Journal der mathematiſchen Ablehnungen

Paper No.31 (2014)

On the number of distinct values of a class of functions with finite domain

Robert S. Coulter and Steven Senger

Ewing Hall
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716, USA

AMS Subject class: 05E99, 11T06

Keywords: bounds on image sets, planar functions

Note: This is a personal preprint; for correct page numbering and references please see the original paper, the proper citation for which is:

R.S. Coulter and S. Senger, *On the number of distinct values of a class of functions with finite domain*, Ann. Comb. **18** (2014), 233–243.

Abstract

By relating the number of images of a function with finite domain to a certain parameter, we obtain both an upper and lower bound for the image set. Even though the arguments are elementary, the bounds are, in some sense, best possible. These bounds are then applied in several contexts. In particular, we obtain the first non-trivial upper bound for the image set of a planar function over a finite field.

§ 1. Introduction

Let A and B be sets, with A finite of order n, and let $f : A \to B$. We define the following notation, which will be used throughout this article.

- The number of distinct images of f is denoted by $V(f)$. That is, $V(f) = |f(A)|$.
- For $r \in \mathbb{N}$, $M_r(f)$ is the number of $y \in B$ for which $f(x) = y$ has r solutions.
- Since A is finite, clearly $M_r(f) = 0$ for all sufficiently large r. We therefore define m to be the largest integer for which $M_m > 0$.
- For each integer $r \geq 2$, $N_r(f)$ is the number of r-tuples $(x_1, \dots, x_r)$ with $x_i = x_j$ if and only if $i = j$ which satisfy $f(x_1) = f(x_2) = \cdots = f(x_r)$.

Several identities follow immediately from these definitions.

Id#1 $V(f) = \sum_{r=1}^{m} M_r(f)$.

Id#2 $n = \sum_{r=1}^{m} rM_r(f)$.

Id#3 $N_s(f) = \sum_{r=s}^{m} P(r,s)M_r(f)$.

(Here $P(r,s)$ denotes the number of s-permutations from r distinct objects. Recall $P(r,s) = 0$ when $r < s$.)

In this paper we are interested in the relationship between $V(f)$ and $N_s(f)$ for a fixed s. Intuitively, knowledge of $N_s(f)$ should imply some knowledge on $V(f)$, and knowledge of $N_s(f)$ should yield more knowledge concerning $V(f)$ than $N_{s'}(f)$ would for $s' > s$. Our main result is to obtain bounds for $V(f)$ in terms of $N_s(f)$ which confirm this intuition. Moreover, when $s = 2$, our lower bound is tight for any value of $N_2(f)$, while our upper bound is tight in infinitely many cases. Our main theorem can be given in the following form.

Theorem 1. *Let $f : A \to B$ with $|A| = n$. Then*

$$\frac{1}{s-1}\left(n - \frac{N_s(f)}{s!}\right) \le V(f) \le n - N_s(f)^{1/s} + O(N_s(f)^{1/(s+1)}).$$

We pay particular attention to the case $s = 2$ because it is more likely that one has information on pairs of elements with the same image than, say, 3-tuples or 4-tuples. In addition, the upper bound can be made explicit in this case.

Theorem 2. *Let $f : A \to B$ with $|A| = n$ and set $N_2(f) = t$. Then $M_1(f) \ge \mathrm{Max}(0, n-t)$ and*

$$n - \frac{t}{2} \le M_1(f) + M_2(f) \le V(f) \le n - \frac{2t}{1+\sqrt{4t+1}}$$

Interestingly, the upper bound in Theorem 2 is related to triangular numbers, and a slight improvement of this bound, in some cases, could be obtained by resolving a problem on them.

Theorems 1 and 2 can be applied in a variety of settings. We choose to limit ourselves to just one main application – to polynomials over finite fields.

Let q be a positive power of some prime p. We use the standard notation of $\mathbb{F}_q$ for the finite field of q elements, $\mathbb{F}_q^\star$ for the non-zero elements of $\mathbb{F}_q$, and $\mathbb{F}_q[X]$ for the ring of polynomials over $\mathbb{F}_q$ in X. We prove that for a polynomial $f \in \mathbb{F}_q[X]$, the expected value of $N_2(f)$ is $q-1$. Consequently, we obtain the following corollary to Theorem 2.

Theorem 3. *Suppose $f \in \mathbb{F}_q[X]$ is a polynomial for which $N_2(f) = q-1$, the expected value. Then*

$$\frac{q+1}{2} \le V(f) \le q - \frac{2(q-1)}{1+\sqrt{4q-3}}.$$

Several classes of polynomials which obtain the expected value for $N_2(f)$ are then described; these include the class of planar polynomials (for further definitions, see Section 3). Planar polynomials are closely related to affine planes [4, 6], semifields [3], and difference sets [7, 11]. Consequently, they have received a significant amount of attention. However, the bound given by Theorem 3 constitutes the first non-trivial upper bound obtained on the size of the image set of a planar function. We suspect that, for planar functions, our upper bound can still be improved as we do not utilise the full set of restrictions implied by the planar property. The lower bound is, for planar functions, tight, and has been derived previously by several authors, see [5, 9, 11]. Our result, in this sense, constitutes a generalisation of the respective results given in each of those three papers.

The paper is set out as follows. In the next section we prove Theorems 1 and 2. We also discuss briefly the connection between Theorem 2 and triangular numbers. In Section 3 we apply our results to polynomials over finite fields. The paper ends with some observations in arithmetic combinatorics and coding theory.

§ 2. Bounding $V(f)$ when $N_s(f)$ is known

For convenience, we set $N_s(f) = t$. By the definitions above,

$$\sum_{r=1}^{s-1} rM_r = n - t + \sum_{r=s}^{m} \left(P(r,s) - r\right) M_r. \tag{1}$$

(We note that, since the sum on the right is at least $m(m-2)$, we must have $\sum_{r=1}^{s-1} rM_r \geq \mathrm{Max}(0, n - t + m(m-2))$.) We may manipulate (1) as follows:

$$\begin{aligned}
\sum_{r=1}^{s-1} rM_r &= n - t + \sum_{r=s}^{m} \left(P(r,s) - r\right) M_r \\
&= n - t + (s! - s)M_s + \sum_{r=s+1}^{m} \left(P(r,s) - r\right) M_r \\
&\geq n - t + (s! - s)M_s + (s! - 1) \sum_{r=s+1}^{m} rM_r \\
&= n - t + (s! - s)M_s \\
&\quad + (s! - 1)\sum_{r=1}^{m} rM_r - (s! - 1)\sum_{r=1}^{s-1} rM_r - (s! - 1)sM_s \\
&= s!\, n - t + s!\,(1 - s)M_s - (s! - 1)\sum_{r=1}^{s-1} rM_r.
\end{aligned}$$

Rearranging, we find

$$\begin{aligned}
s!\, n - t &\leq s! \sum_{r=1}^{s-1} rM_r + s!\,(s-1)M_s \\
&\leq s!\,(s-1) \sum_{r=1}^{s-1} M_r + s!\,(s-1)M_s \\
&= s!\,(s-1) \sum_{r=1}^{s} M_r \\
&\leq s!\,(s-1)\, V(f),
\end{aligned}$$

which establishes the lower bound in Theorem 1. (We mention, in passing, that this proof is a generalisation of the lower bound obtained by Matthews and the first author [5]; it was that note that formed the motivation for this article.)

We now move to determine the upper bound. First, we note that $M_m > 0$, and so $P(m,s) \leq t$, which yields

$$m \leq t^{\frac{1}{s}} + O(t^{\frac{1}{s+1}}). \tag{2}$$

Now, we apply the definitions above to obtain

$$\begin{aligned} t &= N_s(f) \\ &= \sum_{r=s}^{m} P(r,s) M_r = \sum_{r=1}^{m} P(r,s) M_r \\ &\leq m \sum_{r=1}^{m} P(r-1, s-1) M_r \\ &\leq m \cdot P(m-2, s-2) \sum_{r=1}^{m} (r-1) M_r, \end{aligned}$$

from which we deduce

$$\sum_{r=1}^{m} (r-1) M_r \geq \frac{t}{m \cdot P(m-2, s-2)}. \tag{3}$$

Combining (2) and (3), we get

$$\sum_{r=1}^{m} (r-1) M_r \geq t^{\frac{1}{s}} - O(t^{\frac{1}{s+1}}). \tag{4}$$

We can now estimate $V(f)$ using this sum:

$$\begin{aligned} V(f) &= n - n + V(f) \\ &= n - \sum_{r=1}^{m} r M_r - \sum_{r=1}^{m} M_r \\ &= n - \sum_{r=1}^{m} (r-1) M_r \end{aligned}$$

Applying (4) yields

$$V(f) \leq n - t^{\frac{1}{s}} + O(t^{\frac{1}{s+1}}), \tag{5}$$

as claimed.

The proof of Theorem 2 is no more difficult; in fact, the lower bound is precisely that from before, while the upper bound follows from a careful re-working of the proof of the upper bound. We omit the details.

It is easy to see that, provided $N_2(f) < 2n$, this lower bound is tight, as one can easily construct functions that meet this bound. Set $N_2(f) = t$. Randomly choose t distinct elements $x_1, x_2, \ldots, x_t \in A$ and $t/2$ distinct elements $y_1, y_2, \ldots, y_{t/2} \in B$. For $1 \leq i \leq t/2$, assign $f(x_{2i-1}) = f(x_{2i}) = y_i$. At this point, $N_2(f) = t$, so that f must be 1-1 on $A \setminus \{x_1, \ldots, x_t\}$. It follows that $V(f) = \frac{t}{2} + n - t = n - \frac{t}{2}$, which is the lower bound.

It is clear from symmetry that $N_2(f) = t$ is necessarily even. Set $t = 2k$. Then the bounds read

$$n - k \leq V(f) \leq n - \frac{4k}{1 + \sqrt{8k+1}}.$$

It is natural to ask when is $\sqrt{8k+1} \in \mathbb{Z}$? Interestingly, $8k+1$ is a square precisely when k is a triangular number. In such cases, we have $k = u(u-1)/2$ for some integer u, $8k+1 = \delta^2$ where $\delta = 2u-1$, and the upper bound simplifies neatly to

$$V(f) \leq n - \frac{\delta - 1}{2} = n + 1 - u.$$

In all cases where k is a triangular number, there exist functions which attain this bound. To construct such a function, choose u elements $x_1, x_2, \ldots, x_u \in A$ and set $f(x_1) = f(x_2) = \cdots = f(x_u)$. Now set f to behave 1-1 on the remaining elements of A. It can be seen that $N_2(f) = 2k$ and that the upper bound is attained.

In all cases where k is not a triangular number, our upper bound is not exact. To make our upper bound tight, one needs to solve the following problem:

> Let $T_r = \binom{r}{2}$ for any $r \in \mathbb{N}$, and fix $k \in \mathbb{N}$. By a *triangular sum of length l for k* we mean any instance of the equation
>
> $$k = \sum_{i=1}^{l} T_{r_i},$$
>
> where $r_1 \geq r_2 \geq \cdots \geq r_l$. The *weight* of a given triangular sum is given by $-l + (\sum_{i=1}^{l} r_i)$. Given k, we define B_k to be the smallest weight among all triangular sums for k. Find a formula for B_k.

Clearly, when $k = T_u$, $B_k = u - 1$, but we do not know of a general formula for B_k. While Gauss famously proved that there exists a triangular sum for any k with length at most 3, it may not necessarily be the case that one such instance will provide the value for B_k. The connection to our bound should be clear: If $N_2(f) = 2k$, then $V(f) \leq n - B_k$, with equality always possible.

§ 3. Polynomials over finite fields and $N_2(f)$

We now look to apply these bounds on $V(f)$ to polynomials over finite fields. It is, of course, well known that every function over $\mathbb{F}_q$ can be represented uniquely, via Lagrange interpolation, by a polynomial of degree less than q. By the *reduced form* of a polynomial $f \in \mathbb{F}_q[X]$ we shall mean the polynomial $g(X)$ given by $g(X) = f(X) \bmod (X^q - X)$. A polynomial $f \in \mathbb{F}_q[X]$ is a *permutation polynomial* over $\mathbb{F}_q$ if $V(f) = q$.

Research concerning the value of $V(f)$ for polynomials over finite fields is extensive; we restrict ourselves to discussing a few outstanding general results. It is clear that, for lower bounds, there are obvious limits to the results you can expect to obtain – obviously $V(f) \geq 1$ with equality possible, while for polynomials of given degree d, $V(f) \geq 1 + \frac{q-1}{d}$ is clear. That said, we have the following deep result by Cohen [2] concerning the average lower bound of $V(f)$.

Theorem 3.1 (Cohen [2]). *Let $f \in \mathbb{F}_q[X]$ be of the form*

$$f(X) = X^d + \sum_{i=1}^{d-1} a_i X^i.$$

Let t be any integer such that $0 \leq t \leq d-2$ and let $a_{d-1}, \ldots, a_{d-t}$ be fixed. Define $v(d,t) = \sum V(f)/q^{d-t-1}$, where the sum is over all $a_1, \ldots, a_{d-t-1}$. Set $m = \lfloor (d-t)/2 \rfloor$. Then $v(d,t) > c(q,m)q$, where

$$c(q,m) = 1 - \left(\sum_{r=0}^{m} \binom{q}{r} (q-1)^{-r} \right)^{-1}.$$

Setting $t = d-2$ in Cohen's result, we find that, in particular, on average, $V(f) > \frac{q^2}{2q-1} > \frac{q}{2}$.

A specific lower bound was obtained by Wan, Shiue, and Chen [15] under an additional condition on the polynomial. For $f \in \mathbb{F}_q[X]$, define $u_p(f)$ to be the smallest positive integer k such that $\sum_{x \in \mathbb{F}_q} f(x)^k \neq 0$. If no such k exists, define $u_p(f) = \infty$.

Theorem 3.2 (Wan, Shiue, Chen [15]). *If $u_p(f) < \infty$, then $V(f) \geq u_p(f) + 1$.*

The authors note that $u_p(f) \geq \lfloor \frac{q-1}{\mathrm{Degree}(f)} \rfloor$, so that under the conditions, their bound is at least as good as the obvious bound noted above.

In terms of an upper bound, there is the following general bound by Wan [14], given in terms of the degree of the polynomial.

Theorem 3.3 (Wan [14])**.** *Let $f \in \mathbb{F}_q[X]$. If f is not a permutation polynomial over $\mathbb{F}_q$, then*

$$V(f) \leq q - \left\lfloor \frac{q-1}{\mathrm{Degree}(f)} \right\rfloor .$$

A better bound was obtained in [15] using p-adic techniques. To avoid unnecessary technical details, we simply refer the interested reader to [15], Theorem 3.1.

Integral to applying our bounds is having knowledge of $N_s(f)$ for some s. For simplicity, we only discuss the case $s = 2$ here. We do not feel this is particularly limiting as, of the values of $N_s(f)$, knowledge of $N_2(f)$ seems most likely. We approach this issue by first establishing the expected value of $N_2(f)$ for any polynomial $f \in \mathbb{F}_q[X]$ and applying our bounds to polynomials with this expected value. We then consider classes of polynomials which meet this expected value.

Denote the standard trace mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$ by Tr. Let ω be a primitive pth root of unity. Recall that the canonical additive character, χ_1, of $\mathbb{F}_q$ is defined by $\chi_1(x) = \omega^{\mathrm{Tr}(x)}$ for any $x \in \mathbb{F}_q$, and that all additive characters of $\mathbb{F}_q$ are given by $\chi_h(x) = \chi_1(hx)$ for any $h \in \mathbb{F}_q$. The following result is a straight generalisation of a result of Carlitz [1].

Lemma 3.4. *Given a random polynomial $f \in \mathbb{F}_q[X]$, the expected value of $N_2(f)$ is $q-1$. Equivalently, for any $f \in \mathbb{F}_q[X]$,*

$$\sum_{a \in \mathbb{F}_q} N_2(f(X) + aX) = q(q-1). \tag{6}$$

Proof. Fix a polynomial $f \in \mathbb{F}_q[X]$. By the definitions above,

$$\begin{aligned} q(N_2(f) + q) &= q(|\{(x,y) : f(x) = f(y), x, y \in \mathbb{F}_q, x \neq y\}| \\ &\quad + |\{(x : f(x) = f(x), x \in \mathbb{F}_q\}|) \\ &= \sum_{h \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi_h(f(x) - f(y)). \end{aligned}$$

To generate our average value for $N_2(f)$, we consider the average over the set $\{f(X) + aX : a \in \mathbb{F}_q\}$. We have

$$\begin{aligned} &\sum_{a \in \mathbb{F}_q} q(N_2(f(X) + aX) + q) \\ &\qquad = \sum_{a \in \mathbb{F}_q} \sum_{h \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi_h(f(x) - f(y) + a(x-y)) \\ &\qquad = q^3 + \sum_{h \in \mathbb{F}_q^\star} \sum_{x,y \in \mathbb{F}_q} \chi_h(f(x) - f(y)) \sum_{a \in \mathbb{F}_q} \chi_h(a(x-y)) \\ &\qquad = q^3 + \sum_{h \in \mathbb{F}_q^\star} \sum_{x \in \mathbb{F}_q} q \\ &\qquad = q^3 + q^2(q-1), \end{aligned}$$

where, in the second to last line, we have exploited the fact $\sum_{a \in \mathbb{F}_q} \chi(a(x-y)) = 0$ unless $x = y$. Comparing the left and right hand sides yields

$$\sum_{a \in \mathbb{F}_q} N_2(f(X) + aX) = q(q-1). \tag{7}$$

The claimed expected value of $N_2(f)$ now follows at once, for we can, of course, partition the set of polynomials into equivalence classes, with two polynomials being equivalent if they differ only by a linear term aX: the average value of $N_2(f)$ for the polynomials in any equivalence class is $q-1$ by (7). □

Theorem 3 now follows at once from Theorem 2 and Lemma 3.4.

Now suppose $f \in \mathbb{F}_q[X]$ is a polynomial for which $N_2(f) = q-1$, the expected value. For our lower bound, we find $V(f) \geq \frac{q+1}{2}$, which is more or less the same as that obtained by Cohen's result. In the other direction, applying our upper bound to f, we find

$$V(f) \leq q - \frac{2(q-1)}{1+\sqrt{4q-3}}.$$

However, this cannot be compared directly to the result of Wan, for we do not know if $N_2(f) = q-1$ has any direct implication on $\mathrm{Degree}(f)$.

Given Lemma 3.4, one obvious question arises: Is it possible to describe classes of polynomials for which the expected value for $N_2(f)$ is obtained? Are there natural conditions on f which force $N_2(f) = q-1$? We now discuss, for q odd, several such conditions (the case q even is clearly impossible for $N_2(f)$ is necessarily even).

For any $a \in \mathbb{F}_q^\star$, we define the *difference polynomial*, $\Delta_{f,a}(X) = \Delta_a(X)$, to be the polynomial given by $\Delta_a(X) = f(X+a) - f(X)$. A polynomial $f \in \mathbb{F}_q[X]$ is *planar* over $\mathbb{F}_q$ if, for every $a \in \mathbb{F}_q^\star$, the polynomial $\Delta_a(X)$ is a permutation polynomial over $\mathbb{F}_q$. An equivalent definition for planarity is that $|S_h(f(X)+aX)| = |\sum_{x\in\mathbb{F}_q} \chi_h(f(x)+ax)| = \sqrt{q}$ for all $a, h \in \mathbb{F}_q$, $h \neq 0$.

Consider the following conditions on a polynomial $f \in \mathbb{F}_q[X]$:

C_1. f is planar over $\mathbb{F}_q$.

C_2. For $h \in \mathbb{F}_q^\star$, $|S_h(f)| = |\sum_{x\in\mathbb{F}_q} \chi_h(f(x))| = \sqrt{q}$.

C_3. For all $a \in \mathbb{F}_q^\star$, the polynomial $\Delta_{f,a}(X)$ has a unique root.

C_4. $N_2(f) = q-1$.

Clearly, $C_1 \to C_2$ and $C_1 \to C_3 \to C_4$. It is shown in the proof of [5], Theorem 1, that $C_2 \to C_4$, while a counting argument, also given in [5], shows $C_1 \not\equiv C_2$.

The relationship between C_2 and C_3 is less clear. Computations show that they are almost certainly inequivalent for sufficiently large q. Over $\mathbb{F}_3$, they are equivalent; over $\mathbb{F}_5$, they are not, though $(C_2 \wedge C_3) \to C_1$. For $q \in \{7, 9\}$, they are inequivalent, and

- there exist polynomials which satisfy both C_2 and C_3 but not C_1; for example, $f(X) = X^4 + 2X^2 \in \mathbb{F}_7[X]$; and
- there exist polynomials which satisfy one or other but not both conditions; for example, with g a primitive element of $\mathbb{F}_9$, $X^7 + gX^2$ satisfies C_2 but not C_3, while $X^8 + gX^2$ satisfies C_3 but not C_2.

This also shows $C_2 \not\equiv C_4$ and $C_3 \not\equiv C_4$. We suspect that the following statement is true, though we have no direct idea of how to establish it.

Conjecture 3.5. *For any finite field of any characteristic, the number of polynomials satisfying C_3 is greater than or equal to the number of polynomials satisfying C_2.*

§ 4. Two further settings where the bounds apply

We end by describing two settings where our results can be applied, and where we suspect some refinements of our methods might lead to stronger results than those we give here.

§ 4.1. Arithmetic combinatorics

Here, we present a setting where N_2 arises rather naturally. Let G be a (not necessarily abelian) group. For subsets $A, B \subset G$, define the product set of A and B to be

$$A \cdot B = \{ab : a \in A, b \in B\}.$$

Much interest revolves around the relative sizes of A, B, and $A \cdot B$. Some examples are the Cauchy-Davenport Theorem, the Plünnecke-Rusza inequalities, and Freiman's Theorem; see the books by Nathanson [10] or Tao and Vu [13]. One useful tool for these questions is the concept of energy. Various types of energy bounds have been the key ingredient in many recent results, such as the current best known sums and products bound due to Solymosi [12].

Given G, A, and B as above, we define the multiplicative energy, $E(A, B)$, to be

$$E(A, B) = |\{(a, a', b, b') \in A \times A \times B \times B : ab = a'b'\}|.$$

If we consider $f : A \times B \to G, f : (a, b) \mapsto ab$, we get a very close relationship between $N_2(f)$ and $E(A, B)$, namely

$$N_2(f) = E(A, B) - |A| \cdot |B|,$$

which we obtain by removing the "diagonal" elements of the form (a, a, b, b) from the energy count. With this in mind, the following is a direct application of Theorem 2.

Corollary 4.1. *Let G be a group, $A, B \subset G$ and set $n = |A| \cdot |B|$. Then we have*

$$\frac{3n - E(A, B)}{2} \leq |A \cdot B| \leq n - \frac{2(E(A, B) - n)}{1 + \sqrt{4(E(A, B) - n) + 1}} \tag{8}$$

Notice that these bounds are most effective when energy is small.

§ 4.2. Coding theory

Our second setting is in coding theory. Much is known about the interplay between the redundancy of a given code and the amount of information that can be communicated per unit time; see Hall's notes on coding [8], for a good introduction. Here, we investigate messages transmitted through a noisy medium.

Consider a function $f : \mathcal{C} \to \mathcal{M}$, where $\mathcal{C}$ is the codespace and $\mathcal{M}$ is the message space. In order to increase the likelihood that a message is decoded properly, even with errors in transmission, we will often give a single message word more than one code word. That is, it will often be the case that $f(c) = f(c')$ for distinct $c, c' \in \mathcal{C}$. By definition, $V(f)$ will be precisely the number of distinct words in $\mathcal{M}$, and $N_2(f)$ will be the number of times that two code words represent the same message.

There are situations in which one has a particularly uneven message space, where a small number of messages have high priority, and need the best chances of being decoded correctly, while all remaining messages are less important, and their incorrect decodings would have very little consequence. For example, a message space between fire towers in a forest could have a small number of special words about the existence or severity of a fire, and the other words could describe other, less important details, like the weather, in the case that there is no fire. Similar applications exist in a variety of different contexts such as operations in hostile environments. In such situations, an application of Theorem 2 yields the following.

Corollary 4.2. *In a code with a codespace $\mathcal{C}$, a message space $\mathcal{M}$, an assignment function $f : \mathcal{C} \to \mathcal{M}$, and $t = |\{f(c) = f(c') : c, c' \in \mathcal{C}, c \neq c'\}|$, we have*

$$n - \frac{t}{2} \leq |\mathcal{C}| \leq n - \frac{2t}{1 + \sqrt{4t + 1}}$$

In this setting, our bounds can be viewed as providing a guide for balancing between levels of redundancy and flexibility within the code.

References

[1] L. Carlitz, *On the number of distinct values of a polynomial with coefficients in a finite field*, Proc. Japan Acad. **31** (1955), 119–120.

[2] S.D. Cohen, *The values of a polynomial over a finite field*, Glasgow Math. J. **14** (1973), 205–208.

[3] R.S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math. **217** (2008), 282–304.

[4] R.S. Coulter and R.W. Matthews, *Bent polynomials over finite fields*, Bull. Austral. Math. Soc. **56** (1997), 429–437.

[5] ______, *On the number of distinct values of a class of functions over a finite field*, Finite Fields Appl. **17** (2011), 220–224.

[6] P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.

[7] C. Ding and J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), 1526–1535.

[8] J. Hall, *Notes on Coding Theory*, http://www.mth.msu.edu/∼hall/classes/codenotes/coding-notes.html, 2010.

[9] G.M. Kyureghyan and A. Pott, *Some theorems on planar mappings*, Arithmetic of Finite Fields: Proceedings of the 2nd International Workshop, WAIFI 2008 (J. von zur Gathen, J.L. Imanã, and C.K. Koç, eds.), Lecture Notes in Computer Science, vol. 5130, 2008, pp. 117–122.

[10] M. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, 1996.

[11] W. Qiu, Z. Wang, G. Weng, and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr. **44** (2007), 49–62.

[12] J. Solymosi, *Bounding multiplicative energy by the sumset*, Adv. Math. **222** (2009), 402–408.

[13] T. Tao and V. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.

[14] D. Wan, *A p-adic lifting lemma and its applications to permutation polynomials*, Finite Fields, Coding Theory, and Advances in Communications and Computing (New York), Lecture Notes in Pure and Applied Mathematics, vol. 141, Marcel Dekker, 1993, pp. 209–216.

[15] D. Wan, P.J-S. Shiue, and C-S. Chen, *Value sets of polynomials over finite fields*, Proc. Amer. Math. Soc. **119** (1993), 711–717.