Constructing Permutation Arrays from Semilinear Groups

Avi Levy

2/17/2013

Contents

1 Introduction

This is a preliminary writeup of my work with the semilinear groups. These groups yield new permutation arrays with large pairwise Hamming distances. Their properties are well-understood, which allows the minimal pairwise Hamming distance to be obtained without resorting to direct computation.

2 Overview and Notation

2.1 Finite Fields

Given $q = p^n$, a power of a prime, call the unique field with q elements $\mathbb{F}_q$.

$$\mathbb{F}_q = \{0, 1, g, g^2, \cdots, g^{q-2}\}$$

where g is any generator of F_q.

2.2 Permutation Polynomials

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a polynomial function with coefficients in $\mathbb{F}_q$. If f is one-to-one, then f permutes the elements of $\mathbb{F}_q$. In this case, f is called a *permutation polynomial*, and the permutation corresponding to f is:

$$\sigma_f : x \to f(x)$$

2.3 Classical Groups

There are four families of groups that we are concerned with in this paper.

- $AGL(n, \mathbb{F})$: affine general linear group of dimension n over the field $\mathbb{F}$.
- $A\Gamma L(n, \mathbb{F})$: affine general semilinear group of dimension n over $\mathbb{F}$.
- $PGL(n, \mathbb{F})$: projective general linear group of dim n over $\mathbb{F}$.
- $P\Gamma L(n, \mathbb{F})$: projective general semilinear group of dim n over $\mathbb{F}$.

Note 2.1. *We will use shorthand like Group*(n, q) *as a synonym for Group*$(n, \mathbb{F}_q)$.

2.4 Hamming distance and Permutation Arrays

In this section, all permutations act on n elements.

The Hamming distance between two permutations is the number of places in which they differ. Let S and T be sets of permutations. Then $hd(S,T)$ denotes the minimal Hamming distance between distinct elements of S and T.

If $hd(S,S) = d$, then the set S is called a permutation array of Hamming distance d. We say that S is an $M(n,d)$ in this case.

3 Constructions

3.1 $AGL(1, \mathbb{F}_q)$

$AGL(1, \mathbb{F}_q) = AGL(1,q)$ is the group of linear polynomials:

$$AGL(1,q) = \{ax + b | a, b \in \mathbb{F}_q, a \neq 0\}$$

The group operation is function composition:

$$(ax + b) \circ (cx + d) = a(cx + d) + b = acx + (b + d)$$

In fact, all the groups in this paper are presented as sets of polynomials, and the group operation will always be function composition. This group is sharply $2-$transitive and yields an optimal $M(q, q-1)$ with $q(q-1)$ elements.

3.2 $A\Gamma L(1, \mathbb{F}_q)$

Recall that $q = p^n$. Consider the permutation polynomial

$$\mathrm{frob}(x) = x^p$$

called the Frobenius automorphism, which is semilinear in the following sense:

$$\mathrm{frob}(x + y) = (x + y)^p \equiv x^p + y^p = \mathrm{frob}(x) + \mathrm{frob}(y)$$

Starting from $AGL(1,q)$, append $\mathrm{frob}(x)$ and take the group closure, yielding:

$$A\Gamma L(1,q) = \{ax^{p^i} + b | a, b \in \mathbb{F}_q, a \neq 0, 0 \leq i < n\}$$

This group has $nq(q-1)$ elements.

3.3 $PGL(2, \mathbb{F}_q)$

Projective groups act on a "point at infinity". To accommodate this case, form the set $\mathbb{P}^1(\mathbb{F}_q) = \{\infty\} \cup \mathbb{F}_q$. Then $PGL(2, q)$ is constructed as:

$$PGL(2, q) = \left\{ \frac{ax + b}{cx + d} \middle| a, b, c, d \in \mathbb{F}_q, ad \neq bc \right\}$$

These are called *fractional linear* functions. Note that cancelling common factors from the numerator and denominator leaves the function unchanged, so there are only 3 degrees of freedom among (a, b, c, d).

Suppose $h(x) \in PGL(2, q)$. If $h(x)$ is written as $h(x) = \frac{ax+b}{cx+d}$, then h acts on $\mathbb{P}^1(\mathbb{F}_q)$ as follows:

$$h(x) = \begin{cases} \frac{a}{c} & \text{if } x = \infty \\ \infty & \text{if } x = -\frac{d}{c} \\ \frac{ax+b}{cx+d} & \text{otherwise} \end{cases}$$

The group $PGL(2, q)$ is 3−transitive and yields an optimal $M(q + 1, q - 1)$ with $(q + 1)q(q - 1)$ elements.

3.4 $P\Gamma L(1, \mathbb{F}_q)$

In analogy with $A\Gamma L$, start from $PGL(2, q)$ then append frob(x) and take the group closure.

$$P\Gamma L(2, q) = \left\{ \frac{ax^{p^i} + b}{cx^{p^i} + d} \middle| a, b, c, d \in \mathbb{F}_q, ad \neq bc, 0 \leq i < n \right\}$$

This group has $n(q + 1)q(q - 1)$ elements.

4 Hamming Distance Computations

4.1 Preliminaries

In this section, all permutations act on n elements.

Let G be a set of permutations that is also a permutation group. The goal in this section is to compute $hd(G, G)$, and thereby interpret G as a permutation array $M(n, d)$.

Lemma 4.1. *$hd(\{\sigma\tau\}, \{\sigma\rho\}) = hd(\{\tau\}, \{\rho\})$*

Proof. $\sigma\tau(x) = \sigma\rho(x) \iff \tau(x) = \rho(x)$ □

Lemma 4.2. *$hd(G, G) = hd(\{e\}, G)$, where e is the identity permutation*

Proof. Pick $a, b \in G$. Then $hd(a, b) = hd(e, a^{-1}b)$ so the result follows □

Lemma 4.3. *Suppose N is a normal subgroup of a finite group, G. If $\{a_i\}_{i\in I}$ is a set of coset representatives of N, then*

$$hd(G, G) = \min_{i\in I} hd(\{a_i\}, N)$$

Proof. Since N is normal, the set $\{a_i^{-1}\}$ is also a set of coset representatives. Therefore, $G = \bigcup_{i\in I} a_i^{-1}N$, so the Hamming distance is computed as follows:

$$hd(G, G) = hd(\{e\}, G) = \min_{i\in I} hd(\{e\}, a_i^{-1}N) = \min_{i\in I} hd(\{a_i\}, N)$$

where Lemma 4.1 and Lemma 4.2 have been applied. □

Using the following lemma, one can compute the Hamming distance simply by counting roots of polynomials.

Lemma 4.4. *For any polynomial $f \in \mathbb{F}_q[x]$, let $r(f)$ denote the number of distinct roots of $f(x)$ in $\mathbb{F}_q$. Then for any distinct pair of polynomials $g, h \in \mathbb{F}_q[x]$ we have*

$$hd(\{g\}, \{h\}) = n - r(g - h)$$

Proof. $g(x) \neq h(x)$ is equivalent to saying x is not a root of $g - h$ □

4.2 $A\Gamma L$

Theorem 4.5. *$A\Gamma L(1, q)$ is an $M\left(q, q - p^{n^*}\right)$, where n^* denotes the largest proper factor of n.*

Proof. Let $G = A\Gamma L(1, q)$ and let $N = AGL(1, q)$. Note that N is normal in G by construction. To proceed, apply Lemma 4.3 with representatives $\{x^{p^i}\}_{i=0}^{n-1}$ to G, then use Lemma 4.4:

$$\begin{aligned} hd(G, G) &= \min_{0\leq i<n} hd(\{x^{p^i}\}, N) \\ &= q - \max_{\substack{i<n \\ g\in N}} r\left(x^{p^i} - g(x)\right) \end{aligned}$$

By Theorem 5.1,

$$\max_{g \in N} r\left(x^{p^i} - g(x)\right) = r\left(x^{p^i} - x\right)$$

Now by Theorem 5.2,

$$r\left(x^{p^i} - x\right) = p^{\gcd(i,n)}$$

Putting all of our results together,

$$\begin{aligned} hd(G,G) &= q - \max_{\substack{i<n \\ g \in N}} r\left(x^{p^i} - g(x)\right) \\ &= q - \max_{i<n} p^{\gcd(i,n)} \\ &= q - p^{n^*} \end{aligned}$$

Thus $A\Gamma L(1,q)$ is an $M\left(q, q-p^{n^*}\right)$. $\square$

Corollary 4.6. *Suppose $q = 2^p$ where p is prime. Then there exists an $M(q, q-2)$ of size $pq(q-1)$.*

4.3 $P\Gamma L$

Theorem 4.7. *$P\Gamma L(2,q)$ is an $M\left(q+1, q-p^{n^*}\right)$, where n^* denotes the largest proper factor of n.*

Proof. Let $G = P\Gamma L(2,q)$ and $H = \{g \in G | g(\infty) = \infty\}$. H can be identified with $A\Gamma L(1,q)$ by means of the isomorphism $i : AGL(1,q) \to H$

$$i(g)(x) = \begin{cases} g(x) & \text{if } x \in \mathbb{F}_q \\ \infty & \text{if } x = \infty \end{cases}$$

Suppose $g(x), h(x)$ are distinct elements of G. If $g(x) \neq h(x)$ for all x, then $hd(\{g\},\{h\}) = q+1$. Otherwise, pick a point y such that

$$g(y) = h(y) = w$$

Choose the following elements of G:

$$\tau_1(x) = \begin{cases} \dfrac{1}{x-w} & \text{if } w \in \mathbb{F}_q \\ x & \text{if } w = \infty \end{cases}$$

$$\tau_2(x) = \begin{cases} \dfrac{yx+1}{x} & \text{if } y \in \mathbb{F}_q \\ x & \text{if } y = \infty \end{cases}$$

Let $g' = \tau_1 \circ g \circ \tau_2, h' = \tau_1 \circ h \circ \tau_2$. Then $\tau_1(g(\tau_2(\infty))) = \infty$ and likewise for h, so $g', h' \in H$.

By Lemma 4.1, $hd(g', h') = hd(g, h)$. Moreover, the isomorphism i preserves Hamming distance so

$$hd(g', h') = hd\left(i^{-1}(g'), i^{-1}(h')\right)$$

But $i^{-1}(g'), i^{-1}(h') \in A\Gamma L(1, q)$, so by Theorem 4.7

$$hd\left(i^{-1}(g'), i^{-1}(h')\right) \geq q - p^{n^*}$$

Therefore $hd(g, h) \geq q - p^{n^*}$, so $P\Gamma L(2, q)$ is an $M\left(q+1, q - p^{n^*}\right)$. □

Corollary 4.8. *Let $q = 2^p$ where p is prime. Then there exists an $M(q+1, q-2)$ of size $p(q+1)q(q-1) = O\left(q^3 \log q\right)$.*

This improves upon the best current computational results.

5 Root-counting Results

Theorem 5.1. $r\left(x^{p^i} + ax + b\right) \leq r\left(x^{p^i} - x\right)$

Proof. Let $p_1(x) = x^{p^i} + ax + b, p_2(x) = x^{p^i} + ax$ and $p_3(x) = x^{p^i} - x$. We will show that $r(p_1) \leq r(p_2) \leq r(p_3)$.

First, suppose p_1 has at least one root (if not, the result holds trivially). Then pick a root of p_1 and call it y. Observe that for any root y_i of p_1, we have

$$\begin{aligned} p_2(y_i - y) &= (y_i - y)^{p^i} + a(y_i - y) \\ &= y_i^{p^i} - y^{p^i} + a(y_i - y) \\ &= p_1(y_i) - p_1(y) = 0 \end{aligned}$$

Thus $y_1 - y$ is a root of p_2. Since the mapping $y_1 \to y_1 - y$ is a bijection, this shows that $r(p_1) = r(p_2)$ whenever p_1 has at least one root. Thus in general, $r(p_1) \leq r(p_2)$.

To show that $r(p_2) \leq r(p_3)$, we will instead show that $r\left(p_2^\circ\right) \leq r\left(p_3^\circ\right)$, where

$$p_2^\circ = \frac{p_2}{x} = x^{p^i-1} + a \qquad p_3^\circ = \frac{p_3}{x} = x^{p^i-1} - 1$$

If $p_2^\circ(0) = 0$, then $p_2^\circ = x^{p^i-1}$ so $r\left(p_2^\circ\right) = 1 \leq r\left(p_3^\circ\right)$, since p_3° has the trivial root 1.

Otherwise, zero is not a root of p_2°. Suppose p_2° has at least one root (otherwise the result follows trivially). Then pick a root of p_2° and call it z. As z_i ranges over all roots of p_2°, map $z_i \to \frac{z_i}{z}$.

$$\begin{aligned} p_3^\circ\left(\frac{z_1}{z}\right) &= \left(\frac{z_1}{z}\right)^{p^i-1} - 1 \\ &= \left(\frac{z_1^{p^i-1}}{z^{p^i-1}}\right) - 1 \\ &= \frac{-a}{-a} - 1 = 0 \end{aligned}$$

so $\frac{z_i}{z}$ is a root of p_3°. Since the map is a bijection, this establishes $r\left(p_2^\circ\right) = r\left(p_3^\circ\right)$ under the hypotheses on p_2. It follows that in general, $r(p_2) \leq r(p_3)$. Thus, $r(p_1) \leq r(p_3)$ as we intended to show.

$\square$

Theorem 5.2. $r\left(x^{p^i} - x\right) = p^{\gcd(i,n)}$

Proof. Let S be the set of roots of $x^{p^i} - x$. First, observe that the S forms a finite field. This follows by checking closure under addition, multiplication, and division - in a similar manner as in the previous proof.

Thus S is a subfield of $\mathbb{F}_q$. In particular, $S = \mathbb{F}_{p^j}$ where $j|n$.

Now consider the extension of $x^{p^i} - x$ into its splitting field. In this larger field, the expanded root set forms $\mathbb{F}_{p^i}$. But this root set contains S as a subset, so that S is also a subfield of $\mathbb{F}_{p^i}$. Thus $j|i$.

Since subfields are ordered by inclusion, S is the maximal subfield satisfying the above constraints. This implies that j is the maximal integer satisfying $j|n$ and $j|i$ simultaneously. So $j = \gcd(i,n)$ which shows $r\left(x^{p^i} - x\right) = |S| = p^j = p^{\gcd(i,n)}$ $\square$

Theorem 5.3 (Special case of Quan's Conjecture)**.** *The equation*

$$\frac{ax+b}{cx+d} = x^p$$

has at most $p+1$ solutions in $\mathbb{F}_q \cup \{\infty\}$, where $a, b, c, d \in \mathbb{F}_q$.

Proof. Let x_i be a solution of the equation. Then x_i is a root of the following polynomial:

$$cx^{p+1} + dx^p - ax - b$$

By the Fundamental Theorem of Algebra, this polynomial has at most $p+1$ roots. $\square$

Corollary 5.4. *Let $G = PGL(2, q)$ and f be the Frobenius permutation. Then $hd(G, \{f\}) = q - p$.*

Proof. Choose $g(x) \in G$. Then by Lemma 4.4, $hd(\{g\}, \{f\}) = q + 1 - s$, where s is the number of solutions of the equation

$$\frac{ax+b}{cx+d} = x^p$$

By Theorem 5.3, $s \leq p+1$.

Therefore, $hd(\{g\}, \{f\}) \geq (q+1) - (p+1) = q - p$. When $g(x) = x$, equality holds. It follows that $hd(G, \{f\}) = q - p$. $\square$

Corollary 5.5. *Quan's Conjecture holds for $M(2^n+1, 2^n-1)$, with backoff distance* 1*. Quan's Conjecture holds for $M(3^n+1, 3^n-1)$, with backoff distance* 2*.*

Proof. Quan's Conjecture relates to the coset method. Start with $G = PGL(2, q) = M(q+1, q-1)$ and generate random permutations, σ, on $q+1$ elements. If σ has minimal Hamming distance $q-1-d$ from all elements of G, then the coset σG is said to have "backed off by d" from G.

Quan's Conjecture states that when $d \geq 2$, this procedure generates at least one such permutation, σ. The previous results show that Quan's Conjecture holds for $q = 2^n$ and $q = 3^n$, by choosing σ to be the Frobenius automorphism.

Note: An even simpler proof establishes Quan's Conjecture for $M(2^n, 2^n-1)$ and $M(3^n, 3^n-1)$. $\square$

6 Conclusions

Need to write up properly. I want to emphasize that these are novel lower bounds, that this leads to a family with asymptotic growth $O(n^3 \log n)$, and that this can be used as a starting point for a refined coset method.

Also, it may be worth looking for other areas where my technical results about roots of polynomials can be applied.

7 Bibliography

Need to fix up. Useful references included:

Sudborough et. al. paper

Chu et. al. paper

Smith and Montemanni paper

Lidl and Niederreiter, “Introduction to finite fields and their applications”

Gruenberg and Weir, “Linear Geometry (explanation of semilinear groups)”

Rotman, “The Theory of Groups: An Introduction”

James, “The Representation Theory of the Symmetric Group”