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by

$$\sum_{\substack{h | x^n - 1, \\ \deg(h) = n-k}} \Phi_q(h), \tag{1}$$

where divisors are monic and polynomial division is over $\mathbb{F}_q$.

An important extension of the **Normal Basis Theorem** is the **Primitive Normal Basis Theorem** which establishes that, for all pairs (q, n), a normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ exists with α a primitive element of $\mathbb{F}_{q^n}$.

We ask whether an analogous claim can be made about k-normal elements for certain non-zero values of k?

In particular, when $k = 1$, does there always exist a primitive 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$?

Theorem

Let $q = p^e$ be a prime power and $n \in \mathbb{N}$ with $p \nmid n$. Assume that $n \geq 6$ if $q \geq 11$, and that $n \geq 3$ if $3 \leq q \leq 9$. Then there exists a primitive 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Problem

Obtain a complete existence result for primitive 1-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (with or without a computer). We conjecture that such elements always exist.

Problem

For which values of q, n and k can explicit formulas be obtained for the number of k-normal primitive elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$?

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Conjecture

(L. Anderson/M) Let $p \geq 5$ be a prime and let $m \geq 3$. Let a be 1 or 2 and let k be 0 or 1. Then there is an element $\alpha \in F_{p^m}$ of order $\frac{p^m-1}{a}$ which is k-normal.

The $a = 1, k = 0$ case gives the Prim. Nor. Basis Thm.

Problem

Determine the existence of high-order k-normal elements $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Dickson Polynomials

Dickson poly. deg. n**, parameter** $a \in F_q$

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

$D_n(x,0) = x^n$

Theorem

Nöbauer (1968) For $a \neq 0$, $D_n(x,a)$ PP on F_q iff $(n, q^2-1) = 1$.

Theorem

Chou, Gomez-Calderon, M, JNT, (1988)

$$|V_{D_n(x,a)}| = \frac{q-1}{2(n,q-1)} + \frac{q+1}{2(n,q+1)} + \alpha$$

α usually 0

Reverse Dickson Polynomials

Fix $x \in F_q$ and let a be the variable in $D_n(x, a)$

Some basic PP results on RDPs in Hou, Sellers, M, Yucas, FFA, 2009

$f : F_q \to F_q$ is **almost perfect nonlinear (APN)** if for each $a \in F_q^*$ and $b \in F_q$ the eq. $f(x + a) - f(x) = b$ has at most two solutions in F_q

Theorem

For p odd, x^n APN on $F_{p^{2e}}$ implies $D_n(1, x)$ PP on F_{p^e} implies x^n APN on F_{p^e}

Conjecture

Let $p > 3$ be a prime and let $1 \leq n \leq p^2 - 1$. Then $D_n(1, x)$ is a PP on $\mathbb{F}_p$ if and only if

$$n = \begin{cases} 2,\ 2p,\ 3,\ 3p,\ p+1,\ p+2,\ 2p+1 & \text{if } p \equiv 1 \pmod{12}, \\ 2,\ 2p,\ 3,\ 3p,\ p+1 & \text{if } p \equiv 5 \pmod{12}, \\ 2,\ 2p,\ 3,\ 3p,\ p+2,\ 2p+1 & \text{if } p \equiv 7 \pmod{12}, \\ 2,\ 2p,\ 3,\ 3p & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Problem

Complete the PP classification for RDPs over F_p.

Problem

What happens over F_q when q is a prime power?

Problem

Determine value set for RDPs over F_p

THANK YOU!!!