Affinity of Permutations of $\mathbb{F}_2^n$

Xiang-dong Hou

Department of Mathematics and Statistics,
Wright State University,
Dayton, Ohio 45435
xhou@euler.math.wright.edu

Abstract

A conjecture by Canteaut and Dobbertin states that if n is even, then every permutation of $\mathbb{F}_2^n$ is affine on some 2-dimensional affine subspace of $\mathbb{F}_2^n$. We prove that the conjecture is true for $n = 4$ and for quadratic permutations of $\mathbb{F}_2^n$. The conjecture is actually a claim about $(\mathrm{AGL}(n,2), \mathrm{AGL}(n,2))$-double cosets in permutation group $S(\mathbb{F}_2^n)$ of $\mathbb{F}_2^n$. We give a formula for the number of $(\mathrm{AGL}(n,2), \mathrm{AGL}(n,2))$-double cosets in $S(\mathbb{F}_2^n)$ and classify the $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-double cosets in $S(\mathbb{F}_2^4)$.

Keywords. almost perfect nonlinear function, general affine group, general linear group, permutation group, quadratic function.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. In a block cipher, the ciphertext of a plaintext $x \in \mathbb{F}_2^n$ is obtained by applying a composition of several round functions to x; each round function is a permutation of $\mathbb{F}_2^n$. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be such a round function. To resist differential cryptanalysis, the distribution of the values of the function $F(x+a)+F(x)$ should be as uniform as possible for every $0 \neq a \in \mathbb{F}_2^n$ ([6]). A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if for every $a, b \in \mathbb{F}_2^n$ with $a \neq 0$, the equation

$$F(x+a)+F(x) = b$$

has either 0 or 2 solutions x ([1]). Therefore ideal candidates for round functions are permutations of $\mathbb{F}_2^n$ winch are APN. When n is odd, such permutations exist. For an easy example, one can identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ and let $F(x) = x^3$ ([1]). For even n, Canteaut and Dobbertin [2] made the following conjecture.

Conjecture 1.1 *If n is even and F is a permutation of $\mathbb{F}_2^n$, then F is not APN.*

The above conjecture can be formulated in terms of affinity of permutations of $\mathbb{F}_2^n$ on 2-dimensional affine subspaces. Recall that for affine spaces A and B over $\mathbb{F}_2$, a map $f : A \to B$ is called affine if $f(a_1+a_2+a_3) = f(a_1)+f(a_2)+f(a_3)$ for all $a_1, a_2, a_3 \in A$. Conjecture 1.1 is equivalent to

Conjecture 1.2 *Let n be even and let σ be a permutation of $\mathbb{F}_2^n$. Then σ is affine on a 2-dimensional affine subspace A of $\mathbb{F}_2^n$, i.e., $\sigma(A)$ is a 2-dimensional affine subspace of $\mathbb{F}_2^n$.*

Throughout the paper, $S(X)$ always denotes the group of all permutations of a set X. Thus $S(\mathbb{F}_2^n)$ is the permutation group of $\mathbb{F}_2^n$. The group of invertible affine transformations of $\mathbb{F}_2^n$, i.e., the general affine group $\mathrm{AGL}(n,2)$, is a subgroup of $S(\mathbb{F}_2^n)$. Conjecture 1.2 is equivalent to

Conjecture 1.3 *Let $A_0 = \{(x_1, x_2, 0, \cdots, 0)^T : x_i \in \mathbb{F}_2\} \subset \mathbb{F}_2^n$. When n is even,*

$$S(\mathbb{F}_2^n) = \mathrm{AGL}(n,2) \cdot S_{A_0} \cdot \mathrm{AGL}(n,2), \tag{1.1}$$

where $S_{A_0} = \{\sigma \in S(\mathbb{F}_2^n) : \sigma|_{A_0} = \mathrm{id}\}$ is the stabilizer of A_0 in $S(\mathbb{F}_2^n)$. (In (1.1), the multiplication is the operation of the group $S(\mathbb{F}_2^n)$.)

In this paper, we report some partial results on the above conjectures and suggest a group theoretic approach to the problem.

Section 2 contains some miscellaneous results. We prove that Conjectures 1.1 – 1.3 are true for $n = 4$. We also show that the normalizers of $\mathrm{AGL}(n,2)$ and $\mathrm{GL}(n,2)$ in $S(\mathbb{F}_2^n)$ are themselves. In Section 3, we study the affinity of elements in $S(\mathbb{F}_2^n)$ using directional derivatives. In particular, we show that Conjectures 1.1 – 1.3 are true for permutations of $\mathbb{F}_2^n$ with quadratic component functions.

Recall the if H and K are subgroups of a group G and $g \in G$, the (H,K)-double coset with representative g is HgK. Equation (1.1) means that every $(\mathrm{AGL}(n,2), \mathrm{AGL}(n,2))$-double coset in $S(\mathbb{F}_2^n)$ has a representative in S_{A_0}. This suggests the importance of the structure of $(\mathrm{AGL}(n,2), \mathrm{AGL}(n,2))$-double cosets in $S(\mathbb{F}_2^n)$. In Section 4, we give a formula for computing the number of $(\mathrm{AGL}(n,q), \mathrm{AGL}(n,q))$-double cosets in $S(\mathbb{F}_q^n)$. The number of $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-double cosets in $S(\mathbb{F}_2^4)$ is 302; the number of $(\mathrm{AGL}(5,2), \mathrm{AGL}(5,2))$-double cosets in $S(\mathbb{F}_2^5)$ is astronomical. In Section 5, we find representatives for the 302 $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-double cosets in $S(\mathbb{F}_2^4)$ using a computer. This classification answers all questions about affinity of permutations of $\mathbb{F}_2^4$.

Because of the nature of an extended abstract, some proofs are omitted.

2 Miscellaneous Results

Since there are counter examples to Conjectures 1.1 – 1.3 for odd n, one might hope to use them to build a counter example to the conjectures for even n However, the following proposition shows that this approach is not likely to be easy.

Proposition 2.1 *Let $A = \{\left[\begin{smallmatrix}0\\v\end{smallmatrix}\right] : v \in \mathbb{F}_2^{n-1}\} \subset \mathbb{F}_2^n$. Assume that $\sigma \in S(\mathbb{F}_2^n)$ such that $\sigma(A) = A$. Then σ is affine on a 2-dimensional affine subspace of $\mathbb{F}_2^n$.*

Proof.
Assume to the contrary that σ is not affine on any 2-dimensional subspace. Let

$$\sigma(\begin{bmatrix}0\\v\end{bmatrix}) = \begin{bmatrix}0\\\alpha(v)\end{bmatrix}, \quad \sigma(\begin{bmatrix}1\\v\end{bmatrix}) = \begin{bmatrix}1\\\beta(v)\end{bmatrix}, \quad v \in \mathbb{F}_2^{n-1},$$

where α and β are permutations of $\mathbb{F}_2^{n-1}$. Then α and β are not affine on any 2-dimensional subspace of $\mathbb{F}_2^{n-1}$. Fix any $0 \neq a \in \mathbb{F}_2^{n-1}$. The map

$$v \longmapsto \alpha(v) + \alpha(v+a)$$

is 2-to-1 from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^{n-1} \setminus \{0\}$. (Otherwise, α would be affine on a 2-dimensional affine subspace of $\mathbb{F}_2^{n-1}$.) Let

$$D(\alpha) = \{\alpha(v) + \alpha(v+a) : v \in \mathbb{F}_2^{n-1}\} \subset \mathbb{F}_2^{n-1} \setminus \{0\}.$$

Then $|D(\alpha)| = 2^{n-2}$. In the same way, $D(\beta) \subset \mathbb{F}_2^{n-1} \setminus \{0\}$ and $|D(\beta)| = 2^{n-2}$. Hence $D(\alpha) \cap D(\beta) \neq \emptyset$, i.e.,

$$\alpha(u) + \alpha(u+a) = \beta(v) + \beta(v+a)$$

for some $u, v \in \mathbb{F}_2^{n-1}$. Then σ is affine on the 2-dimensional affine subspace

$$\left\{ \begin{bmatrix} 0 \\ u \end{bmatrix}, \begin{bmatrix} 0 \\ u+a \end{bmatrix}, \begin{bmatrix} 1 \\ v \end{bmatrix}, \begin{bmatrix} 1 \\ v+a \end{bmatrix} \right\}.$$

◇

By a k-frame, we mean an affinely independent subset $X \subset \mathbb{F}_2^n$ with $|X| = k+1$, i.e., a $(k+1)$-element subset of $\mathbb{F}_2^n$ which spans a k-dimensional affine subspace. If X and Y are two k-frames of $\mathbb{F}_2^n$, then any bijection $f : X \to Y$ can be extended to an element in $\mathrm{AGL}(n,2)$.

Lemma 2.2 *(i) Let $\sigma \in S(\mathbb{F}_2^n)$. Then there exists an n-frame $X \subset \mathbb{F}_2^n$ such that $\sigma(X)$ is also an n-frame.*

(ii) Let $e_1, \cdots, e_n$ be the standard basis of $\mathbb{F}_2^n$ and let $e_0 = 0 \in \mathbb{F}_2^n$. Then

$$S(\mathbb{F}_2^n) = \mathrm{AGL}(n,2) \cdot S_{e_0, e_1, \cdots, e_n} \cdot \mathrm{AGL}(n,2),$$

where $S_{e_0, e_1, \cdots, e_n}$ is the stabilizer of $e_0, e_1, \cdots, e_n$.

Proof.
Omitted. ◇

Theorem 2.3 *Conjectures 1.1 – 1.3 are true for $n = 4$.*

Proof.
By Lemma 2.2 (ii), we only have to prove Conjecture 1.2 for $\sigma \in S_{\{e_0, e_1, \cdots, e_4\}}$, i.e., for permutations of $\mathbb{F}_2^4$ which stabilize e_i $(0 \leq i \leq 4)$. There are 11! such permutations and the claim is easily verified using a computer. The theorem also follows from the classification of $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-double cosets in $S(\mathbb{F}_2^4)$ in Section 5. ◇

For $\sigma, \tau \in S(\mathbb{F}_2^n)$, we say σ and τ are equivalent $(\sigma \sim \tau)$ if σ and τ are in the same $(\mathrm{AGL}(n,2), \mathrm{AGL}(n,2))$-double coset of $S(\mathbb{F}_2^n)$.

Corollary 2.4 *Let n be even, $\sigma \in S(\mathbb{F}_2^n)$, and identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$. Then σ is affine on a 2-dimensional affine subspace of $\mathbb{F}_{2^n}$ if one of the following is true.*

(i) $\sigma \sim f$ for some permutation polynomial f of $\mathbb{F}_{2^n}$ such that $f \in \mathbb{F}_{2^2}[x]$.

(ii) $4 \mid n$ and $\sigma \sim f$ for some permutation polynomial of f of $\mathbb{F}_{2^n}$ such that $f \in \mathbb{F}_{2^4}[x]$.

Proof.
(i) is obvious since f maps $\mathbb{F}_{2^2}$ to $\mathbb{F}_{2^2}$.

(ii) f maps $\mathbb{F}_{2^4}$ to $\mathbb{F}_{2^4}$. By Theorem 2.3, f is affine on a 2-dimensional affine subspace of $\mathbb{F}_{2^4}$. ◇

Proposition 2.5 *The normalizer of* $\mathrm{AGL}(n,2)$ *in* $S(\mathbb{F}_2^n)$ *is* $\mathrm{AGL}(n,2)$.

Proof.
Omitted. ◇

Proposition 2.6 *The normalizer of* $\mathrm{GL}(n,2)$ *in* $S(\mathbb{F}_2^n)$ *is* $\mathrm{GL}(n,2)$.

Proof.
Omitted. ◇

3 Quadratic Permutations of $\mathbb{F}_2^n$

It is well known that the algebra of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is

$$\mathcal{P}_n = \mathbb{F}_2[X_1, \cdots, X_n]/(X_1^2 - X_1, \cdots, X_n^2 - X_n).$$

Also recall that the rth order Reed-Muller code of length 2^n is $R(r,n) = \{f \in \mathcal{P}_n : \deg f \leq r\}$. Let $\sigma = (f_1, \cdots, f_n)^T$ be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ where $f_i \in \mathcal{P}_n$. We define

$$\deg \sigma = \max_{1 \leq i \leq n} \deg f_i.$$

When n is odd, the counter example to the conjectures, $f(x) = x^3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, is a quadratic permutation of $\mathbb{F}_{2^n}$. Thus it is natural to ask if the conjectures are true for quadratic permutations of $\mathbb{F}_{2^n}$ when n is even. We will see that the answer is positive.

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be any function and let $a \in \mathbb{F}_2^n$. We define

$$\begin{array}{rccc} D_aF: & \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^m \\ & x & \longmapsto & F(x+a) + F(x) \end{array}$$

Lemma 3.1 *Let* $\sigma = (f_1, \cdots, f_n)^T : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be any function such that* σ *is not affine on any 2-dimensional affine subspace of* $\mathbb{F}_2^n$. *Let* $\tau = (f_2, \cdots, f_n)^T : \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$ *and* $e_1 = (1, 0, \cdots, 0)^T \in \mathbb{F}_2^n$. *If* $D_{e_1} f_1$ *is a constant, then*

$$D_{e_1}\tau = (D_{e_1}f_2, \cdots, D_{e_1}f_n)^T : \{0\} \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-1}$$

is a bijection.

Proof.
Assume the contrary. Then there exist $a, b \in \{0\} \times \mathbb{F}_2^{n-1}$, $a \neq b$, such that

$$\tau(a + e_1) + \tau(a) = \tau(b + e_1) + \tau(b).$$

But since $f_1(a + e_1) + f_1(a) = (D_{e_1}f_1)(a) = (D_{e_1}f_1)(b) = f_1(b + e_1) + f_1(b)$, we have

$$\sigma(a + e_1) + \sigma(a) = \sigma(b + e_1) + \sigma(b),$$

i.e., σ is affine on the 2-dimensional affine subspace $\{a, b, a+e_1, b+e_1\}$. This is a contradiction. $\diamond$

For any $f \in \mathcal{P}_n$, define

$$N(f) = \{a \in \mathbb{F}_2^n : D_a f = \text{constant}\}.$$

Corollary 3.2 *Let $\sigma = (f_1, \cdots, f_n)^T : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be any function such that σ is not affine on any 2-dimensional affine subspace of $\mathbb{F}_2^n$. Then $N(f_1) \cap N(f_2) = \{0\}$.*

Proof.
Otherwise, we may assume that $e_1 \in N(f_1) \cap N(f_2)$. Then both $D_{e_1} f_1$ and $D_{e_1} f_2$ are constants, which is impossible by Lemma 3.1. $\diamond$

Theorem 3.3 *Let n be even and let $\sigma = (f_1, \cdots, f_n)^T \in S(\mathbb{F}_2^n)$ such that*

$$\dim_{\mathbb{F}_2} \big(\langle f_1, \cdots, f_n\rangle + R(2,n)\big)/R(2,n) \le 1, \tag{3.1}$$

where $\langle f_1, \cdots, f_n\rangle$ is the linear span of $f_1, \cdots, f_n$. Then σ is affine on a 2-dimensional affine subspace of $\mathbb{F}_2^n$.

Proof.
Of course, we may assume that $n \ge 4$. Because of (3.1), we may assume that $f_1, \cdots, f_{n-1} \in R(2,n)$. For each $f \in R(2,n)$, its homogeneous part of degree 2 corresponds to an $n \times n$ symmetric matrix A over $\mathbb{F}_2$ whose diagonal entries are 0. The quadratic rank of f, denoted by $\mathrm{rank}(f)$, is $\mathrm{rank}(A)$. It is well known that $\dim N(f) = n - \mathrm{rank}(f)$. For any $0 \ne (c_1, \cdots, c_{n-1}) \in \mathbb{F}_2^{n-1}$, we have $\mathrm{rank}(c_1 f_1 + \cdots + c_{n-1} f_{n-1}) \le n-2$. (Otherwise, the Hamming weight of $\sum_{i=1}^{n-1} c_i f_i$ is $|\sum_{i=1}^{n-1} c_i f_i| = 2^{n-1} \pm 2^{\frac{n}{2}-1} \ne 2^{n-1}$. Then $\sigma = (f_1, \cdots, f_n)^T$ cannot be a permutation of $\mathbb{F}_2^n$, which is a contradiction.) Therefore

$$\dim N(c_1 f_1 + \cdots + c_{n-1} f_{n-1}) \ge 2 \quad \text{for all } 0 \ne (c_1, \cdots, c_{n-1}) \in \mathbb{F}_2^{n-1}.$$

We claim that there exist $(u_1, \cdots, u_{n-1})$, $(v_1, \cdots, v_{n-1}) \in \mathbb{F}_2^{n-1} \setminus \{0\}$, $(u_1, \cdots, u_{n-1}) \ne (v_1, \cdots, v_{n-1})$, such that

$$N(u_1 f_1 + \cdots + u_{n-1} f_{n-1}) \cap N(v_1 f_1 + \cdots + v_{n-1} f_{n-1}) \ne \{0\}.$$

Otherwise,

$$\Big| \bigcup_{(c_1, \cdots, c_{n-1}) \in \mathbb{F}_2^{n-1} \setminus \{0\}} N(c_1 f_1 + \cdots + c_{n-1} f_{n-1}) \Big| \ge 1 + 3(2^{n-1} - 1) > 2^n,$$

which is a contradiction.

Through a suitable linear transformation, we may assume that $(u_1, \cdots, u_{n-1}) = (1, 0, \cdots, 0)$ and $(v_1, \cdots, v_{n-1}) = (0, 1, 0, \cdots, 0)$. Then $N(f_1) \cap N(f_2) \ne \{0\}$. By Corollary 3.2, σ is affine on a 2-dimensional affine subspace of $\mathbb{F}_2^n$. $\diamond$

Corollary 3.4 *Let n be even. If $\sigma \in S(\mathbb{F}_2^n)$ and $\deg \sigma \le 2$, then σ is affine on a 2-dimensional affine subspace of $\mathbb{F}_2^n$.*

4 Number of $\mathrm{AGL}(n,q)$, $\mathrm{AGL}(n,q))$-Double Cosets in $S(\mathbb{F}_q^n)$

Let p be a prime and q a power of p. In this section we work with $\mathbb{F}_q$ instead of $\mathbb{F}_2$. In fact, the q-ary case does not require any extra work.

The group $\mathrm{AGL}(n,q)\times\mathrm{AGL}(n,q)$ acts on $S(\mathbb{F}_q^n)$: For $(f,g)\in\mathrm{AGL}(n,q)\times\mathrm{AGL}(n,q)$ and $\sigma\in S(\mathbb{F}_q^n)$,

$$(f,g)(\sigma)=f\cdot\sigma\cdot g^{-1}.$$

The orbits of this action are precisely the $(\mathrm{AGL}(n,q),\ \mathrm{AGL}(n,q))$-double cosets in $S(\mathbb{F}_q^n)$. By Burnside Lemma, the number of $(\mathrm{AGL}(n,q),\ \mathrm{AGL}(n,q))$-double cosets in $S(\mathbb{F}_q^n)$, denoted by $N(n,q)$, is given by

$$N(n,q)=\sum_{f,g\in\mathcal{C}}\frac{1}{|\mathrm{cent}_{\mathrm{AGL}(n,q)}(f)|\cdot|\mathrm{cent}_{\mathrm{AGL}(n,q)}(g)|}|F(f,g)|,$$

where $\mathcal{C}$ is a system of representatives of the conjugacy classes of $\mathrm{AGL}(n,q)$, $\mathrm{cent}_{\mathrm{AGL}(n,q)}(f)$ is the centralizer of f in $\mathrm{AGL}(n,q)$, and

$$F(f,g)=\{\sigma\in S(\mathbb{F}_q^n):f\sigma g^{-1}=\sigma\}.$$

We have

$$\begin{aligned}&|F(f,g)|\\=&\big|\{\sigma\in S(\mathbb{F}_q^n):f=\sigma g\sigma^{-1}\}\big|\\=&\begin{cases}0, & \text{if } f \text{ and } g \text{ are of different cycle types,}\\ (\lambda_1!\lambda_2!\cdots)(1^{\lambda_1}2^{\lambda_2}\cdots), & \text{if } f \text{ and } g \text{ are both of cycle type } (\lambda_1,\lambda_2,\cdots)\vdash q^n,\end{cases}\end{aligned}$$

where $(\lambda_1,\lambda_2,\cdots)\vdash q^n$ means that $(\lambda_1,\lambda_2,\cdots)$ is a partition of q^n, i.e., $\lambda_i\geq 0$ and $1\lambda_1+2\lambda_2+\cdots=q^n$. That f is of cycle type $(\lambda_1,\lambda_2,\cdots)$ means that in the decomposition of f into disjoint cycles, there are λ_i cycles of length i. For each $\lambda=(\lambda_1,\lambda_2,\cdots)\vdash q^n$, put

$$C_\lambda=\{f\in\mathcal{C}:f \text{ is of cycle type } \lambda\}.$$

Then we have

$$N(n,q)=\sum_{\lambda=(\lambda_1,\lambda_2,\cdots)\vdash q^n}(\lambda_1!\lambda_2!\cdots)(1^{\lambda_1}2^{\lambda_2}\cdots)\Big[\sum_{f\in C_\lambda}\frac{1}{|\mathrm{cent}_{\mathrm{AGL}(n,q)}(f)|}\Big]^2. \tag{4.1}$$

To use formula (4.1), we have to know three things: (i) a system $\mathcal{C}$ of representatives of the conjugacy classes of $\mathrm{AGL}(n,q)$, (ii) $|\mathrm{cent}_{\mathrm{AGL}(n,q)}(f)|$ for every $f\in\mathcal{C}$, and (iii) the cycle type of every $f\in\mathcal{C}$.

Items (i) and (ii) have been determined in [3] and [4]. Elements in $\mathcal{C}$ form a 3-parameter family $f_{\lambda,t,B}$ where $\lambda=(\lambda_1,\lambda_2,\cdots)$ is a partition with $|\lambda|=1\lambda+2\lambda_2+\cdots\leq n$, $t\geq 0$ is a certain integer and B is a representative of conjugacy classes of $\mathrm{GL}(n-|\lambda|,q)$ which has no eigenvalue 1. (See [3] for the details.)

As for (iii), let $(\lambda_1,\lambda_2,\cdots)$ be the cycle type of $f\in\mathcal{C}$ and put $\mathrm{Fix}(f)=\{x\in\mathbb{F}_q^n:f(x)=x\}$. Then for integer $k\geq 1$, we have

$$|\mathrm{Fix}(f^k)|=\sum_{i|k}i\lambda_i.$$

By Möbius inversion, we obtain

$$i\lambda_i = \sum_{k|i} \mu(\frac{i}{k})|\mathrm{Fix}(f^k)|,$$

where μ is the classical Möbius function. Thus

$$\lambda_i = \frac{1}{i}\sum_{k|i} \mu(\frac{i}{k})|\mathrm{Fix}(f^k)|.$$

Therefore we only have to determine $|\mathrm{Fix}(f^k)|$ for $f \in \mathcal{C}$ and $k \geq 1$. We use ν_p to denote the p-adic order function.

Proposition 4.1 *In the above notation, we have*

$$\left|\mathrm{Fix}(f^k_{\lambda,0,B})\right| = q^{\sum_i \lambda_i \min\{i, p^{\nu_p(k)}\} + \mathrm{null}(B^k - I)}, \tag{4.2}$$

and for $t > 0$,

$$\left|\mathrm{Fix}(f^k_{\lambda,t,B})\right| = \begin{cases} q^{\sum_i \lambda_i \min\{i, p^{\nu_p(k)}\} + \mathrm{null}(B^k - I)}, & \text{if } p^{\nu_p(k)} > t, \\ 0, & \text{if } p^{\nu_p(k)} \leq t. \end{cases} \tag{4.3}$$

Proof.
Omitted. ◇

Using a computer we find that

$$N(4,2) = 302$$

and

$$N(5,2) = 2,569,966,041,123,938,084.$$

5 Classification of $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-Double Cosets in $S(\mathbb{F}_2^4)$

To find representatives of $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-double Cosets in $S(\mathbb{F}_2^4)$, by Lemma 2.2 (ii), we only have to search through permutations of $\mathbb{F}_2^4$ which fix $0, e_1, \cdots, e_4$. The search is complete when 302 mutually non equivalent permutations have been found. Note that for $\sigma, \tau \in S(\mathbb{F}_2^4)$, $\sigma \sim \tau$ if and only if $\sigma f \tau^{-1} \in \mathrm{AGL}(4,2)$ for some $f \in \mathrm{AGL}(4,2)$. The indicator functions of all 2-dimensional subspaces of $\mathbb{F}_2^4$ generate the Reed-Muller code $R(2,4)$ ([5]). Since $\dim R(2,4) = 2^4 - 1 - 4 = 11$, we can find 2-dimensional subspaces $V_1, \cdots, V_{11}$ of $\mathbb{F}_2^4$ such that their indicator functions form a basis of $R(2,4)$. Then $\sigma f \tau^{-1} \in \mathrm{AGL}(4,2)$ if and only if

$$\sum_{x \in V_i} \sigma f \tau^{-1}(x) = 0 \quad \text{for } 1 \leq i \leq 11.$$

In this way, we have found the representatives of the $(\mathrm{AGL}(4,2), \mathrm{AGL}(4,2))$-double cosets in $S(\mathbb{F}_2^4)$ using a computer. However, the list of representatives is too long to be included in this paper. Using this classification, we can answer all questions concerning the affinity of permutations of $\mathbb{F}_2^4$. In particular, we find that every element in $S(\mathbb{F}_2^4)$ is affine on at least 7 two-dimensional affine subspaces of $\mathbb{F}_2^4$.

References

[1] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs, Codes and Cryptography, **15** (1998), 125 – 156.

[2] A. Canteaut and H. Dobbertin, *private communication.*

[3] X. Hou, $AGL(m,2)$ *acting on* $R(r,m)/R(s,m)$, J. Algebra **171** (1995), 921 – 938.

[4] X. Hou, $\mathrm{GL}(m,2)$ *acting on* $R(r,m)/R(r-1,m)$, Discrete Math., **149** (1996), 99 – 122.

[5] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[6] D. R. Stinson, *Cryptography, Theory and Practice*, 2nd ed., Chapman & Hall, New York, 2002.