DE A E A C

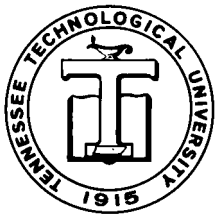
EC CA E

E A A A E A
A A E EC ACE

D . ED C A
D . A -D
D . A EC A

2004

. 2004-3



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

Definition 1.1.

It is well known that the number of k-dimensional subspaces of 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 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 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 $f \in \mathrm{Per}(\mathrm{F}_q^n)$.

The present paper is a continuation of the second author's work [5]. In [5], the notion of 2-affinity of permutations of F_2^n was implicitly introduced and permutations of F_2^n with 2-affinity 0 were studied. We point out that a permutation $f \in \mathrm{Per}(\mathrm{F}_2^n)$ 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 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, $q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$.) 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 $\mathrm{Per}(\mathrm{F}_q^n)$ 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 -affinity(f). For example, there are permutations f_1, f_2, f_3, f_4 in

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

$$1\text{-a}\square\text{nity}(f_1) = 1 \text{ and } 2\text{-a}\square\text{nity}(f_1) = 0$$
$$1\text{-a}\square\text{nity}(f_2) = 0 \text{ and } 2\text{-a}\square\text{nity}(f_2) = 1$$
$$1\text{-a}\square\text{nity}(f_3) = 0 \text{ and } 2\text{-a}\square\text{nity}(f_3) = 0$$
$$1\text{-a}\square\text{nity}(f_4) = 1 \text{ and } 2\text{-a}\square\text{nity}(f_4) = 1$$

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

Theorem 2.1.

(i) *If* $q = 2$ *and* $n \ge 3$ *is odd, there exists* $f \in \mathrm{Per}(\mathrm{F}_2^n)$ *such that* 2-a$\square$nity$(f) = 0$.
(ii) *If* $q = 2$ *and* $n \ge 4$ *, there exists* $f \in \mathrm{Per}(\mathrm{F}_2^n)$ *such that* k-a$\square$nity$(f) = 0$ *for all* $3 \le k \le n-1$.
(iii) *If* $q \ge 4$ *and* $n \ge 2$*, there exists* $f \in \mathrm{Per}(\mathrm{F}_q^n)$ *such that* k-a$\square$nity$(f) = 0$ *for all* $1 \le k \le n-1$.
(iv) *If* $q = 3$ *and* $n \ge 3$*, there exists* $f \in \mathrm{Per}(\mathrm{F}_3^n)$ *such that* k-a$\square$nity$(f) = 0$ *for all* $2 \le k \le n-1$.
(v) *If* $q = 3$ *and* $n \ge 2$*, there exists* $f \in \mathrm{Per}(\mathrm{F}_3^n)$ *such that* 1-a$\square$nity$(f) = 0$.

The proof of Theorem 2.1 is spread out in parts in the rest of this section. Part

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 $f(\pi_1(X)) = \pi_1((f \times g)(X))$ 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

Clearly,

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

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 $q \geq 4$, $k \geq 1$, or $q = 3$, $k \geq 2$, or $q = 2$, $k \geq 3$,*

$$\left(\frac{k}{q^{k+1}}\right)^q < \frac{1}{q^{q^k-k}}. \tag{3.4}$$

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 $1 \leq i \leq q^k-4$,

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

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

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

Let

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

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:

$$\left(\frac{\binom{4}{2}}{2^3}\right)^2=\frac{5}{286}<\frac{1}{32}=\frac{1}{2^{2^3-3}}.$$

□

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,

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

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

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

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

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 $\varphi_i \in \mathrm{Per}(\mathbb{F}_2)$, $i = 1, 2$, such that

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

Clearly, $b_1 = b_2$. Since $\mathbb{F}_2$ has only two permutations, $t \to t$ or $t \to t+1$, we see that $\varphi_1 + \varphi_2$ 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 $f(x) \in H(b_i, \varphi_i(t))$. It follows that

$$\langle b_1 + b_2, f(x)\rangle = \varphi_1(t) + \varphi_2(t) = \epsilon,$$

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

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 $X \subseteq \mathbb{F}_2^n$ 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

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

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

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

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

$$k\text{-a□nity}(f) > \frac{(q^{n-k}-2)(q^n-1)}{q^k-1} + 2\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q,$$

then k-a□nity$(f) = q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$. *That is, the next to largest* k*-a nity 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 a□ne 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 P_n. Every function in P_n is uniquely represented by a polynomial in $\mathbb{F}_2[X_1, \ldots, X_n]$ whose degree in each X_i is at most 1. Namely,

$$P_n = \mathbb{F}_2[X_1, \ldots, X_n]/\langle X_1^2 - X_1, \ldots, X_n^2 - X_n \rangle.$$

For each $g \in P_n$, put $|g| = |g^{-1}(1)|$. The Fourier transform of $g \in P_n$ 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

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

and

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

(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 $A \leq \sum \hat{g}(a)^2 \leq B$

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

$$
\begin{aligned}
2^n\left(\frac{B-A}{2}\right)^2 &\geq \sum_{a \in \mathbb{F}_2^n}\left(\hat{g}(a)^2 - \frac{A+B}{2}\right)^2 \\
&= \sum_{a \in \mathbb{F}_2^n}\hat{g}(a)^4 - (A+B)\sum_{a \in \mathbb{F}_2^n}\hat{g}(a)^2 + 2^n\left(\frac{A+B}{2}\right)^2 \\
&= \sum_{a \in \mathbb{F}_2^n}\hat{g}(a)^4 - 2^{2n}(A+B) + 2^n\left(\frac{A+B}{2}\right)^2.
\end{aligned}
$$

Thus

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

Combining the above with (7.3), we have

B A n A n 4

(7.4)

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 $h \in P_n$ 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 $\hat{g}(a)^2 = 2^2$ 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*

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

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 $q = 2$, $k = 2$, $n > 2$.*

Then

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

We have

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

Therefore,

$$2\text{-coa}\square\text{nity}(f) = \frac{1}{3}|G| \geq \frac{8}{3}(2^{n-1}-1)(2^{n-2}-1).$$

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 $h \in P_{n-1}$ 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,

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

is a transposition.

Case 2. $f(x + d) + f(x) =$ 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, $f(\Delta(d)) = \Delta(c)$ 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

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

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

$$\Big|f(\Delta(d)) \cap \sum_{a \in A} \Delta(a)\Big| \geq 2,$$

$$\Big|f(\Delta(d)) \cap \sum_{b \in B} \Delta(b)\Big| \geq 2.$$

Note that $\Delta(a)$, $a \in \mathbb{F}_2^n \setminus \{0\}$ form a partition of $\binom{\mathbb{F}_2^n}{2}$. If $|f(\Delta(d)) \cap \Delta(a)| \leq 1$ 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 $|f(\Delta(d)) \cap \Delta(a_i)| = 1$, $i = 1, 2$. Then $A = \{a_1, a_2\}$, $B = \mathbb{F}_2^n \setminus \{0, a_1, a_2\}$ have the desired property. If $|f(\Delta(d)) \cap \Delta(a)| \geq 2$ 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

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

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

$$2\text{-affinity}(f) \geq \frac{2 \cdot (2^{n-1} - 2) \cdot (2^n - 1)}{}$$

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

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

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

( ) Assume to the contrary that $f(a) + f(0) = a$. Then $f\{0, a\} = \{0, a\}$. Without loss of generality, we may assume $f^{-1}(0) \neq \{0, a\}$. By the proof of ( ) of (i), it suffices to show that there is a 2-flat A

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-coa□nity$(f) \geq 2q$.

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

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

where $b \in \mathbb{F}_q \setminus \{0\}$. Then $f(L)$ is the line through $(\varphi(a), 0)$ and $(0, \varphi(b))$. (See Figure 1.) For each $x \in \mathbb{F}_q$, the intersection of L and the vertical line through $(x, 0)$ is

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

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

$$\left(\varphi(x), \ -\frac{\varphi(b)}{\varphi(a)}\left(\varphi(x) - \varphi(a)\right)\right).$$

By (i), we have

$$\varphi\left(-\frac{b}{a}(x-a)\right) = -\frac{\varphi(b)}{\varphi(a)}\left(\varphi(x) - \varphi(a)\right).$$

Using (8.1), we obtain

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

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

$$\varphi(ba - bx) = \varphi(b)\varphi(a-x) = \varphi(b)\left(\varphi(a) - \varphi(x)\right) = \varphi(ba) - \varphi(bx). \tag{8.3}$$

Combining (8.1) and (8.3), φ Γ-34Td[(602389.963Tf0-501(A)-500(PERMUTbF1158-2Γ-50T87)]TF15119F1

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

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

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

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

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

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

□

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

$$\text{1-coa}\square\text{nity}(f) \geq 2q\binom{n-1}{1}_q = \frac{2q(q^{n-1}-1)}{q-1}.$$

The equality holds if and only if $f \in \mathrm{A\Gamma L}(n, \mathrm{F}_q) \circ \tau \circ \mathrm{A\Gamma L}(n, \mathrm{F}_q)$, where $\tau \in \mathrm{Per}(\mathrm{F}_q^n)$ 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 F_q^n, f is not semi-a□ne on at least one of H_1 and H_2. By Lemma 8.3 and (8.4),

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

Case 2. There are two nonparallel hyperplanes H_1 and H_2 in F_q^n such that f is semi-a□ne 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 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-a□ne on H_3. By (8.8), we have

$$\text{1-coa}\square\text{nity}(f) \geq q\left[\frac{q^n-1}{q-1} - 2\right] - (q-1) > \frac{2q(q^{n-1}-1)}{q-1}.$$

Case 2.2. There exists a hyperplane H_3 in 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-a□ne 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 $a_1, \ldots, a_5 \in \mathbb{F}_q^n \setminus (H_1 \cup H_2 \cup H_3)$ such that $f(a_i) = a_i$, $1 \le i \le 5$. By (8.10), we have

$$\text{1-coa}\square\text{nity}(f) \ge 5\left[q^{n-3}(q^2+q-6) - 1\right] - \binom{5}{2} = 5q^{n-3}(q^2+q-6) - 15. \tag{8.11}$$

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 $|L \cap (H_1 \cup H_2 H_{1974}\text{T}\text{f}4.84\text{H}$

[9] E. Snapper and R. J. Troyer, *Metric A ne 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