DEPARTMENT OF MATHEMATICS

TECHNICAL REPORT

THE AFFINITY OF A PERMUTATION OF A FINITE VECTOR SPACE

DR. W. EDWIN CLARK
DR. XIANG-DONG HOU
DR. ALEC MIHAILOVS

JULY 2004

No. 2004-3

TENNESSEE TECHNOLOGICAL UNIVERSITY
Cookeville, TN 38505

THE AFFINITY OF A PERMUTATION OF A FINITE VECTOR SPACE

W. EDWIN CLARK, XIANG-DONG HOU*, AND ALEC MIHAILOVS

Abstract. For a permutation f of an n-dimensional vector space V over a finite field of order q we let k-affinity(f) denote the number of k-flats X of V such that $f(X)$ is also a k-flat. By k-spectrum(n, q) we mean the set of integers k-affinity(f) where f runs through all permutations of V. The problem of the complete determination of k-spectrum(n, q) seems very difficult except for small or special values of the parameters. However, we are able to establish that $0 \in k$-spectrum(n, q) in the following cases: (i) $q \geq 3$ and $1 \leq k \leq n-1$; (ii) $q = 2$, $3 \leq k \leq n-1$; (iii) $q = 2$, $k = 2$, $n \geq 3$ odd. The maximum of k-affinity(f) is, of course, obtained when f is any semi-affine mapping. We conjecture that the next to largest value of k-affinity(f) is when f is a transposition and we are able to prove this when $q = 2$, $k = 2$, $n \geq 3$ and when $q \geq 3$, $k = 1$, $n \geq 2$.

1. Introduction

It is a classical result, see, *e.g.*, Snapper and Troyer [9], that if V is an n-dimensional vector space over a field F such that $n \geq 2$ and $|F| \geq 3$ then a bijection $f : V \to V$ which takes 1-flats to 1-flats is a semi-affine mapping, that is, there is an automorphism σ of F, an additive automorphism $g : V \to V$ and a vector $b \in V$ such that $g(\alpha x) = \sigma(\alpha)g(x)$ for all $x \in V$, $\alpha \in F$ and

$$f(x) = g(x) + b \qquad \text{for all } x \in V.$$

We remark that if the automorphism σ is the identity then g is just a non-singular linear mapping and f is said to be affine. This will be the case when F has no non-trivial automorphisms.

The above result is not true when $|F| = 2$. In this case, a 1-flat in V is just a two element subset, hence every permutation of V takes all 1-flats to 1-flats. However, the above result has an easy analog for the case $|F| = 2$: A permutation of V which takes every 2-flat to a 2-flat must be affine (cf. [5]).

Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. In this paper, we are concerned with permutations of $\mathbb{F}_q^n$. Let $\mathrm{Per}(\mathbb{F}_q^n)$ denote the group of all permutations of $\mathbb{F}_q^n$. Recall that a k-flat (or k-dimensional affine subspace) X in $\mathbb{F}_q^n$ is a coset $U + x$ of a k-dimensional subspace U of $\mathbb{F}_q^n$.

Definition 1.1. For $f \in \mathrm{Per}(\mathbb{F}_q^n)$ and $0 \leq k \leq n$ we define k-affinity(f) to be the number of k-flats X in $\mathbb{F}_q^n$ such that $f(X)$ is a k-flat. We define k-coaffinity(f) to be the number of k-flats X in $\mathbb{F}_q^n$ such that $f(X)$ is not a k-flat.

Key words and phrases. affine, almost perfect nonlinear, finite field, flat, general affine group, permutation, semi-affine group, vector space.

* Partially supported by NSA grant MDA 904-02-1-0080.

It is well known that the number of k-dimensional subspaces of $\mathbb{F}_q^n$ is given by the q-binomial coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q^1-1)}$$

and the number of k-flats in $\mathbb{F}_q^n$ is given by

$$q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q.$$

It follows that

$$k\text{-affinity}(f) + k\text{-coaffinity}(f) = q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$$

for all permutations f of $\mathbb{F}_q^n$ and all $0 \le k \le n$.

The cases $k = 0$ and $k = n$ are trivial and we shall ignore them.

Definition 1.2. For integers $0 \le k \le n$ and prime power q, we define k-spectrum(n,q) to be the set of values k-affinity(f) for all $f \in \mathrm{Per}(\mathbb{F}_q^n)$.

The present paper is a continuation of the second author's work [5]. In [5], the notion of 2-affinity of permutations of $\mathbb{F}_2^n$ was implicitly introduced and permutations of $\mathbb{F}_2^n$ with 2-affinity 0 were studied. We point out that a permutation $f \in \mathrm{Per}(\mathbb{F}_2^n)$ with 2-affinity$(f) = 0$ is an *almost perfect nonlinear* (APN) permutation. APN permutations arose in cryptography as a means to resist the differential cryptanalysis [2, 8]. APN permutations of $\mathbb{F}_2^n$ are known to exist for odd $n \ge 3$ ([2, 7]) and not to exist for $n = 4$ ([5]). Their existence for even $n \ge 6$ is an open question. For recent work on APN permutations and related topics, we refer the reader to [1, 2, 3, 4, 5]. However, we must remind the reader that this paper is not a response to any problem from cryptography. Rather, it is a pure mathematical exploration.

Our primary interest is the set k-spectrum(n,q). In particular, we would like to know if $0 \in k$-spectrum(n,q) and what the second largest number in k-spectrum(n,q) is. (The largest number in k-spectrum(n,q) is, of course, $q^{n-k}\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$.) In Section 2, we show that with few exceptions, $0 \in k$-spectrum(n,q). The result of Section 2 relies on an inequality involving q-binomial coefficients whose proof is given in Section 3. Hou [5] showed that 2-spectrum(4,2) is

$$\{5-20, 22, 24-26, 28, 30, 32, 36, 38, 44, 48, 52, 56, 76, 84, 140\}$$

where $a - b$ denotes all integers from a to b. More examples of k-spectra are given in Section 4. In Section 5, we determine $(n-1)$-spectrum$(n,2)$ completely. These examples and results led to the conjecture that the next to largest k-affinity is that of a transposition. We compute the k-affinity $T(n,k,q)$ of a transposition in $\mathrm{Per}(\mathbb{F}_q^n)$ in Section 6. We call this conjecture *The Threshold Conjecture* since it says that if k-affinity$(f) > T(n,k,q)$ then f takes every k-flat to a k-flat. We prove that the conjecture holds for $q = 2$, $k = 2$, $n \ge 3$ in Section 7 and for $q > 2$, $k = 1$, $n \ge 2$ in Section 8.

2. When k-affinity$(f) = 0$

It should be noted that there appears to be no clear relationship between k-affinity(f) and ℓ-affinity(f). For example, there are permutations f_1, f_2, f_3, f_4 in

$\mathrm{Per}(\mathbb{F}_3^3)$ such that

$$\begin{aligned}
&1\text{-affinity}(f_1) = 1 \text{ and } 2\text{-affinity}(f_1) = 0\\
&1\text{-affinity}(f_2) = 0 \text{ and } 2\text{-affinity}(f_2) = 1\\
&1\text{-affinity}(f_3) = 0 \text{ and } 2\text{-affinity}(f_3) = 0\\
&1\text{-affinity}(f_4) = 1 \text{ and } 2\text{-affinity}(f_4) = 1
\end{aligned}$$

In the following theorem, we see that with few exceptions there is a permutation $f \in \mathrm{Per}(\mathbb{F}_q^n)$ such that simultaneously k-affinity$(f) = 0$ for all $1 \leq k \leq n-1$.

Theorem 2.1.

(i) *If $q = 2$ and $n \geq 3$ is odd, there exists $f \in \mathrm{Per}(\mathbb{F}_2^n)$ such that* 2-affinity$(f) = 0$.

(ii) *If $q = 2$ and $n \geq 4$, there exists $f \in \mathrm{Per}(\mathbb{F}_2^n)$ such that* k-affinity$(f) = 0$ *for all $3 \leq k \leq n-1$.*

(iii) *If $q \geq 4$ and $n \geq 2$, there exists $f \in \mathrm{Per}(\mathbb{F}_q^n)$ such that* k-affinity$(f) = 0$ *for all $1 \leq k \leq n-1$.*

(iv) *If $q = 3$ and $n \geq 3$, there exists $f \in \mathrm{Per}(\mathbb{F}_3^n)$ such that* k-affinity$(f) = 0$ *for all $2 \leq k \leq n-1$.*

(v) *If $q = 3$ and $n \geq 2$, there exists $f \in \mathrm{Per}(\mathbb{F}_3^n)$ such that* 1-affinity$(f) = 0$.

The proof of Theorem 2.1 is spread out in parts in the rest of this section. Part (i) of Theorem 2.1 is well known. (See [3, 4] for several families of permutations of $\mathbb{F}_2^{2m+1}$ with 2-affinity 0.) It also follows from the following example in which we compute the 2-affinity of the permutation f of $\mathbb{F}_2^n$ ($\cong \mathbb{F}_{2^n}$) defined by $f(x) = x^{2^n-2}$. We remark that this permutation has been discussed by Nyberg [7] in terms of differential uniformity and that our computation is slightly different from that of [7].

Example 2.2. Identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$. Define $f \in \mathrm{Per}(\mathbb{F}_{2^n})$ by $f(x) = x^{2^n-2}$ for $x \in \mathbb{F}_{2^n}$. Note that

$$f(x) = \begin{cases} 0 & \text{if } x = 0,\\ \frac{1}{x} & \text{if } x \neq 0. \end{cases}$$

We claim that

$$2\text{-affinity}(f) = \begin{cases} 0 & \text{if } n \text{ is odd},\\ \frac{2^n-1}{3} & \text{if } n \text{ is even}. \end{cases}$$

Suppose $X \subset \mathbb{F}_{2^n}$ is some 2-flat such that $f(X)$ is also a 2-flat. Then we can write $X = \{x, y, z, w\}$ where $x + y + z + w = 0$. Suppose first that x, y, z, and w are all nonzero. Then we have $f(X) = \{\frac{1}{x}, \frac{1}{y}, \frac{1}{z}, \frac{1}{w}\}$ and $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w} = 0$. It follows that $w = x + y + z$ and

$$0 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{x+y+z} = \frac{(x+y)(x+z)(y+z)}{xyz(x+y+z)}.$$

It follows that $x = y$ or $x = z$ or $y = z$ which contradicts the assumption that X is a 2-flat. Thus without loss of generality we may assume that $w = 0$. Then $X = \{0, x, y, x+y\}$, $f(X) = \{0, \frac{1}{x}, \frac{1}{y}, \frac{1}{x+y}\}$ and

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{x+y} = 0.$$

This is equivalent to

$$\left(\frac{y}{x}\right)^2 + \left(\frac{y}{x}\right) + 1 = 0. \tag{2.1}$$

Hence $\frac{y}{x}$ is a root of the irreducible polynomial $g(t) = t^2 + t + 1 \in \mathbb{F}_2[t]$. Therefore $\mathbb{F}_2(\frac{y}{x})$ is a subfield of $\mathbb{F}_{2^n}$ with $[\mathbb{F}_2(\frac{y}{x}) : \mathbb{F}_2] = 2$. It follows that n is even. So if n is odd, no such x and y exist and 2-affinity$(f) = 0$.

On the other hand, if n is even, $g(t)$ has two roots β and $1+\beta$ in $\mathbb{F}_{2^n}$ and $K = \{0, 1, \beta, 1+\beta\}$ is the unique subfield of order 4 in $\mathbb{F}_{2^n}$. It follows from (2.1) that $\frac{y}{x} = \beta$ or $1+\beta$. In both cases,

$$\begin{aligned} X &= \{0, x, y, x+y\} \\ &= \{0, x, x\beta, x(1+\beta)\} \\ &= xK \\ &= \{0\} \cup xK^* \end{aligned}$$

where K^* is the multiplicative group of K and xK^* is a coset of the subgroup K^* in $\mathbb{F}_{2^n}^*$. There are $(2^n - 1)/3$ cosets of K^* in $\mathbb{F}_{2^n}^*$ and therefore the same number of 2-flats of the form xK. Since $f(xK) = \frac{1}{x}K$, it follows that 2-affinity$(f) = (2^n - 1)/3$, as claimed.

Note that when $n = 4$, $\frac{2^4-1}{3} = 5$ is the minimum 2-affinity of permutations of $\mathbb{F}_2^4$ ([5]).

The proof of parts (ii) – (iv) of Theorem 2.1 relies on the following theorem whose proof will be given in Section 3.

Theorem 2.3. *Let q, m, n be integers such that $n > m$ and q, m satisfy one of the following conditions:*

(a) $q = 2$, $m = 3$,
(b) $q = 3$, $m = 2$,
(c) $q \geq 4$, $m = 1$.

Then

$$\sum_{k=m}^{n-1} q^{2(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^k! \, (q^n - q^k)! < q^n!. \tag{2.2}$$

Proof of Theorem 2.1 (ii) – (iv). Let Φ_k denote the set of all $f \in \mathrm{Per}(\mathbb{F}_q^n)$ such that k-affinity$(f) \geq 1$. Let X be any fixed k-flat in $\mathbb{F}_q^n$ and define

$$S_X = \{f \in \mathrm{Per}(\mathbb{F}_q^n) : f(X) = X\}.$$

Note that since $|X| = q^k$ we have $|S_X| = q^k! \, (q^n - q^k)!$.

The group of invertible affine transformations of $\mathbb{F}_q^n$, i.e., the general affine group $\mathrm{AGL}(n, \mathbb{F}_q)$, acts transitively on the set of all k-flats of $\mathbb{F}_q^n$. Hence for every k-flat W, there exists $\alpha_W \in \mathrm{AGL}(n, \mathbb{F}_q)$ such that $\alpha_W(W) = X$. Let $f \in \Phi_k$ and assume that $f(W) = Z$ where W and Z are k-flats. Then $\alpha_Z \circ f \circ \alpha_W^{-1} \in S_X$, i.e., $f \in \alpha_Z^{-1} \circ S_X \circ \alpha_W$. Since there are $q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q$ k-flats in $\mathbb{F}_q^n$ it follows that

$$|\Phi_k| \leq \left(q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q \right)^2 |S_X| = q^{2(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^k! \, (q^n - q^k)!.$$

Hence if q and m satisfy one of the conditions in Theorem 2.3 and $n > m$, we have

$$\sum_{k=m}^{n-1} |\Phi_k| \leq \sum_{k=m}^{n-1} q^{2(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^k! \, (q^n - q^k)! < q^n!.$$

Thus there exists $f \in \mathrm{Per}(\mathbb{F}_q^n)$ such that $f \notin \bigcup_{k=m}^{n-1} \Phi_k$. □

Note that inequality (2.2) does not cover the case $q = 3$ and $m = 1$, that is, part (v) of Theorem 2.1. This case is dealt with as a corollary to the following lemma.

Lemma 2.4. *Let F be any field. If the permutations $f : F^n \to F^n$ and $g : F^m \to F^m$ each have 1-affinity 0 then the permutation $f \times g : F^n \times F^m \to F^n \times F^m$ has 1-affinity 0.*

Proof. Assume to the contrary that there exists a 1-flat X in $F^n \times F^m$ such that $(f \times g)(X)$ is also a flat. Let $\pi_1 : F^n \times F^m \to F^n$ and $\pi_2 : F^n \times F^m \to F^m$ be the projections. Then either $\pi_1(X)$ is a 1-flat in F^n or $\pi_2(X)$ is a 1-flat in F^m. Without loss of generality, assume that the former is the case. Thus $f\big(\pi_1(X)\big) = \pi_1\big((f \times g)(X)\big)$ is a 1-flat in F^n, which is impossible since 1-affinity$(f) = 0$. □

Corollary 2.5. *If $n \geq 2$, there exists $f \in \mathrm{Per}(\mathbb{F}_3^n)$ such that* 1-affinity$(f) = 0$.

Proof. By Lemma 2.4, it suffices to show that $\mathbb{F}_3^2$ and $\mathbb{F}_3^3$ have permutations of 1-affinity 0. Such permutations are easily found through a computer search. For $\mathbb{F}_3^2$, label the elements $(0, 0)$, $(0, 1)$, $\ldots$, $(2, 2)$ with $0, 1, \ldots, 8$. A desirable permutation f is given by

$$\big(f(0), \cdots, f(8)\big) = (0,\ 1,\ 8,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7).$$

For $\mathbb{F}_3^3$, we label the elements $(0, 0, 0)$, $(0, 0, 1)$, $\ldots$, $(2, 2, 2)$ with $0, 1, \ldots, 26$. A desirable permutation f in this case is given by

$$\begin{aligned}\big(f(0), \cdots, f(26)\big) = &(0,\ 1,\ 24,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\\ &14,\ 25,\ 15,\ 16,\ 17,\ 26,\ 18,\ 19,\ 23,\ 20,\ 21,\ 22).\end{aligned}$$

□

3. Inequalities between Binomial and q-Binomial Coefficients

In this section we assume that i, k, m, n, q are integers.

Lemma 3.1. *For $q > 2$, $n > k \geq 1$ and $q = 2$, $n > k \geq 2$,*

$$\frac{\begin{bmatrix} n \\ k \end{bmatrix}_q^2}{\dbinom{q^n}{q^k}} < \frac{1}{q^{q^k - 2k}} \cdot \frac{\begin{bmatrix} n-1 \\ k \end{bmatrix}_q^2}{\dbinom{q^{n-1}}{q^k}}. \tag{3.1}$$

Proof. Inequality (3.1) is equivalent to

$$\frac{(q^n - 1)^2}{q^n(q^n - 1) \ldots (q^n - (q^k - 1))} < \frac{(q^n - q^k)^2}{q^n(q^n - q) \ldots (q^n - (q^k - 1)q)}, \tag{3.2}$$

which can be further rewritten as

$$\frac{1}{\prod_{i=2}^{q^k-2}(q^n - i)} \cdot \frac{q^n - 1}{q^n - (q^k - 1)} < \frac{1}{\prod_{\substack{1 \leq i \leq q^k - 2 \\ i \neq q^{k-1}}}(q^n - qi)} \cdot \frac{q^n - q^k}{q^n - (q^k - 1)q}.$$

Clearly,

$$\prod_{i=2}^{q^k-2}(q^n-i)\ge \prod_{\substack{1\le i\le q^k-2\\ i\ne q^{k-1}}}(q^n-qi).$$

Thus it suffices to show that

$$\frac{q^n-1}{q^n-(q^k-1)}<\frac{q^n-q^k}{q^n-(q^k-1)q}. \tag{3.3}$$

Inequality (3.3) follows from

$$\begin{aligned}&(q^n-q^k)(q^n-(q^k-1))-(q^n-1)(q^n-(q^k-1)q)\\ =&(q^k-1)(q^n(q-2)+q^k-q)\\ >&0.\end{aligned}$$

□

Lemma 3.2. *For $q\ge 4$, $k\ge 1$, or $q=3$, $k\ge 2$, or $q=2$, $k\ge 3$,*

$$\frac{\begin{bmatrix}k+1\\ k\end{bmatrix}_q^2}{\binom{q^{k+1}}{q^k}}<\frac{1}{q^{q^k-k}}. \tag{3.4}$$

Proof. The left hand side of (3.4) equals

$$\frac{q^{k+1}-1}{q^{k+1}}\cdot\frac{2\cdot 3}{(q-1)^2(q^{k+1}-q^k+1)(q^{k+1}-q^k+2)}\cdot q^k\cdot\prod_{i=1}^{q^k-4}\frac{q^k-i}{q^{k+1}-i-1}.$$

In this product,

$$\frac{q^{k+1}-1}{q^{k+1}}<1$$

and for every $1\le i\le q^k-4$,

$$\frac{q^k-i}{q^{k+1}-i-1}\le\frac{1}{q} \tag{3.5}$$

(To see (3.5), note that since $q\ge 2$, we have $q^{k+1}-i-1\ge q^{k+1}-qi$.) Therefore, it suffices to show that

$$\frac{6}{(q-1)^2(q^{k+1}-q^k+1)(q^{k+1}-q^k+2)}\le\frac{1}{q^4}.$$

Let

$$f(q,k)=(q-1)^2\Big(q^{k-2}(q-1)+\frac{1}{q^2}\Big)\Big(q^{k-2}(q-1)+\frac{2}{q^2}\Big).$$

It suffices to show that

$$f(q,k)\ge 6.$$

The function $f(q,k)$ is increasing with respect to k for fixed $q>1$. For $k\ge 2$ and $q\ge 2$ or $k=1$ and $q\ge 4$, we have

$$\frac{d}{dq}\Big[q^{k-2}(q-1)+\frac{1}{q^2}\Big]=(k-1)q^{k-2}-(k-2)q^{k-3}-2q^{-3}>0$$

and

$$\frac{d}{dq}\left[q^{k-2}(q-1)+\frac{2}{q^2}\right]=(k-1)q^{k-2}-(k-2)q^{k-3}-4q^{-3}\geq 0.$$

Hence $f(q,k)$ is increasing with respect to q for q and k in the above range. Thus, for $q \geq 4$ and $k \geq 1$,

$$f(q,k)\geq f(4,1)=\frac{819}{128}>6;$$

for $q=3$ and $k\geq 2$,

$$f(q,k)\geq f(3,2)=\frac{1520}{81}>6;$$

for $q=2$ and $k\geq 4$,

$$f(q,k)\geq f(2,4)=\frac{153}{8}>6.$$

For $q=2$ and $k=3$, (3.4) is verified directly:

$$\frac{\begin{bmatrix}4\\3\end{bmatrix}_2^2}{\binom{2^4}{2^3}}=\frac{5}{286}<\frac{1}{32}=\frac{1}{2^{2^3-3}}.$$

□

Corollary 3.3. *For $q\geq 4$, $n>k\geq 1$, or $q=3$, $n>k\geq 2$, or $q=2$, $n>k\geq 3$,*

$$\frac{\begin{bmatrix}n\\k\end{bmatrix}_q^2}{\binom{q^n}{q^k}}<\frac{1}{q^{(n-k)(q^k-2k)+k}}. \tag{3.6}$$

Proof. Applying Lemma 3.1 to the left hand side of (3.6) $n-k-1$ times and applying Lemma 3.2 after that, we get

$$\begin{aligned}\frac{\begin{bmatrix}n\\k\end{bmatrix}_q^2}{\binom{q^n}{q^k}}&<\frac{1}{q^{(n-k-1)(q^k-2k)}}\cdot\frac{\begin{bmatrix}k+1\\k\end{bmatrix}_q^2}{\binom{q^{k+1}}{q^k}}\\&<\frac{1}{q^{(n-k-1)(q^k-2k)}}\cdot\frac{1}{q^{q^k-k}}\\&=\frac{1}{q^{(n-k)(q^k-2k)+k}}.\end{aligned}$$

□

Lemma 3.4. *For $q\geq 4$, $k\geq 1$, or $q=3$, $k\geq 2$, or $q=2$, $k\geq 3$,*

$$q^k-2k-2\geq 0. \tag{3.7}$$

Proof. Let $g(q,k)$ denote the left hand side of (3.7). For fixed $k\geq 1$, $g(q,k)$ is increasing with respect to q. Also note that

$$\frac{\partial g}{\partial k}=q^k\ln q-2>\frac{q^k-4}{2},$$

which is non-negative in the described range for q and k. So, $g(q,k)$ is increasing with respect to k in such range. Thus, for $q \geq 4$ and $k \geq 1$

$$g(q,k) \geq g(4,1) = 0;$$

for $q = 3$ and $k \geq 2$,

$$g(q,k) \geq g(3,2) = 3 > 0;$$

for $q = 2$ and $k \geq 3$,

$$g(q,k) \geq g(2,3) = 0.$$

□

Proof of Theorem 2.3. Let q and m satisfy one of the conditions (a) – (c) in Theorem 2.3 and let $n > m$. By Corollary 3.3 and Lemma 3.4, for $m \leq k < n$, we have

$$q^{2(n-k)} \frac{{\begin{bmatrix} n \\ k \end{bmatrix}_q}^2}{\binom{q^n}{q^k}} < \frac{1}{q^{(n-k)(q^k-2k-2)+k}} \leq \frac{1}{q^k}.$$

Therefore,

$$\sum_{k=m}^{n-1} q^{2(n-k)} \frac{{\begin{bmatrix} n \\ k \end{bmatrix}_q}^2}{\binom{q^n}{q^k}} < \sum_{k=m}^{n-1} \frac{1}{q^k} < \sum_{k=1}^{\infty} \frac{1}{q^k} = \frac{1}{q-1} \leq 1,$$

which proves the theorem. □

4. Examples of k-Spectra for Small Values of k, n, q

Recall that for given k, n, q,

$$k\text{-spectrum}(n,q) = \{k\text{-affinity}(f) : f \in \mathrm{Per}(\mathbb{F}_q^n)\}.$$

Here we give some examples. In all cases $a - b$ denotes all integers from a to b. Only a few of the spectra (as indicate below) are proved to be complete. The other examples are spectra obtained by random searches. In such cases it is possible but not certain that some values are missing, hence the results are called *partial spectra*.

The full spectrum for $k = 1, n = 2, q = 3$:
$\{0 - 4,\ 6,\ 12\}$

The full spectrum for $k = 1, n = 2, q = 4$:
$\{0 - 6,\ 8,\ 12,\ 20\}$

A partial spectrum for $k = 1, n = 2, q = 5$:

$\{0 - 12,\ 14,\ 15,\ 20,\ 30\}$

A partial spectrum for $k = 1, n = 2, q = 7$:

$\{0 - 2,\ 5 - 7,\ 10 - 12,\ 14 - 18,\ 20 - 30,\ 32,\ 35,\ 42,\ 56\}$

A partial spectrum for $k = 1, n = 3, q = 3$:

$\{0 - 64,\ 66,\ 70,\ 71,\ 73,\ 75,\ 81,\ 93,\ 117\}$

The full spectrum for $k = 2, n = 3, q = 2$:

$\{0,\ 2,\ 6,\ 14\}$

A partial spectrum for $k = 2, n = 3, q = 3$:

{0 – 9, 11 – 13, 15, 21, 39}

The full spectrum for $k = 2, n = 4, q = 2$:

{5 – 20, 22, 24 – 26, 28, 30, 32, 36, 38, 44, 48, 52, 56, 76, 84, 140}

A partial spectrum for $k = 2, n = 5, q = 2$:

{0, 9 – 416, 418, 420, 422, 424, 426 – 428, 430 – 432, 434, 436 – 440, 442, 444 – 452, 454, 456 – 462, 464, 466, 468 – 472, 474, 476, 480, 482, 484, 486, 488, 490, 492, 496, 500, 504, 506, 508, 512, 514 – 515, 517 – 518, 520, 526 – 528, 530, 532, 536, 540, 548, 550, 552, 554, 556, 560, 564, 568, 576, 600, 604 – 605, 608, 618, 620, 640, 648, 664, 704, 706, 728, 732, 736, 792, 820, 960, 1240}

A partial spectrum for $k = 2, n = 6, q = 2$:

{21, 28 – 5132, 5134, 5136 – 5140, 5142 – 5148, 5150 – 5384, 5386, 5388, 5390, 5392, 5394, 5396 – 5418, 5420, 5422 – 5446, 5448 – 5464, 5466 – 5468, 5470, 5472 – 5480, 5482, 5484 – 5486, 5488, 5490, 5492, 5496, 5498, 5500, 5502, 5504, 5506, 5508, 5510, 5512, 5514, 5516, 5520, 5522, 5524, 5526, 5528, 5530, 5532, 5534, 5536, 5538, 5540, 5544, 5548, 5550 – 5552, 5554 – 5556, 5558, 5560 – 5562, 5564, 5566 – 5568, 5570 – 5572, 5574, 5576, 5578, 5580 – 5581, 5584, 5586, 5588 – 5606, 5608 – 5610, 5612 – 5634, 5636 – 5712, 5716 – 5736, 5738, 5740 – 5760, 5765 – 5774, 5776 – 5784, 5786, 5788 – 5790, 5792, 5794, 5796, 5820, 5822, 5824, 5830, 5832, 5834, 5836, 5840, 5844, 5849, 5855 – 5857, 5860 – 5861, 5868, 5874, 5876, 5878, 5880, 5882, 5884, 5886, 5888, 5890, 5892, 5896, 5898, 5900, 5904, 5908, 5912, 5936, 5940, 5944, 5948, 5952, 5960, 5974, 5976, 5978, 5984, 5986, 5988, 5990, 5994, 6000, 6012, 6020, 6030, 6032, 6034, 6045 – 6058, 6070 – 6084, 6086, 6088, 6090, 6092, 6096, 6099 – 6111, 6120 – 6136, 6138, 6140, 6142, 6144, 6146, 6148, 6152, 6160, 6178 – 6180, 6182 – 6184, 6186, 6188 – 6190, 6192, 6194, 6202, 6208, 6228, 6230, 6232, 6234, 6236, 6238, 6240, 6242, 6244, 6248, 6256, 6260, 6264, 6286, 6288, 6290, 6296, 6298, 6316, 6336, 6340, 6352, 6360, 6384, 6444, 6448, 6452, 6460, 6475 – 6480, 6482, 6484, 6488, 6496, 6501 – 6503, 6505 – 6508, 6528 – 6534, 6536, 6538, 6540, 6544, 6557 – 6560, 6586, 6588, 6590, 6592, 6594, 6596, 6640, 6642, 6644, 6648, 6650, 6656, 6756, 6764, 6768, 6832, 6955, 6957 – 6958, 6982 – 6984, 6986, 6988, 6992, 7036, 7038, 7040, 7042, 7044, 7048, 7056, 7152, 7156, 7160, 7384, 7461, 7490, 7492, 7552, 7994, 8052, 8056, 8176, 8556, 9176, 10416}

Observations:

(1) From Theorem 2.1, $0 \in k$-spectrum(n, q) for $1 \leq k \leq n-1$ unless $k = 1$, $q = 2$ or $k = 2$, $q = 2$ and n is even.

(2) Near the beginning in each example spectrum there is a long sequence of consecutive values. For $q = 2$ and $k = 2$, there seems to be a gap preceding the first non-zero affinity. For $q > 2$ the limited experimental data shows no such gaps. This suggests that for $q = 2$, if there is one 2-flat that is carried to a 2-flat then there are a certain number of other 2-flats that must also be carried to 2-flats.

(3) Preceding the largest value in k-spectrum(n,q) there appears to a gap of size $2q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$. Note that this gap may be considered a threshold in the sense that if k-affinity$(f) > q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q - 2q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$, then f takes all k-flats to k-flats.

5. $(n-1)$-SPECTRUM$(n,2)$

In this section, we will determine $(n-1)$-spectrum$(n,2)$, which is the set of all $(n-1)$-affinities of permutations of $\mathbb{F}_2^n$. The standard dot product of $a, b \in \mathbb{F}_2^n$ is denoted by $\langle a, b\rangle$. Every $(n-1)$-flat in $\mathbb{F}_2^n$ is uniquely of the form

$$H(a,\epsilon) := \{x \in \mathbb{F}_2^n : \langle a, x\rangle = \epsilon\}$$

for some $a \in \mathbb{F}_2^n \setminus \{0\}$ and $\epsilon \in \mathbb{F}_2$. Let $f \in \mathrm{Per}(\mathbb{F}_2^n)$. If for some $a \in \mathbb{F}_2^n \setminus \{0\}$ and some $\epsilon \in \mathbb{F}_2$, $f\big(H(a,\epsilon)\big)$ is an $(n-1)$-flat, say $f\big(H(a,\epsilon)\big) = H(b,\delta)$ for some $b \in \mathbb{F}_2^n \setminus \{0\}$ and $\delta \in \mathbb{F}_2$, we must have $f\big(H(a,1+\epsilon)\big) = H(b,1+\delta)$. Therefore, for each such a and b, there exists $\phi \in \mathrm{Per}(\mathbb{F}_2)$ such that

$$f\big(H(a,t)\big) = H\big(b,\phi(t)\big) \quad \text{for all } t \in \mathbb{F}_2. \tag{5.1}$$

Lemma 5.1. *Let $f \in \mathrm{Per}(\mathbb{F}_2^n)$ and let*

$$V_f = \{0\} \cup \big\{a \in \mathbb{F}_2^n \setminus \{0\} : f\big(H(a,0)\big) \text{ is an } (n-1)\text{-flat}\big\}.$$

Then V_f is a subspace of $\mathbb{F}_2^n$

Proof. For $a_1, a_2 \in V_f$, we prove that $a_1 + a_2 \in V_f$. We may assume that $a_1 \neq 0$, $a_2 \neq 0$, and $a_1 \neq a_2$. By (5.1), there exist $b_i \in \mathbb{F}_2^n \setminus \{0\}$ and $\phi_i \in \mathrm{Per}(\mathbb{F}_2)$, $i = 1, 2$, such that

$$f\big(H(a_i,t)\big) = H\big(b_i,\phi_i(t)\big) \quad \text{for all } t \in \mathbb{F}_2.$$

Clearly, $b_1 \neq b_2$. Since $\mathbb{F}_2$ has only two permutations, $t \mapsto t$ or $t \mapsto t+1$, we see that $\phi_1 + \phi_2$ is a constant, say ϵ. For any $x \in H(a_1+a_2, 0)$, let $t = \langle a_1, x\rangle = \langle a_2, x\rangle$. Then $x \in H(a_i, t)$, hence $f(x) \in H\big(b_i, \phi_i(t)\big)$. It follows that

$$\langle b_1 + b_2,\ f(x)\rangle = \phi_1(t) + \phi_2(t) = \epsilon,$$

i.e., $f(x) \in H(b_1+b_2, \epsilon)$. Thus we have proved that $f\big(H(a_1+a_2, 0)\big) = H(b_1+b_2, \epsilon)$, which implies that $a_1 + a_2 \in V_f$. $\square$

Theorem 5.2. *Let $n > 2$. Then*

$$(n-1)\text{-spectrum}(n,2) = \{2^i - 2 : 1 \le i \le n+1\}.$$

Proof. For each $f \in \mathrm{Per}(\mathbb{F}_2^n)$, by Lemma 5.1, we have

$$(n-1)\text{-affinity}(f) = 2|V_f \setminus \{0\}| = 2^{\dim V_f + 1} - 2 \in \{2^i - 2 : 1 \le i \le n+1\}.$$

It remains to show that for each $1 \le i \le n+1$, there exists $f \in \mathrm{Per}(\mathbb{F}_2^n)$ with

$$(n-1)\text{-affinity}(f) = 2^i - 2.$$

We prove this claim by induction on n. For $n = 3$, the claim was established by computer as mentioned in Section 4. Assume $n > 3$. If $i = 1$, the claim follows from Theorem 2.1. Thus we will assume $2 \le i \le n+1$. By the induction hypothesis, there exists $g \in \mathrm{Per}(\mathbb{F}_2^{n-1})$ such that $(n-2)$-affinity$(g) = 2^{i-1} - 2$. Define $f \in \mathrm{Per}(\mathbb{F}_2^n)$ by $f(c,x) = (c, g(x))$, $c \in \mathbb{F}_2$, $x \in \mathbb{F}_2^{n-1}$. Clearly, $\{i\} \times \mathbb{F}_2^{n-1}$, $i = 0, 1$, are mapped into flats by f. Let $X \subset \mathbb{F}_2^n$ be any $(n-1)$-flat other than $\{i\} \times \mathbb{F}_2^{n-1}$, $i = 0, 1$, such that $f(X)$ is a flat. Write

$$X \cap \big(\{i\} \times \mathbb{F}_2^{n-1}\big) = \{i\} \times U_i, \quad i = 0, 1.,$$

where $U_i \subset \mathbb{F}_2^{n-1}$ is an $(n-2)$-flat and $U_0 = U_1$ or $\mathbb{F}_2^{n-1} \setminus U_1$. Then

$$X = \big(\{0\} \times U_0\big) \cup \big(\{1\} \times U_1\big). \tag{5.2}$$

Since

$$\{i\} \times g((U_i) = f\Big(X \cap \big(\{i\} \times \mathbb{F}_2^{n-1}\big)\Big) = f(X) \cap \big(\{i\} \times \mathbb{F}_2^{n-1}\big)$$

is an $(n-2)$-flat, $g(U_i)$ is an $(n-2)$-flat. On the other hand, given any $(n-2)$-flats $U_0, U_1 \subset \mathbb{F}_2^{n-1}$ such that $U_0 = U_1$ or $\mathbb{F}_2^{n-1} \setminus U_1$ and $g(U_i)$, $i = 0, 1$, are $(n-2)$-flats, both X (in (5.2)) and $f(X)$ are $(n-1)$-flats in $\mathbb{F}_2^n$. Therefore,

$$\begin{aligned}(n-1)\text{-affinity}(f) &= 2 + 2 \cdot \big((n-2)\text{-affinity}(g)\big)\\ &= 2 + 2(2^{i-1} - 2)\\ &= 2^i - 2.\end{aligned}$$

The proof is now complete. □

6. Threshold Conjecture for k-Affinity

In many cases it appears that the next to largest k-affinity is the k-affinity of a transposition. We calculate this value in the following lemma. In this case it is more convenient to compute the k-coaffinity.

Lemma 6.1. *Let $f \in \mathrm{Per}(\mathbb{F}_q^n)$ be any transposition. Then*

$$k\text{-coaffinity}(f) = 2q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$$

and

$$k\text{-affinity}(f) = \left(\frac{(q^{n-k} - 2)(q^n - 1)}{q^k - 1} + 2\right) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q.$$

Proof. Assume that f interchanges x and y, where $x, y \in \mathbb{F}_q^n$ are distinct. If U is a k-flat, then $f(U)$ is not a k-flat if and only if U contains exactly one of x and y.

The number of k-flats in $\mathbb{F}_q^n$ containing a fixed point is $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$; the number of k-flats in $\mathbb{F}_q^n$ containing two fixed points is $\left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right]_q$. Hence

$$k\text{-coaffinity}(f) = 2\left(\begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q\right) = 2q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q.$$

It follows that

$$\begin{aligned}k\text{-affinity}(f) &= q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q - 2q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q\\ &= \left(\frac{(q^{n-k} - 2)(q^n - 1)}{q^k - 1} + 2\right) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q.\end{aligned}$$

□

It is natural to call the next largest k-affinity a threshold for affinity and we make the following conjecture:

Conjecture 6.2 (Threshold Conjecture)**.** *Let $1 \le k \le n-1$ and $f \in \mathrm{Per}(\mathbb{F}_q^n)$. If*

$$k\text{-coaffinity}(f) < 2q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q,$$

then k-coaffinity$(f) = 0$*, i.e.,* $f \in \mathrm{AGL}(n, \mathbb{F}_q)$*. Equivalently, if*

$$k\text{-affinity}(f) > \left(\frac{(q^{n-k}-2)(q^n-1)}{q^k-1} + 2\right) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q,$$

then k-affinity$(f) = q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$*. That is, the next to largest* k*-affinity is that of a transposition.*

This conjecture is supported by the examples in Section 4 and the result in Section 5. More importantly it is supported by the proof for $q = 2$, $k = 2$, $n > 2$ in Section 7, and the proof for $q > 2$, $k = 1$, $n > 1$ in Section 8.

7. Proof of the Threshold Conjecture for $k = 2$, $q = 2$

Recall that a 2-flat in $\mathbb{F}_2^n$ is simply a 4-element subset $\{x_1, x_2, x_3, x_4\}$ such that $x_1 + x_2 + x_3 + x_4 = 0$. For $f \in \mathrm{Per}(\mathbb{F}_2^n)$ and a 2-flat $X \subset \mathbb{F}_2^n$, $f(X)$ is a 2-flat if and only if f is affine on X.

For the proof in this section, the reader's familiarity with the Fourier transformation of boolean functions will be helpful. We first introduce the necessary notation. The set of all functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is denoted by $\mathcal{P}_n$. Every function in $\mathcal{P}_n$ is uniquely represented by a polynomial in $\mathbb{F}_2[X_1, \dots, X_n]$ whose degree in each X_i is at most 1. Namely,

$$\mathcal{P}_n = \mathbb{F}_2[X_1, \dots, X_n]/\langle X_1^2 - X_1, \dots, X_n^2 - X_n\rangle.$$

For each $g \in \mathcal{P}_n$, put $|g| = |g^{-1}(1)|$. The Fourier transform of $g \in \mathcal{P}_n$ is the function $\hat{g} : \mathbb{F}_2^n \to \mathbb{C}$ defined by

$$\hat{g}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x) + \langle a, x\rangle}, \quad a \in \mathbb{F}_2^n,$$

where $\langle a, x\rangle$ is the standard dot product in $\mathbb{F}_2^n$. Clearly,

$$\hat{g}(a) = 2^n - 2|g + \langle a, \cdot\rangle|. \tag{7.1}$$

Note that for $n \geq 2$, $|g + \langle a, \cdot\rangle| \equiv |g| \pmod 2$, hence

$$\hat{g}(a) \equiv 2|g| \pmod 4.$$

It is well known (also straightforward to prove) that

$$\sum_{a \in \mathbb{F}_2^n} \big(\hat{g}(a)\big)^2 = 2^{2n} \tag{7.2}$$

and

$$\sum_{a \in \mathbb{F}_2^n} \big(\hat{g}(a)\big)^4 = 2^n \sum_{a \in \mathbb{F}_2^n} \Big[\sum_{x \in \mathbb{F}_2^n} (-1)^{g(x+a)+g(x)}\Big]^2. \tag{7.3}$$

(Equation (7.2) is the Parseval identity; equation (7.3) is a relation between the Fourier transform and the convolution of the function. Cf. [6].) If $A \leq \big(\hat{g}(a)\big)^2 \leq B$

for all $a \in \mathbb{F}_2^n$, from (7.2), we have

$$\begin{aligned} 2^n\Big(\frac{B-A}{2}\Big)^2 &\ge \sum_{a\in\mathbb{F}_2^n}\Big[\big(\hat{g}(a)\big)^2-\frac{A+B}{2}\Big]^2 \\ &= \sum_{a\in\mathbb{F}_2^n}\big(\hat{g}(a)\big)^4-(A+B)\sum_{a\in\mathbb{F}_2^n}\big(\hat{g}(a)\big)^2+2^n\Big(\frac{A+B}{2}\Big)^2 \\ &= \sum_{a\in\mathbb{F}_2^n}\big(\hat{g}(a)\big)^4-2^{2n}(A+B)+2^n\Big(\frac{A+B}{2}\Big)^2. \end{aligned}$$

Thus

$$\sum_{a\in\mathbb{F}_2^n}\big(\hat{g}(a)\big)^4 \le 2^{2n}(A+B)-2^nAB.$$

Combining the above with (7.3), we have

$$\sum_{a\in\mathbb{F}_2^n}\Big[\sum_{x\in\mathbb{F}_2^n}(-1)^{g(x+a)+g(x)}\Big]^2 \le 2^n(A+B)-AB. \tag{7.4}$$

The equality in (7.4) holds if and only if $\big(\hat{g}(a)\big)^2 = A$ or B for all $a \in \mathbb{F}_2^n$.

Lemma 7.1. *Let $g \in \mathcal{P}_n$ with $\deg g \ge 2$. Then*

$$\sum_{a\in\mathbb{F}_2^n}\Big[\sum_{x\in\mathbb{F}_2^n}(-1)^{g(x+a)+g(x)}\Big]^2 \le 2^{2n}+(2^n-1)(2^n-4)^2. \tag{7.5}$$

The equality holds if and only if $|g+h| = 1$ for some $h \in \mathcal{P}_n$ with $\deg h \le 1$.

Proof. Since $\deg g \ge 2$, $\hat{g}(a) \ne \pm 2^n$ for all $a \in \mathbb{F}_2^n$.

Case 1. $|g|$ is even. By (7.1), $0 \le |\hat{g}(a)| \le 2^n - 4$ for all $a \in \mathbb{F}_2^n$. Hence

$$0 \le \big(\hat{g}(a)\big)^2 \le (2^n-4)^2 \quad \text{for all } a \in \mathbb{F}_2^n.$$

By (7.4),

$$\sum_{a\in\mathbb{F}_2^n}\Big[\sum_{x\in\mathbb{F}_2^n}(-1)^{g(x+a)+g(x)}\Big]^2 \le 2^n(2^n-4)^2 < 2^{2n}+(2^n-1)(2^n-4)^2.$$

Case 2. $|g|$ is odd, By (7.1), $2 \le |\hat{g}(a)| \le 2^n - 2$ for all $a \in \mathbb{F}_2^n$. Hence

$$2^2 \le \big(\hat{g}(a)\big)^2 \le (2^n-2)^2 \quad \text{for all } a \in \mathbb{F}_2^n.$$

By (7.4),

$$\begin{aligned} \sum_{a\in\mathbb{F}_2^n}\Big[\sum_{x\in\mathbb{F}_2^n}(-1)^{g(x+a)+g(x)}\Big]^2 &\le 2^n\big[2^2+(2^n-2)^2\big]-2^2(2^n-2)^2 \\ &= 2^{2n}+(2^n-1)(2^n-4)^2. \end{aligned}$$

The equality holds if and only if $\big(\hat{g}(a)\big)^2 = 2^2$ or $(2^n-2)^2$ for all $a \in \mathbb{F}_2^n$.

First assume that the equality in (7.5) holds. Since $\sum_{a\in\mathbb{F}_2^n}\big(\hat{g}(a)\big)^2 = 2^{2n}$, for at least one $a \in \mathbb{F}_2^n$, $\big(\hat{g}(a)\big)^2 = (2^n-2)^2$. By (7.1),

$$\big(2^n - 2|g+\langle a,\cdot\rangle|\big)^2 = (2^n-2)^2.$$

Thus $|g+\langle a,\,\cdot\rangle|=1$ or 2^n-1. Let

$$h=\begin{cases}\langle a,\,\cdot\rangle & \text{if } |g+\langle a,\,\cdot\rangle|=1,\\ \langle a,\,\cdot\rangle+1 & \text{if } |g+\langle a,\,\cdot\rangle|=2^n-1.\end{cases}$$

Then $|g+h|=1$, as claimed.

Now assume that $|g+h|=1$ for some $h\in\mathcal{P}_n$ with $\deg h\le 1$. Then for every $a\in\mathbb{F}_2^n$,

$$|g+\langle a,\,\cdot\rangle|=2^{n-1}\pm 1,\ \text{ or } 1, \text{or } 2^n-1.$$

It follows from (7.1) that $\hat{g}(a)=\pm 2$ or $\pm(2^n-2)$. Hence $\big(\hat{g}(a)\big)^2=2^2$ or $(2^n-2)^2$ for all $a\in\mathbb{F}_2^n$. Therefore the equality holds in (7.5). □

Theorem 7.2. *Let $n\ge 3$ and $f\in\mathrm{Per}(\mathbb{F}_2^n)\setminus\mathrm{AGL}(n,\mathbb{F}_2)$. Then*

$$\text{2-coaffinity}(f)\ge\frac{8}{3}(2^{n-1}-1)(2^{n-2}-1).$$

The equality holds if and only if $f\in\mathrm{AGL}(n,\mathbb{F}_2)\circ\tau\circ\mathrm{AGL}(n,\mathbb{F}_2)$ where $\tau\in\mathrm{Per}(\mathbb{F}_2^n)$ is any transposition.

Corollary 7.3. *The Threshold Conjecture (Conjecture 6.2) holds for $q=2$, $k=2$, $n>2$.*

Proof of Theorem 7.2. **Case 1**. $f(x+d)+f(x)=$ constant for some $d\in\mathbb{F}_2^n\setminus\{0\}$. Without loss of generality, assume $d=(1,0,\dots,0)$. Write $f=(f_1,\dots,f_n)$ where $f_i:\mathbb{F}_2^n\to\mathbb{F}_2$. Then

$$f_i=c_iX_1+g_i(X_2,\dots,X_n)$$

for all $1\le i\le n$, where $c_i\in\mathbb{F}_2$ and $g_i\in\mathcal{P}_{n-1}$. Note that $(c_1,\dots,c_n)\ne 0$ since otherwise, f is independent of X_1 and cannot be a permutation of $\mathbb{F}_2^n$. By composing a suitable element of $\mathrm{GL}(n,\mathbb{F}_2)$ to the left of f, we may assume $(c_1,\dots,c_n)=(1,0,\dots,0)$. Thus

$$f=\big(X_1+g_1(X_2,\dots,X_n),\ g_2(X_2,\dots,X_n),\ \dots,\ g_n(X_2,\dots,X_n)\big).$$

It follows that $g=(g_2,\dots,g_n)$ is a permutation of $\mathbb{F}_2^{n-1}$.

Case 1.1. $g\notin\mathrm{AGL}(n-1,\mathbb{F}_2)$. Using induction, we may assume

$$\text{2-coaffinity}(g)\ge\frac{8}{3}(2^{n-2}-1)(2^{n-3}-1).$$

Note that if g is not affine on a 2-flat $\{y_1,y_2,y_3,y_4\}$ in $\mathbb{F}_2^{n-1}$, f is not affine on the 2-flat $\{(x_i,y_i):i\le i\le 4\}$ where $x_1+\cdots+x_4=0$. Hence

$$\text{2-coaffinity}(f)\ge 8\cdot\big(\text{2-coaffinity}(g)\big)>\frac{8}{3}(2^{n-1}-1)(2^{n-2}-1).$$

Case 1.2. $g\in\mathrm{AGL}(n-1,\mathbb{F}_2)$. Then $\deg g_1\ge 2$. We may assume $g=\mathrm{id}$. In this case, the 2-flats on which f is not affine are precisely

$$\{(x_i,y_i):1\le i\le 4\}$$

where $\{y_1,\dots,y_4\}$ is a 2-flat in $\mathbb{F}_2^{n-1}$ such that $\sum_{i=1}^4 g_1(y_i)=1$ and $x_1,\dots,x_4\in\mathbb{F}_2$ with $\sum_{i=1}^4 x_i=0$. Define

$$\begin{array}{rccl} G: & (\mathbb{F}_2^{n-1})^3 & \longrightarrow & \mathbb{F}_2\\ & (y,a,b) & \longmapsto & g_1(y)+g_1(y+a)+g_1(y+b)+g_1(y+a+b)\end{array}$$

Then

$$\text{2-coaffinity}(f) = \frac{8}{4!}|G| = \frac{1}{3}|G|.$$

We have

$$\begin{aligned}
|G| &= \frac{1}{2}\Big[2^{3(n-1)} - \sum_{y,a,b\in\mathbb{F}_2^{n-1}} (-1)^{G(y,a,b)}\Big] \\
&= \frac{1}{2}\Big[2^{3(n-1)} - \sum_{a\in\mathbb{F}_2^{n-1}} \sum_{y,b\in\mathbb{F}_2^{n-1}} (-1)^{g_1(y)+g_1(y+a)+g_1(y+b)+g_1(y+a+b)}\Big] \\
&= \frac{1}{2}\Big[2^{3(n-1)} - \sum_{a\in\mathbb{F}_2^{n-1}} \Big(\sum_{y\in\mathbb{F}_2^{n-1}} (-1)^{g_1(y)+g_1(y+a)}\Big)^2\Big] \\
&\ge \frac{1}{2}\Big[2^{3(n-1)} - \big[2^{2(n-1)} + (2^{n-1}-1)(2^{n-1}-4)^2\big]\Big] \quad \text{(by Lemma 7.1)} \\
&= 2^3(2^{n-1}-1)(2^{n-2}-1).
\end{aligned}$$

Therefore,

$$\text{2-coaffinity}(f) = \frac{1}{3}|G| \ge \frac{8}{3}(2^{n-1}-1)(2^{n-2}-1).$$

If the equality holds in the above, then the equality in (7.5) holds with g_1 in place of g. By Lemma 7.1, there exists $h \in \mathcal{P}_{n-1}$ such that $|g_1 + h| = 1$. Using a linear transformation, we may replace g_1 with $g_1 + h$. Thus we may assume $|g_1| = 1$. Then clearly,

$$f = \big(X_1 + g_1(X_2, \dots, X_n),\ X_2,\ \dots,\ X_n\big)$$

is a transposition.

Case 2. $f(x+d) + f(x) \ne$ constant for all $d \in \mathbb{F}_2^n \setminus \{0\}$. For each $d \in \mathbb{F}_2^n \setminus \{0\}$, let

$$\Delta(d) = \big\{\{x, x+d\} : x \in \mathbb{F}_2^n\big\} \subset \binom{\mathbb{F}_2^n}{2},$$

where $\binom{\mathbb{F}_2^n}{2}$ denotes the set of all 2-element subsets of $\mathbb{F}_2^n$. Denote $\{f(X) : X \in \Delta(d)\}$ by $f(\Delta(d))$ (an abuse of notation for the convenience). By the assumption, $f\big(\Delta(d)\big) \not\subset \Delta(c)$ for every $c \in \mathbb{F}_2^n \setminus \{0\}$. Since the subsets in $\Delta(d)$ and $\Delta(c)$ form partitions of $\mathbb{F}_2^n$, we have

$$\big|f\big(\Delta(d)\big) \cap \Delta(c)\big| \le 2^{n-1} - 2. \tag{7.6}$$

We claim that we can partition $\mathbb{F}_2^n \setminus \{0\}$ into A and B such that

$$\Big|f\big(\Delta(d)\big) \cap \Big(\bigcup_{a\in A} \Delta(a)\Big)\Big| \ge 2,$$

$$\Big|f\big(\Delta(d)\big) \cap \Big(\bigcup_{b\in B} \Delta(b)\Big)\Big| \ge 2.$$

Note that $\Delta(a)$, $a \in \mathbb{F}_2^n \setminus \{0\}$ form a partition of $\binom{\mathbb{F}_2^n}{2}$. If $\big|f\big(\Delta(d)\big) \cap \Delta(a)\big| \le 1$ for all $a \in \mathbb{F}_2^n \setminus \{0\}$, choose $a_1, a_2 \in \mathbb{F}_2^n \setminus \{0\}$ distinct such that $\big|f\big(\Delta(d)\big) \cap \Delta(a_i)\big| = 1$, $i = 1, 2$. Then $A = \{a_1, a_2\}$, $B = \mathbb{F}_2^n \setminus \{0, a_1, a_2\}$ have the desired property. If $\big|f\big(\Delta(d)\big) \cap \Delta(a)\big| \ge 2$ for some $a \in \mathbb{F}_2^n \setminus \{0\}$, let $A = \{a\}$ and $B = \mathbb{F}_2^n \setminus \{0, a\}$. By (7.6), we have

$$\Big|f\big(\Delta(d)\big) \cap \Big(\bigcup_{b\in B} \Delta(b)\Big)\Big| = 2^{n-1} - \big|f\big(\Delta(d)\big) \cap \Delta(a)\big| \ge 2.$$

Hence A and B also have the desired property.

Therefore, among the 2-flats which are a union of two elements in $\Delta(d)$, there are at least

$$2\cdot(2^{n-1}-2)$$

on which f is not affine. Since this statement is true for all $d\in\mathbb{F}_2^n\setminus\{0\}$, it follows that

$$\text{2-coaffinity}(f)\ge\frac{2\cdot(2^{n-1}-2)\cdot(2^n-1)}{3}>\frac{8}{3}(2^{n-1}-1)(2^{n-2}-1).$$

□

For the remainder of this section, we compute the number of permutations $f\in\mathrm{Per}(\mathbb{F}_2^n)$ with $\text{2-coaffinity}(f)=2^2\left[{n-1\atop 2}\right]_2=\frac{8}{3}(2^{n-1}-1)(2^{n-2}-1)$.

Lemma 7.4. *Let $n\ge 3$ and choose $a\in\mathbb{F}_2^n\setminus\{0\}$. Let $\tau\in\mathrm{Per}(\mathbb{F}_2^n)$ be the transposition which permutes 0 and a and let $f\in\mathrm{AGL}(n,\mathbb{F}_2)$.*

(i) *If $n\ge 4$, then $\tau\circ f\circ\tau\in\mathrm{AGL}(n,\mathbb{F}_2)$ if and only if $f(\{0,a\})=\{0,a\}$.*
(ii) *If $n=3$, then $\tau\circ f\circ\tau\in\mathrm{AGL}(n,\mathbb{F}_2)$ if and only if $f(a)+f(0)=a$.*

Proof. (i) ($\Leftarrow$) In fact, $\tau\circ f\circ\tau=f$.

($\Rightarrow$) Assume to the contrary that $f(\{0,a\})\ne\{0,a\}$. Without loss of generality, assume $f^{-1}(0)\notin\{0,a\}$. Since $n\ge 4$, there is a 2-flat A in $\mathbb{F}_2^n$ which contains $f^{-1}(0)$ but does contain $0,a$ and $f^{-1}(a)$. Write $A=\{f^{-1}(0),b_2,b_3,b_4\}$ where $b_i\notin\{0,a\}$, $f(b_i)\notin\{0,a\}$ and $f(b_2)+f(b_3)+f(b_4)=0$. We then have

$$(\tau\circ f\circ\tau)(A)=\tau\big(f(A)\big)=\tau\big(\{0,f(b_2),f(b_3),f(b_4)\}\big)=\{a,f(b_2),f(b_3),f(b_4)\},$$

which is not a 2-flat. This is a contradiction.

(ii) ($\Leftarrow$) Without loss of generality, assume $a=(1,0,0)$. Then

$$\tau(x_1,x_2,x_3)=(x_1+g(x_2,x_3),\,x_2,\,x_3)$$

where

$$g(x_2,x_3)=\begin{cases}1 & \text{if } (x_2,x_3)=0,\\ 0 & \text{if } (x_2,x_3)\ne 0.\end{cases}\tag{7.7}$$

Since $f(a)+f(0)=a$, we have

$$f(x)=xA+b,$$

where $b\in\mathbb{F}_2^3$, $A\in\mathrm{GL}(3,\mathbb{F}_2)$ and $aA=a$, i.e.,

$$A=\begin{bmatrix}1&0\\c&B\end{bmatrix},\quad B\in\mathrm{GL}(2,\mathbb{F}_2),\ c\in\mathbb{F}_2^2.$$

Let $b=(b',b'')$ where $b'\in\mathbb{F}_2$ and $b''\in\mathbb{F}_2^2$. Then

$$\begin{aligned}&(\tau\circ f\circ\tau)(x_1,x_2,x_3)\\ =&(\tau\circ f)(x_1+g(x_2,x_2),\,x_2,\,x_3)\\ =&\tau\Big((x_1+g(x_2,x_2),\,x_2,\,x_3)A+b\Big)\\ =&\tau\Big(x_1+g(x_2,x_3)+(x_2,x_3)c+b',\ (x_2,x_3)B+b''\Big)\\ =&\Big(x_1+g(x_2,x_3)+(x_2,x_3)c+b'+g\big((x_2,x_3)B+b''\big),\ (x_2,x_3)B+b''\Big).\end{aligned}$$

By (7.7), $g\big((x_2,x_3)B+b''\big)=g\big((x_2,x_3)+b''B^{-1}\big)$. Thus

$$g(x_2,x_3)+g\big((x_2,x_3)B+b''\big)=g(x_2,x_3)+g\big((x_2,x_3)+b''B^{-1}\big)$$

has degree ≤ 1 since $\deg g\le 2$. Therefore $\tau\circ f\circ\tau\in \mathrm{AGL}(3,\mathbb{F}_2)$.

($\Rightarrow$) Assume to the contrary that $f(a)+f(0)\ne a$. Then $f\big(\{0,a\}\big)\ne\{0,a\}$. Without loss of generality, we may assume $f^{-1}(0)\notin\{0,a\}$. By the proof of ($\Rightarrow$) of (i), it suffices to show that there is a 2-flat A in $\mathbb{F}_2^3$ which contains $f^{-1}(0)$ but not $0,a$ and $f^{-1}(a)$. By the assumption, the set $\{0,a,f^{-1}(0),f^{-1}(a)\}$ is not 2-flat of $\mathbb{F}_2^3$, hence it either has only three distinct elements or is a frame of $\mathbb{F}_2^3$. (A set of $k+1$ elements in an affine space is called frame if their affine span is a k-flat.) To see the existence of a desirable 2-flat A, first note that $\big\{(0,0,0),(1,0,0),(0,1,0),(0,0,1)\big\}$ is a frame of $\mathbb{F}_2^3$ and $\big\{(x_1,x_2,x_3):x_1+x_2+x_3=0\big\}$ is a 2-flat which contains exactly one of the elements in the frame. Using a suitable affine transformation, we see that for any frame $\{\epsilon_0,\dots,\epsilon_3\}$ of $\mathbb{F}_2^3$, there is a 2-flat A such that $A\cap\{\epsilon_0,\dots,\epsilon_3\}=\{\epsilon_0\}$. $\square$

Corollary 7.5. *In the notation of Lemma 7.4, we have*

$$\big|\big(\tau\circ \mathrm{AGL}(n,\mathbb{F}_2)\circ\tau\big)\cap \mathrm{AGL}(n,\mathbb{F}_2)\big|=\begin{cases}2^n|\mathrm{GL}(n-1,\mathbb{F}_2)| & \text{if } n\ge 4,\\ 2^5|\mathrm{GL}(2,\mathbb{F}_2)| & \text{if } n=3.\end{cases}\tag{7.8}$$

Proof. Let $f\in\mathrm{AGL}(n,\mathbb{F}_2)$ be given by

$$f(x)=xA+b,$$

where $A\in\mathrm{GL}(n,\mathbb{F}_2)$ and $b\in\mathbb{F}_2^n$. By Lemma 7.4, when $n\ge 4$, $f\in\tau\circ\mathrm{AGL}(n,\mathbb{F}_2)\circ\tau$ if and only if $aA=a$ and $b=0$ or a; when $n=3$, $f\in\tau\circ\mathrm{AGL}(n,\mathbb{F}_2)\circ\tau$ if and only if $aA=a$. Equation (7.8) follows immediately. $\square$

Corollary 7.6. *Assume $n\ge 3$. The number of permutations $f\in\mathrm{Per}(\mathbb{F}_2^n)$ with* 2-coaffinity$(f)=2^2\left[\begin{smallmatrix}n-1\\2\end{smallmatrix}\right]_2$ *is given by*

$$\begin{cases}2^{\frac12(n^2+3n-2)}(2^n-1)^2\prod_{j=1}^{n-1}(2^j-1) & \text{if } n\ge 4,\\ 2^6\cdot 3\cdot 7^2 & \text{if } n=3.\end{cases}$$

Proof. Let $\tau\in\mathrm{Per}(\mathbb{F}_2^n)$ be any transposition. By Theorem 7.2, the number of $f\in\mathrm{Per}(\mathbb{F}_2^n)$ with 2-coaffinity$(f)=2^2\left[\begin{smallmatrix}n-1\\2\end{smallmatrix}\right]_2$ is

$$|\mathrm{AGL}(n,\mathbb{F}_2)\circ\tau\circ\mathrm{AGL}(n,\mathbb{F}_2)|=\frac{|\mathrm{AGL}(n,\mathbb{F}_2)|^2}{\big|\big(\tau\circ\mathrm{AGL}(n,\mathbb{F}_2)\circ\tau\big)\cap\mathrm{AGL}(n,\mathbb{F}_2)\big|}.$$

The result follows immediately from the above corollary. $\square$

8. Proof of the Threshold Conjecture for $k=1$, $q>2$

The Threshold Conjecture for $k=1$, $q>2$ is proved in two steps: first $n=2$ then $n\ge 3$. For $n=2$, the cases $q=3$ and $q\ge 4$ require different treatments. The group of all invertible semi-affine transformations of $\mathbb{F}_q^n$ is denoted by $\mathrm{A\Gamma L}(n,\mathbb{F}_q)$. For any two distinct points $x,y\in\mathbb{F}_q^n$, $\overline{xy}$ denotes the line through x and y in $\mathbb{F}_q^n$.

Theorem 8.1. *Let $q\ge 4$ and $f\in\mathrm{Per}(\mathbb{F}_q^2)\setminus\mathrm{A\Gamma L}(2,\mathbb{F}_q)$. Then*

$$\text{1-coaffinity}(f)\ge 2q\begin{bmatrix}1\\1\end{bmatrix}_q=2q.$$

Proof. Among the $q+1$ parallel classes of lines in $\mathbb{F}_q^2$, we first assume that at most one parallel class has the property that all lines in the class are mapped to lines by f. In each of the remaining q parallel classes, there are at least 2 lines which are not mapped to lines by f. (Since the lines in a parallel class form a partition of $\mathbb{F}_q^2$, it cannot be the case that exactly one line in a parallel class is not mapped to a line.) Therefore 1-coaffinity$(f) \geq 2q$.

Now assume that there are two parallel classes of lines in $\mathbb{F}_q^2$ such that all lines in the two parallel classes are mapped to lines by f. By composing suitable linear transformations to both sides of f, we may assume that f maps all horizontal lines to horizontal lines and all vertical lines to vertical lines. (A horizontal line in $\mathbb{F}_q^2$ is a line with direction vector $(1,0)$; a vertical line in $\mathbb{F}_q^2$ is a line with direction vector $(0,1)$.)

Assume that for every $z \in \mathbb{F}_q^2$, there is a line through z which is not mapped to a line by f. Then there are at least two lines through z which are not mapped to lines. Since each line contains q points, we have

$$\text{1-coaffinity}(f) \geq \frac{2q^2}{q} = 2q.$$

Therefore, we may assume that there exists $z \in \mathbb{F}_q^2$ such that all lines through z are mapped to lines by f. Using suitable affine transformations, we may further assume that

(i) f maps all horizontal (vertical) lines to horizontal (vertical) lines,
(ii) $f(0,0) = (0,0)$, $f(1,0) = (1,0)$, $f(0,1) = (0,1)$,
(iii) all lines through $(0,0)$ are mapped to lines.

Let

$$\begin{aligned} f(x,0) &= (\phi(x), 0) \qquad \forall x \in \mathbb{F}_q, \\ f(0,y) &= (0, \psi(y)) \qquad \forall y \in \mathbb{F}_q, \end{aligned}$$

where ϕ and ψ are permutations of $\mathbb{F}_q$ with $\phi(0) = \psi(0) = 0$ and $\phi(1) = \psi(1) = 1$. For any $(x,y) \in \mathbb{F}_q^2$, it is the intersection of the vertical line through $(x,0)$ and the horizontal line through $(0,y)$. Hence $f(x,y)$ is the intersection of the vertical line through $(\phi(x),0)$ and the horizontal line through $(0,\psi(y))$, i.e.,

$$f(x,y) = \big(\phi(x),\, \psi(y)\big).$$

Since $f(1,1) = (1,1)$, by (iii), the line $\{(x,x) : x \in \mathbb{F}_q\}$ is mapped to itself. Hence $\phi = \psi$. Let $k \in \mathbb{F}_q$. By (iii), $f\big(\{(x,kx) : x \in \mathbb{F}_q\}\big) = \{(\phi(x), \phi(kx)) : x \in \mathbb{F}_q\}$ is a line. Hence

$$\frac{\phi(kx)}{\phi(x)} = g(k) \quad \forall x \in \mathbb{F}_q \setminus \{0\},$$

where $g(k) \in \mathbb{F}_q$ is a function of k. Setting $x = 1$, we have $g(k) = \phi(k)$. Thus

$$\phi(kx) = \phi(k)\phi(x) \quad \text{for all } x, k \in \mathbb{F}_q. \tag{8.1}$$

Assume that for every $a \in \mathbb{F}_q \setminus \{0\}$, all lines through $(a,0)$ which are neither horizontal nor vertical are not mapped to lines. Then we have

$$\text{1-coaffinity}(f) \geq (q-1)(q+1-2) > 2q,$$

since $q \geq 4$.

Therefore, we may assume that there exist $a \in \mathbb{F}_q \setminus \{0\}$ and a line L through $(a,0)$ such that L is neither horizontal nor vertical and $f(L)$ is a line. Let $(0,b) \in L$, where $b \in \mathbb{F}_q \setminus \{0\}$. Then $f(L)$ is the line through $(\phi(a), 0)$ and $(0, \phi(b))$. (See Figure 1.) For each $x \in \mathbb{F}_q$, the intersection of L and the vertical line through $(x, 0)$ is

$$\big(x,\ -\frac{b}{a}(x-a)\big);$$

the intersection of $f(L)$ and the vertical line through $(\phi(x), 0)$ is

$$\Big(\phi(x),\ -\frac{\phi(b)}{\phi(a)}\big(\phi(x)-\phi(a)\big)\Big).$$

By (i), we have

$$\phi\big(-\frac{b}{a}(x-a)\big) = -\frac{\phi(b)}{\phi(a)}\big(\phi(x)-\phi(a)\big).$$

Using (8.1), we obtain

$$\phi(a-x) = \phi(a) - \phi(x). \tag{8.2}$$

For any $b, x \in \mathbb{F}_q$, by (8.1) and (8.2),

$$\phi(ba-bx) = \phi(b)\phi(a-x) = \phi(b)\big(\phi(a)-\phi(x)\big) = \phi(ba) - \phi(bx). \tag{8.3}$$

Combining (8.1) and (8.3), ϕ is an automorphism of $\mathbb{F}_q$. Hence $f \in \mathrm{A\Gamma L}(2, \mathbb{F}_q)$, which is a contradiction. $\square$

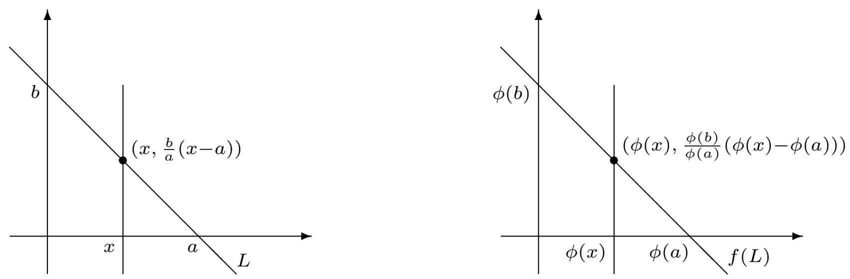

Figure 1. Proof of Theorem 8.1

Theorem 8.2. *Let $f \in \mathrm{Per}(\mathbb{F}_3^2) \setminus \mathrm{AGL}(2, \mathbb{F}_3)$. Then*

$$1\text{-coaffinity}(f) \geq 6.$$

The equality holds if and only if $f \in \mathrm{AGL}(2, \mathbb{F}_3) \circ \tau \circ \mathrm{AGL}(2, \mathbb{F}_3)$, where $\tau \in \mathrm{Per}(\mathbb{F}_3^n)$ is any transposition.

Proof. **Case 1**. There do not exist two nonparallel lines in $\mathbb{F}_3^2$ which are mapped into lines by f. Then

$$1\text{-coaffinity}(f) \geq 3\big(\frac{3^2-1}{3-1} - 1\big) = 9 > 6.$$

Case 2. There are two nonparallel lines L_1 and L_2 in $\mathbb{F}_3^2$ which are mapped into lines. Note that f is affine on each of these two lines. (This a special property of $\mathbb{F}_3$.) Therefore, through suitable affine transformations, we may assume that $L_1 = \mathbb{F}_3 \times \{0\}$, $L_2 = \{0\} \times \mathbb{F}_3$ and that $f|_{L_1} = \mathrm{id}$, $f|_{L_2} = \mathrm{id}$.

Case 2.1. f moves exactly two elements in $\mathbb{F}_3^2 \setminus (L_1 \cup L_2) = \{1, -1\} \times \{1, -1\}$. f is a transposition and $1\text{-coaffinity}(f) = 6$.

Case 2.2. f moves exactly three elements in $\{1,-1\}\times\{1,-1\}$, say, $f=(a_1,a_2,a_3)$ where $\{1,-1\}\times\{1,-1\}=\{a_1,a_2,a_3,a_4\}$. For each $a\in\{1,-1\}\times\{1,-1\}$, let L_a be the unique line through a such that $|L_a\cap(L_1\cup L_2)|=2$. Then $f(L_{a_i})$ $(1\le i\le 3)$ is not a line since a_i is not fixed by f but the other two points on L_{a_i} are. Note that the third point on the line $\overline{a_4a_i}$ $(1\le i\le 3)$ is on $L_1\cup L_2$. Thus $f(\overline{a_4a_i})$ $(1\le i\le 3)$ is not a line. We also claim that for $1\le i<j\le 3$, $f(\overline{a_ia_j})$ is not a line. Otherwise, without loss of generality, assume that $f(\overline{a_1a_2})$ is a line. $\overline{a_1a_2}$ must intersect $L_1\cup L_2$, say, at a_0. Note that $a_0,a_2\in f(\overline{a_1a_2})$. Hence $f(\overline{a_1a_2})=\overline{a_0a_2}=\overline{a_0a_1}$. Thus $a_2,a_3\in f(\overline{a_1a_2})=\overline{a_0a_1}$, which is impossible.

Therefore,

$$\text{1-coaffinity}(f)\ge 3+\binom{4}{2}=9>6.$$

Case 2.3. $f=(a_1,a_2,a_3,a_4)$, where $\{1,-1\}\times\{1,-1\}=\{a_1,a_2,a_3,a_4\}$. By the argument in Cases 2.2, $f(L_{a_i})$ $(1\le i\le 4)$ and $f(\overline{a_1a_2})$, $f(\overline{a_2a_3})$, $f(\overline{a_3a_4})$, $f(\overline{a_4a_1})$ are not lines. Hence

$$\text{1-coaffinity}(f)\ge 8>6.$$

Case 2.4. $f=(a_1,a_2)(a_3,a_4)$, where $\{1,-1\}\times\{1,-1\}=\{a_1,a_2,a_3,a_4\}$. Assume $a_1=(1,1)$. If $a_2=(1,-1)$, let $g\in\mathrm{GL}(2,\mathbb{F}_3)$ be given by

$$g(x,y)=(x,-y).$$

Then it is easy to see that $g\circ f$ is the transposition which moves $(0,1)$ and $(0,-1)$.

If $a_2=(-1,1)$, let $h\in\mathrm{GL}(2,\mathbb{F}_3)$ be given by

$$h(x,y)=(-x,y).$$

Then $h\circ f$ is the transposition which moves $(1,0)$ and $(-1,0)$.

If $a_2=(-1,-1)$, then $f(L_{a_i})$ $(1\le i\le 4)$ and $f(\overline{a_1a_3})$, $f(\overline{a_1a_4})$, $f(\overline{a_2a_3})$, $f(\overline{a_2a_4})$ are not lines. Hence

$$\text{1-coaffinity}(f)\ge 8>6.$$

□

We now turn to the proof of the Threshold Conjecture with $k=1$, $q>2$ and $n\ge 3$.

Lemma 8.3. *Let $m\ge n\ge 2$ and let $f:\mathbb{F}_q^n\to\mathbb{F}_q^m$ be a one-to-one mapping which is not semi-affine. Let* 1-coaffinity(f) *denote the number of lines L in $\mathbb{F}_q^n$ such that $f(L)$ is not a line in $\mathbb{F}_q^m$. Then*

$$\text{1-coaffinity}(f)\ge\frac{q^n-1}{q-1}.$$

Proof. Use induction on n. First assume $n=2$.

Case 1. There do not exist two nonparallel lines in $\mathbb{F}_q^2$ which are not mapped into line by f. Then

$$\text{1-coaffinity}(f)\ge q(q+1-1)>q+1.$$

Case 2. There are two nonparallel lines L_1 and L_2 in $\mathbb{F}_q^2$ such that $f(L_1)$, $f(L_2)$ are lines in $\mathbb{F}_q^m$. Since $f(L_1)$ and $f(L_2)$ are intersecting lines in $\mathbb{F}_q^m$, their affine span in $\mathbb{F}_q^m$ is a 2-flat which, without loss of generality, is assumed to be $\mathbb{F}_q^2\times\{0\}$.

If for every line L_3 in $\mathbb{F}_q^2$ such that $L_i\cap L_j$ $(1\le i<j\le 3)$ are 3 distinct points $f(L_3)$ is not a line, then

$$\text{1-coaffinity}(f)\ge(q-1)^2\ge q+1.$$

So, we assume that there exists a line L_3 in $\mathbb{F}_q^2$ such that $L_i \cap L_j$ $(1 \le i < j \le 3)$ are 3 distinct points and $f(L_3)$ is a line in $\mathbb{F}_q^m$. Since $f(L_1) \cup f(L_2) \subset \mathbb{F}_q^2 \times \{0\}$, it follows that $f(L_3) \subset \mathbb{F}_q^2 \times \{0\}$.

If $f(\mathbb{F}_q^2) \subset \mathbb{F}_q^2 \times \{0\}$, by Theorems 8.1 and 8.2,

$$1\text{-coaffinity}(f) \ge 2q > q+1.$$

So we assume that $f(\mathbb{F}_q^2) \not\subset \mathbb{F}_q^2 \times \{0\}$.

Let $a \in \mathbb{F}_q^2 \setminus (L_1 \cup L_2 \cup L_3)$ such that $f(a) \notin \mathbb{F}_q^2 \times \{0\}$. If L is a line through a such that $|L \cap (L_1 \cup L_2 \cup L_3)| \ge 2$, then $f(L)$ is not a line since two points on L (belonging to $L \cap (L_1 \cup L_2 \cup L_3)$) are mapped to $\mathbb{F}_q^2 \times \{0\}$ by f but a is not mapped to $\mathbb{F}_q^2 \times \{0\}$. There are only 3 lines L_i' $(i = 1, 2, 3)$ in $\mathbb{F}_q^2$ such that $|L_i' \cap (L_1 \cup L_2 \cup L_3)| < 2$: the lines through $L_j \cap L_k$ and parallel to L_i where $\{i, j, k\} = \{1, 2, 3\}$.

If there are two points $a_1, a_2 \in \mathbb{F}_q^2 \setminus (L_1 \cup L_2 \cup L_3)$ such that $f(a_i) \notin \mathbb{F}_q^2 \times \{0\}$, $i = 1, 2$, then for any line L in $\mathbb{F}_q^2$ through a_1 or a_2 with $L \ne L_i'$, $i = 1, 2, 3$, $f(L)$ is not a line. Hence

$$1\text{-coaffinity}(f) \ge 2(q+1) - 1 - 3 \ge q+1.$$

If there is exactly one point $a \in \mathbb{F}_q^2 \setminus (L_1 \cup L_2 \cup L_3)$ such that $f(a) \notin \mathbb{F}_q^2 \times \{0\}$, then every line in $\mathbb{F}_q^2$ through a is not a line in $\mathbb{F}_q^m$. Thus,

$$1\text{-coaffinity}(f) \ge q+1.$$

Now assume $n \ge 3$.

Case 1. For any two nonparallel hyperplanes H_1 and H_2 in $\mathbb{F}_q^n$, f is not semi-affine on at least one of H_1 and H_2. Then f is not semi-affine on at least

$$q\Big(\frac{q^n-1}{q-1} - 1\Big) = \frac{q^2(q^{n-1}-1)}{q-1}$$

hyperplanes in $\mathbb{F}_q^n$. By the induction hypothesis, at least $\frac{q^{n-1}-1}{q-1}$ lines on each of these hyperplanes are not mapped into lines. Since each line in $\mathbb{F}_q^n$ lies in $\frac{q^{n-1}-1}{q-1}$ hyperplanes, we have

$$1\text{-coaffinity}(f) \ge \frac{\frac{q^2(q^{n-1}-1)}{q-1} \cdot \frac{q^{n-1}-1}{q-1}}{\frac{q^{n-1}-1}{q-1}} = \frac{q^2(q^{n-1}-1)}{q-1} > \frac{q^n-1}{q-1}. \tag{8.4}$$

Case 2. There are two nonparallel hyperplanes H_1 and H_2 in $\mathbb{F}_q^n$ such that f is semi-affine on both H_1 and H_2. Since $f(H_1)$ and $f(H_2)$ are $(n-1)$-flats in $\mathbb{F}_q^m$ whose intersection is an $(n-2)$-flat, their affine span in $\mathbb{F}_q^m$ is an n-flat which, without loss of generality, is assumed to be $\mathbb{F}_q^n \times \{0\}$. Through a suitable semi-affine transformation, we may assume that

$$f(x) = (x, 0) \quad \text{for all } x \in H_1. \tag{8.5}$$

Since $f(x) = (x, 0)$ for all $x \in H_1 \cap H_2$ and since $\dim(H_1 \cap H_2) \ge 1$, $f|_{H_2}$ must be affine. Then it is clear that through an additional affine transformation, we may assume that in addition to (8.5),

$$f(x) = (x, 0) \quad \text{for all } x \in H_2. \tag{8.6}$$

Thus we have

$$f(x) = (x, 0) \quad \text{for all } x \in H_1 \cup H_2. \tag{8.7}$$

Case 2.1. For every hyperplane H_3 in $\mathbb{F}_q^n$ such that $H_i \cap H_j$ $(1 \le i < j \le 3)$ are 3 distinct $(n-2)$-flats, f is not semi-affine on H_3. By the induction hypothesis, at least $\frac{q^{n-1}-1}{q-1}$ lines on H_3 are not mapped into lines. The number of such hyperplanes H_3 is $q(\frac{q^n-1}{q-1} - 2) - (q-1)$. By the same argument for (8.4), we have

$$\text{1-coaffinity}(f) \ge q(\frac{q^n-1}{q-1} - 2) - (q-1) > \frac{q^n-1}{q-1}. \tag{8.8}$$

Case 2.2. There exists a hyperplane H_3 in $\mathbb{F}_q^n$ such that $H_i \cap H_j$ $(1 \le i < j \le 3)$ are 3 distinct $(n-2)$-flats and f is semi-affine on H_3. By (8.7),

$$f(x) = (x, 0) \quad \text{for all } x \in (H_3 \cap H_1) \cup (H_3 \cap H_2).$$

Since $H_3 \cap H_1$ and $H_3 \cap H_2$ affinely span H_3, we have

$$f(x) = (x, 0) \quad \text{for all } x \in H_3.$$

Thus

$$f(x) = (x, 0) \quad \text{for all } x \in H_1 \cup H_2 \cup H_3.$$

Since f is not semi-affine, $f(a) \ne (a, 0)$ for some $a \in \mathbb{F}_q \setminus (H_1 \cup H_2 \cup H_3)$. If L is a line through a such that $|L \cap (H_1 \cup H_2 \cup H_3)| \ge 2$ and $f(a) \notin L \times \{0\}$, then $f(L)$ is not a line. (Let $b_1, b_2 \in L \cap (H_1 \cup H_2 \cup H_3)$. Then $f(b_i) = (b_i, 0) \in L \times \{0\}$, but $f(a) \notin L \times \{0\}$.) We claim that number of lines L in $\mathbb{F}_q^n$ through a with $|L \cap (H_1 \cup H_2 \cup H_3)| \le 1$ is

$$7 \cdot q^{n-3} + \frac{q^{n-3}-1}{q-1}. \tag{8.9}$$

In fact, we may assume

$$\begin{aligned} H_1 &= \{0\} \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^{n-3}, \\ H_2 &= \mathbb{F}_q \times \{0\} \times \mathbb{F}_q \times \mathbb{F}_q^{n-3}, \\ H_3 &= \mathbb{F}_q \times \mathbb{F}_q \times \{0\} \times \mathbb{F}_q^{n-3}. \end{aligned}$$

Let $a = (a^{(1)}, a^{(2)}, a^{(3)}, \dots)$ where $a^{(1)}, a^{(2)}, a^{(3)} \in \mathbb{F}_q \setminus \{0\}$ and let L be a line through a with direction vector $v = (v^{(1)}, v^{(2)}, v^{(3)}, \dots)$. Then $|L \cap (H_1 \cup H_2 \cup H_3)| \le 1$ if and only if one of the following is true:

(i) at least two of $v^{(1)}, v^{(2)}, v^{(3)}$ are 0;
(ii) $v^{(k)} = 0$ and $(v^{(i)}, v^{(j)}) = t(a^{(i)}, a^{(j)})$ for some $t \in \mathbb{F}_q \setminus \{0\}$ where $\{i, j, k\} = \{1, 2, 3\}$;
(iii) $(v^{(1)}, v^{(2)}, v^{(3)}) = t(a^{(1)}, a^{(2)}, a^{(3)})$ for some $t \in \mathbb{F}_q \setminus \{0\}$.

Formula (8.9) follows from these conditions.

Therefore, the number of lines L in $\mathbb{F}_q^n$ through a such that $|L \cap (H_1 \cup H_2 \cup H_3)| \ge 2$ and $f(a) \notin L \times \{0\}$ is at least

$$\frac{q^n-1}{q-1} - 7q^{n-3} - \frac{q^{n-3}-1}{q-1} - 1 = q^{n-3}(q^2 + q - 6) - 1. \tag{8.10}$$

First assume that there are at least 4 points $a_1, \dots, a_4 \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$ such that $f(a_i) \neq (a_i, 0)$. From the above,

$$\begin{aligned}
\text{1-coaffinity}(f) &\geq 4\big[q^{n-3}(q^2+q-6)-1\big] - \binom{4}{2} \\
&= 4q^{n-3}(q^2+q-6) - 10 \\
&> \frac{q^n-1}{q-1}.
\end{aligned}$$

Next, assume that there are exactly s points $a_1, \dots, a_s \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$, where $s = 2$ or 3, such that $f(a_i) \neq (a_i, 0)$, $1 \leq i \leq s$. Then for every line L passing through exactly one of $a_1, \dots, a_s$, $f(L)$ is not a line. Hence

$$\text{1-coaffinity}(f) \geq s \cdot \frac{q^n-1}{q-1} - 2\binom{s}{2} > \frac{q^n-1}{q-1}.$$

Finally, assume that there is exactly one point $a \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$ such that $f(a) \neq (a, 0)$. Then the lines in $\mathbb{F}_q^n$ which are not mapped into lines by f are precisely the ones passing through a. Thus,

$$\text{1-coaffinity}(f) = \frac{q^n-1}{q-1}.$$

□

Theorem 8.4. *Let $n \geq 3$ and $f \in \mathrm{Per}(\mathbb{F}_q^n) \setminus \mathrm{A\Gamma L}(n, \mathbb{F}_q)$. Then*

$$\text{1-coaffinity}(f) \geq 2q\begin{bmatrix} n-1 \\ 1 \end{bmatrix}_q = \frac{2q(q^{n-1}-1)}{q-1}.$$

The equality holds if and only if $f \in \mathrm{A\Gamma L}(n, \mathbb{F}_q) \circ \tau \circ \mathrm{A\Gamma L}(n, \mathbb{F}_q)$, where $\tau \in \mathrm{Per}(\mathbb{F}_q^n)$ is any transposition.

Proof. The arguments in this proof are very similar to those in the proof of Lemma 8.3.

Case 1. For any two nonparallel hyperplanes H_1 and H_2 in $\mathbb{F}_q^n$, f is not semi-affine on at least one of H_1 and H_2. By Lemma 8.3 and (8.4),

$$\text{1-coaffinity}(f) \geq \frac{q^2(q^{n-1}-1)}{q-1} > \frac{2q(q^{n-1}-1)}{q-1}.$$

Case 2. There are two nonparallel hyperplanes H_1 and H_2 in $\mathbb{F}_q^n$ such that f is semi-affine on both H_1 and H_2. By the proof of Lemma 8.3, we may assume that $f|_{H_1} = \mathrm{id}$, $f|_{H_2} = \mathrm{id}$.

Case 2.1. For every hyperplane H_3 in $\mathbb{F}_q^n$ such that $H_i \cap H_j$ $(1 \leq i < j \leq 3)$ are 3 distinct $(n-2)$-flats, f is not semi-affine on H_3. By (8.8), we have

$$\text{1-coaffinity}(f) \geq q\Big(\frac{q^n-1}{q-1} - 2\Big) - (q-1) > \frac{2q(q^{n-1}-1)}{q-1}.$$

Case 2.2. There exists a hyperplane H_3 in $\mathbb{F}_q^n$ such that $H_i \cap H_j$ $(1 \leq i < j \leq 3)$ are 3 distinct $(n-2)$-flats and f is semi-affine on H_3. By the same argument in Case 2.2 of the proof of Lemma 8.3, we have

$$f(x) = x \quad \text{for all } x \in H_1 \cup H_2 \cup H_3.$$

First assume that there are at least 5 elements $a_1, \dots, a_5 \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$ such that $f(a_i) \neq a_i$, $1 \le i \le 5$. By (8.10), we have

$$\text{1-coaffinity}(f) \ge 5\big[q^{n-3}(q^2+q-6)-1\big] - \binom{5}{2} = 5q^{n-3}(q^2+q-6) - 15. \tag{8.11}$$

When $q \ge 4$, we have

$$5q^{n-3}(q^2+q-6) - 15 > \frac{2q(q^{n-1}-1)}{q-1}.$$

When $q = 3$, any line L in $\mathbb{F}_3^n$ with $|L \cap (H_1 \cup H_2 \cup H_3)| \ge 2$ cannot pass through more than one of $a_1, \dots, a_5$ since $|L| = 3$. Thus (8.11) can be improved to

$$\text{1-coaffinity}(f) \ge 5\big[q^{n-3}(q^2+q-6)-1\big] > \frac{2q(q^{n-1}-1)}{q-1}.$$

Next, assume that there are exactly s elements $a_1, \dots, a_s \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$, where $s = 3$ or 4, such that $f(a_i) \neq a_i$, $1 \le i \le s$. Then for every line L passing through exactly one of $a_1, \dots, a_s$, $f(L)$ is not a line. Hence

$$\text{1-coaffinity}(f) \ge s\,\frac{q^n-1}{q-1} - 2\binom{s}{2} = \frac{s}{q-1}\big[q^n - (s-1)q + s - 2\big] > \frac{2q(q^{n-1}-1)}{q-1}.$$

Finally, assume that there are exactly 2 elements $a_1, a_2 \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$ such that $f(a_i) \neq a_i$, $i = 1, 2$. Then f is a transposition. □

Combining Theorems 8.1, 8.2 and 8.4, we have the following corollary.

Corollary 8.5. *The Threshold Conjecture holds for $q \ge 3$, $k = 1$ and $n > 1$.*

Remark. Theorems 8.2 and 8.4 state that for $q = 3$, $k = 1$, $n \ge 2$ or $q > 3$, $k = 1$, $n \ge 3$, $\text{1-coaffinity}(f) = 2q\begin{bmatrix} n-1 \\ 1 \end{bmatrix}_q$ only when $f \in \mathrm{A\Gamma L}(n, \mathbb{F}_q) \circ \tau \circ \mathrm{A\Gamma L}(n, \mathbb{F}_q)$ for some transposition $\tau \in \mathrm{Per}(\mathbb{F}_q^n)$. It is an open question whether the same holds for $q > 3$, $k = 1$ and $n = 2$.

Acknowledgment

The proof of Theorem 8.1 is based on a method by Professor W-X. Ma.

References

[1] T. Beth and C. Ding, *On almost perfect nonlinear permutations*, Eurocrypt '93 (Lofthus, 1993) Lecture Notes in Computer Science **765**, 65 – 76, Springer, 1994.
[2] C. Carlet, P. Charpin, V. Zinoview, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs, Codes and Cryptography, **15** (1998), 125 – 156.
[3] H. Dobbertin, *Almost perfect nonlinear power functions on* GF(2^n)*: the Niho case*, Inform. Comput. **151** (1999), 57 – 72.
[4] H. Dobbertin, *Almost perfect nonlinear power functions on* GF(2^n)*: a new case for n divisible by* 5, Finite Fields and Applications (Augsburg, 1999), 113–121, Springer, Berlin, 2001.
[5] X. Hou, *Affinity of permutations of* $\mathbb{F}_2^n$, Discrete Appl. Math., to appear.
[6] P. Langevin, *On the orphans and covering radius of the Reed-Muller codes*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (New Orleans, LA, 1991), Lecture Notes in Computer Science **539**, 234 – 240, Springer, Berlin, 1991.
[7] K. Nyberg, *Differentially uniform mappings for cryptography*, Eurocrypt '93 (Lofthus, 1993) Lecture Notes in Computer Science **765**, 55 – 64, Springer, 1994.
[8] K. Nyberg, *S-boxes and round functions with controllable linearity and differential uniformity*, Fast Software Encryption (Leuven, 1994), Lecture Notes in Computer Science **1008**, 111 – 130, Springer, Berlin, 1995.

[9] E. Snapper and R. J. Troyer, *Metric Affine Geometry*, Academic Press, New York and London 1971.

Department of Mathematics, University of South Florida, Tampa, FL 33620
E-mail address: eclark@math.usf.edu

Department of Mathematics, University of South Florida, Tampa, FL 33620
E-mail address: xhou@tarski.math.usf.edu

Department of Mathematics, Tennessee Technological University, Cookeville, TN 38505
E-mail address: alec@mihailovs.com