Crooked binomials

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)
and
Gohar M. Kyureghyan
Department of Mathematics
Otto-von-Guericke University
Magdeburg (Germany)

June 13, 2006

Abstract

We prove that a crooked function $f(x) = x^d + ux^e$ defined on $GF(2^n)$ either is equivalent to a power function of Gold type or satisfies that both exponents d, e have 2-weights at most 2.

1 Introduction

Definition 1. *Let $F = \mathbb{F}_q$, where $q = 2^r$. A function $f : F \longrightarrow F$ is* **almost perfectly nonlinear** *(APN) if for every $0 \neq a \in F$ the additive derivative $\delta_{f,a}$ defined by $\delta_{f,a}(x) = f(x + a) + f(x)$ is two-to-one: it has $q/2$ different images (equivalently: each image has precisely two preimages).*

The APN function f is crooked if for every a the image $\delta_{f,a}(F)$ is either a hyperplane or the complement of a hyperplane of F (seen as an r-dimensional vector space over $\mathbb{F}_2$).

We refer to the second set of conditions in Definition 1 as the hyperplane conditions. They are a little more general than the original definition of crooked functions (see van Dam and Fon-Der-Flaass [5]) where it is demanded that f be bijective. This restricted notion is quite natural as well because of a link to non-linear binary codes with Preparata parameters.

It is clear that addition of a constant and concatenation with invertible linear mappings leaves the APN and crooked property invariant. If g is obtained from f by such operations, then f and g are called **affine equivalent.** Until recently all known APN functions were affine equivalent to power functions $f(x) = x^d$ for suitable exponents d. The first examples of APN functions which are not affine equivalent to a power function were constructed in [6]. An infinite family was given in [3]. All those examples are quadratic binomials: $f(x) = x^d + ux^e$, where $u \in F$ and d, e are exponents of 2-weight 2. They are in fact crooked and they are not equivalent to an APN power function under a more general notion of equivalence, which became known as CCZ-equivalence [4]. We describe this notion in the following section.

In the present paper we deal with crooked binomial functions $f(x) = x^d + ux^e$. Here the exponents d, e can be regarded as integers mod $2^r - 1$. The following terminology will turn out to be useful:

Definition 2. *Let $q = 2^r$, $G = Gal(F)$ the Galois group of $F = \mathbb{F}_q$ over $\mathbb{F}_2$. Write $G = \{g_0, g_1, \ldots, g_{r-1}\}$, where $g_i(x) = x^{2^i}$.*

Let d be an integer mod $q-1$, $0 \leq d = 2^i+2^j+\cdots < q-1$. We describe d by the subset $D = \{i, j, \ldots\} \subseteq \{0, 1, \ldots, r-1\}$ and write $d = n(D)$. Observe that the 2-weight of $d = n(D)$ equals the cardinality $|D|$ and $x^{n(D)} = \prod_{i \in D} g_i(x)$.

As addition of constants and of linear functions cx^{2^i} does not affect the APN and crooked properties we can and will assume that all exponents have 2-weight at least 2. It was proved in [7] that a power function $x^{n(D)}$ is crooked if and only if the exponent $n(D)$ is of Gold type: $D = \{i, j\}$ and $gcd(i - j, r) = 1$. In the present paper we study crooked binomial functions. Our main result is the following:

Theorem 1. *If $f(x) = x^{n(D)} + ux^{n(E)}$ is a crooked function defined on $F = \mathbb{F}_{2^r}$, then $|D|, |E| \leq 2$.*

2 Generalities

To a function $f : F \longrightarrow F$ certain linear codes are associated in a natural way:

Definition 3. *Let $f : F \longrightarrow F$ and $\overline{\mathcal{B}}_f$ the F-linear length q code whose codewords $v(a,b,c)$ for $a,b,c \in F$ have entry*

$$v(a,b,c)_x = a + bx + cf(x)$$

in coordinate x.

Proposition 1 (see [4]). *The following are equivalent:*

- *f is an APN function*
- *The trace code $tr(\overline{\mathcal{B}}_f)^\perp$ has minimum distance ≥ 6.*

We consider the code $\overline{\mathcal{B}}_f$, its trace code and the corresponding dual as canonical objects associated to the APN function f. The definition of CCZ equivalence as given in [4] can simply be expressed as follows: f and g are equivalent if and only if $tr(\overline{\mathcal{B}}_f)$ and $tr(\overline{\mathcal{B}}_g)$ are equivalent linear codes. By construction $tr(\overline{\mathcal{B}}_f)$ has dimension $\leq 2r+1$. Brouwer-Tolhuizen [2] show that $[2^r-2, 2^r-2r-1, 5]_2$-codes cannot exist when $r \geq 4$. This implies that the code $tr(\overline{\mathcal{B}}_f)$ associated to an APN function f does indeed have dimension $2r+1$ (see also [4]).

Application of the field automorphism $g_i(x) = x^{2^i}$ corresponds to multiplication with 2^i in the exponent (calculating mod 2^r-1) and to translation $j \mapsto j+i$ in $\Omega = \{0,1,\ldots,r-1\} = \mathbb{Z}/r\mathbb{Z}$, which may be seen as an additive way of writing the Galois group G. It is therefore natural to study orbits of G in its action on Ω, equivalently on its own subsets. Those orbits are known as **cyclotomic cosets.** Write $S \sim T$ if subsets S, T are in the same orbit.

The case of monomials

The main result of [7] states that a power function $f(x) = x^{n(D)}$ with $|D| > 2$ does not satisfy the hyperplane condition of Definition 1. In particular f cannot be crooked. It is instructive to paraphrase the proof in our terminology. Assume the hyperplane condition is satisfied. First it is easy to see that D must be in an orbit of full length r. Assume there is some $\alpha \in F$ such that $tr(\alpha((x+1)^d + x^d))$ is a constant function (0 or 1). It has to be shown that necessarily $\alpha = 0$. Observe

$$(x+a)^{n(S)} = \prod_{s \in S}(x^{2^s} + a^{2^s}) = \sum_{T \subseteq S} x^{n(T)} a^{n(S \setminus T)}$$

for all $S \subseteq \Omega$. Expanding $(x+1)^{n(D)}$ yields

$$\delta_{f,1}(x) = (x+1)^{n(D)} + x^{n(D)} = \sum_{S \subset D} x^{n(S)}$$

where S varies over the proper subsets of D. Let now M vary over representatives of orbits of subsets of Ω. Then

$$\delta_{f,1}(x) = \sum_{M} \sum_{S \subset D, S \sim M} x^{n(S)}.$$

Let H_α be the hyperplane described by $tr(\alpha x) = 0$. We have that $\delta_{f,1}(F)$ is contained either in H_α or in the complement of H_α if and only if $tr(\alpha \delta_{f,1}(x))$ is a constant function. As the space of all boolean functions $g : F \longrightarrow \mathbb{F}_2$ is the direct sum of the spaces $x \mapsto tr(cx^{n(M)})$ (here $c \in F$ is a constant, the dimension of the space equals the length $|Z(M)|$ of the corresponding orbit) this is the case if and only if the above summands vanish for all $M \neq \emptyset$. Define

$$\beta_1(M) = \sum_{S = M - i \subset D} g_i(\alpha).$$

Our summand vanishes if and only if

$$tr(x^{n(M)} \beta_1(M)) = 0$$

for all x. The subfield generated by the $x^{n(M)}$ is the subfield L of order $2^{|Z(M)|}$. We have shown the following:

Lemma 1. *For every $\alpha \neq 0$ the following are equivalent:*

- *$tr(\alpha \delta_{f,1}(x))$ is a constant function of x.*
- *For all representatives M of orbits of nonempty proper subsets of $\Omega = \{0, 1, \ldots, r-1\}$ we have that $\beta_1(M)$ is orthogonal, with respect to the trace form, to the subfield of order $2^{|Z(M)|}$.*

In particular $\beta_1(M) = 0$ if M is in an orbit of full length. Observe that each summand in the definition of $\beta_1(M)$ is nonzero. A contradiction is obtained if D contains a subset K which satisfies the following:

1. K is in an orbit of full length r,

2. K is the only element of its orbit which is a subset of D.

It is then proved that there is only one type of sets D which do not possess a maximal subset $S \subset D$ of this type. Those special sets are the punctured cosets: cosets of proper subgroups of G with one element removed. They are then excluded by an ad hoc argument.

The case of binomials

Let now $f(x) = x^{n(D)} + ux^{n(E)}$ for some $0 \neq u \in F$ and $D, E \subseteq \Omega$, where we assume (without restriction) $|D|, |E| \geq 2$. As before let H_α be the hyperplane described by $tr(\alpha x) = 0$. In order to exploit the hyperplane condition we use the same method as in the case of monomials. This time it will not be sufficient to consider only case $a = 1$.

$$\delta_{f,a}(x) = \sum_{S \subset D} x^{n(S)} a^{n(D \setminus S)} + u\alpha \sum_{T \subset E} x^{n(T)} a^{n(E \setminus T)}.$$

Here S, T vary over the proper subsets of D, E, respectively. Let M vary over representatives of orbits of subsets of Ω. Then

$$\delta_{f,a}(x) = \sum_{M} \sum_{S \subset D, S \sim M} x^{n(S)} a^{n(D \setminus S)} + u \sum_{T \subset E, T \sim M} x^{n(T)} a^{n(E \setminus T)}.$$

The same arguments as in the monomial case shows the following:

Lemma 2. *Let*

$$\beta_a(M) = \sum_{S = M - i \subset D} g_i(\alpha) a^{n(D+i \setminus M)} + \sum_{T = M - j \subset E} g_j(u\alpha) a^{n(E+j \setminus M)}.$$

For every $\alpha \neq 0$ the following are equivalent:

- *$tr(\alpha \delta_a(x))$ is a constant function of x.*
- *For all representatives M of orbits of nonempty proper subsets of $\Omega = \{0, 1, \ldots, r-1\}$ we have that $\beta_a(M)$ is orthogonal, with respect to the trace form, to the subfield of order $2^{|Z(M)|}$.*

If in particular we find M such that M is in an orbit of full length, $M - i \subset D$ for exactly one i and $M - j \not\subset E$ for all j, then necessarily $\alpha = 0$ and we have shown that $f(x)$ is not crooked.

A degenerate case occurs when D, E are in the same orbit. We treat this in a slightly more general context:

Theorem 2. *A function of the form $h(X) = f(X) + uf(X)^{2^i}$ defined on $F = \mathbb{F}_{2^r}$ for $r > 2$ is APN if and only if the following hold:*

- *$f(X)$ is APN*
- *The linear function $l(y) = y + uy^{2^i}$ is invertible.*

In this case f and h are CCZ-equivalent (not necessarily affine equivalent).

Proof. We have $h(x) = l(f(x))$ and $\delta_{h,a}(x) = l(\delta_{f,a}(x))$. As $|\delta_{h,a}(F)| = q/2$ it follows that l has rank at least $r - 1$.

Assume h is APN and l has rank $r-1$. Then $gcd(i, r) = 1$ and the equation $1+uy^{2^i-1} = 0$ has a unique solution y_0, in other words $u = y_0/g_i(y_0)$. Because of the APN property we must have $\delta_{h,a}(F) = l(F)$ for all a. Let $z \in l(F)$. It has two preimages $y, y + y_0$ under l. One of them, say y, must be in $\delta_{f,a}(F)$. As $\delta_{f,a}(x) = \delta_{f,a}(x + a)$ it follows that $y + y_0 \notin \delta_{f,a}(F)$. We have that for every y and every a

$$|\{y, y + y_0\} \cap \delta_{f,a}(F)| = 1.$$

In particular f is APN. Consider codes $\overline{\mathcal{B}}_f$ and $\overline{\mathcal{B}}_h$. We have $h(x) = y_0(f(x)/y_0+g_i(f(x)/y_0))$, so $h(x)/y_0 \in H_0$, the hyperplane consisting of the elements of trace 0. It follows that the Galois closure of $\overline{\mathcal{B}}_h$ (see [1]) has dimension $\leq 2r$. This yields a code $[q, q - 2r, 6]_2$, which by [2] cannot exist.

Let now l have full rank r. It follows that h is APN if and only f is.

Let f and h be APN. As CCZ-equivalence is based on the trace code and $tr(h(x)) = tr(f(x) + g_i^{-1}(u)f(x))$ CCZ-equivalence is obvious. □

As a consequence, $f(x)+ug_i(f(x))$ is crooked if and only if $f(x)$ is crooked and u is chosen as prescribed. In particular in the proof of the main theorem we can assume that D, E are in different orbits. The strategy of the proof will be the following:

1. Show that D and E are in orbits of full length.
2. Show $|D| = |E|$ except for the sporadic situation of Theorem 1.
3. Show that if D and E have the same cardinality, then they have the same type in the sense of Section 3.
4. Show that if $|D| = |E| = l \geq 3$, then D, E must be in the same orbit.

In the next section we give a typology of orbits of cyclic groups in their natural action on subsets. This will be used throughout the proof of the main theorem.

3 Cyclic sets

Let G be an abelian group of order r, written additively. It acts by translation on its subsets. In particular the lengths of the orbits are divisors of r. Let $D \subseteq G$ and denote the orbit of D by $Z(D)$. The orbit $Z(D)$ is **short** if its length is $< r$, it is **long** otherwise. An **interval** (or: an arithmetic progression) of stepwidth a is a set of the form $I = \{x, x+a, \dots, x+(d-1)a\}$. A **punctured coset** of G is a coset with respect to a subgroup with one element removed. An interval is **ordinary** if it is neither a coset nor a punctured coset. Let $r = st$. A t-**periodic set** is a union of cosets with respect to the subgroup of order t. Clearly $D \subseteq G$ is t-periodic if and only if $D = D + a$ where $ord(a) = t$, and D is in a short orbit if and only if it is t-periodic for some $t < r$. Write $K \sim L$ if K and L are in the same orbit.

A typology of subsets

We aim at a typology of subsets $D \subset G$ from long orbits as regards the distribution of subsets of D on orbits.

Definition 4. *Denote $|D| = l$. Let $i(D)$ be the number of long orbits of $(l-1)$-sets with the property that precisely one member of the orbit is a subset of D, and let $j(D)$ be the number of long orbits of $(l-1)$-sets that have more than one representative in D.*

The generic situation is that all maximal subsets $K \subset D$ are from different long orbits: $i(D) = l,\ j(D) = 0$. This is type $\mathcal{A}$. In particular singletons have type $\mathcal{A}$.

Lemma 3. *Let $D \subseteq G$. At most one of the maximal subsets $K \subset D$ is in a short orbit.*

Proof. Assume at first D itself is in a short orbit. This means that $D = H_1 \cup \dots \cup H_m$ is a union of cosets of the subgroup H of order t, where $t \mid r$. The distribution of $D \setminus \{x\}$ on cosets of H is characterized by the numbers $t-1, t, t, \dots$. It follows that if $D \setminus \{y\} = D \setminus \{y\} + c$, then x, y are from the same coset of $H : x, y \in H_1$ and $c \in H$. This forces $x = y$.

Let D be in a long orbit. Cases $|D| = 1, 2$ are trivial, so we can assume $|D| > 2$. We have to prove that the following cannot happen: elements $x, y \in D, x \neq y$ and nonzero elements a, b such that

$$(D \setminus x) + a = D \setminus x$$
$$(D \setminus y) + b = D \setminus y$$

As $y \in (D \setminus x)$ we have $y \pm a \in D$, as $a \neq 0$ in fact $y + a \in D \setminus y$ and $y \pm a \pm b \in D \setminus y$. As $y \notin D \setminus y$ it follows $y \pm b \notin D$ and $(y \pm b) \pm a \notin D \setminus x$. Necessarily $y \pm a \pm b = x$. By symmetry $a = -a, b = -b$, hence $a = b$ and $y = x$, contradiction. □

Assume now there is a maximal subset $K_0 \subset D$ in a short orbit. We know from Lemma 3 that K_0 is uniquely determined. The generic case is that all maximal subsets $K \neq K_0$ are from different orbits: $i(D) = l - 1,\ j(D) = 0$. This is type $\mathcal{B}$. The following Lemma 4 describes the situation when D is not of type $\mathcal{B}$.

Lemma 4. *Let $D \subset G$ in a long orbit and $K_0 \subset D$ a maximal subset in a short orbit. Assume $i(D) < l - 1$.*

The stabilizer of K_0 has order 2 and there is an even divisor $2g > 2$ of r such that D is obtained by puncturing a $2g$-periodic set.

Proof. We know that D is the union of the t_0-periodic set K_0 and a point outside. Here t_0 is a proper divisor of r. Assume $t_0 > 2$. Any maximal subset $K \neq K_0$ is the union of a t_0-periodic set, an isolated point and a punctured t_0-orbit. As the isolated point is uniquely determined we see that no two such maximal subsets can be translates of one another. We have $t_0 = 2$. Let a be the involution.

Then D is the union of an isolated point and a 2-periodic part. We can choose notation such that the isolated point is 0 and therefore

$$D = \{0\} \cup \{k_1, k_1 + a\} \cup \{k_2, k_2 + a\} \cup \ldots$$

As all maximal subsets $K \neq K_0$ are in long orbits we are assuming that two different such maximal subsets are in the same orbit. There are two conceivable situations. The first is $K = D \setminus \{k_1\}, K + c = D \setminus \{k_1 + a\}$. Considering the isolated points we see that

$$\{0, k_1 + a\} + c = \{0, k_1\}.$$

It follows $c = k_1 = -k_1 + a$ and $2k_1 = a$. In particular k_1 has order 4 and D is obtained by puncturing the 4-periodic set $D \cup \{a\}$.

The generic situation is

$$K = D \setminus \{k_1\}, K + c = D \setminus \{k_2\}.$$

As the isolated points must be translates of one another it follows $c = k_2 + a = -k_1 + a$ and $k_2 = -k_1$. Let t' be the order of the stabilizer of $D \cup \{a\}$. This stabilizer contains the involution a and k_2. It follows that t' is even and > 2. $\square$

We have seen that sets D from long orbits containing a maximal subset K_0 from a short orbit are either of type $\mathcal{B}$ or are obtained by puncturing a $2g$-periodic set, where $2g > 2$. The latter sets are those of type $\mathcal{C}$. The type is guaranteed to be $\mathcal{B}$ if the stabilizer of K_0 has order > 2. Assume the stabilizer of K_0 has order 2. Let $\tilde{D} \supset D$ the 2-periodic $(l+1)$-set containing D. Then D has type $\mathcal{C}$ if and only if the stabilizer of $\tilde{D}$ has order $2g > 2$. Sets of type $\mathcal{C}$ are precisely those obtained by puncturing unions of cosets of subgroups of even order $2g > 2$. Let $l = 2mg + 2g - 1$ where $m \geq 0$ (D is the punctured union of $m+1$ cosets). Then $i(D) = 2mg,\ j(D) = g - 1$. In particular puncturings of cosets of subgroups of even order > 2 have type $\mathcal{C}$.

Assume now all maximal subsets of D are in long orbits and at least two of them are in the same orbit (we would have type $\mathcal{A}$ otherwise). This is the situation considered in Lemma 5.

Lemma 5. *Let $D \subset G$ in a long orbit, $K \subset D$ a maximal subset and $a \in G$ such that $K = D \cap (D + a)$. Let $ord(a) = t$ and H the subgroup of order t. Then D is the union of a non-empty interval I of stepwidth a which is not a complete coset of H and of cosets of H. Also, I is in a long orbit.*

Proof. There is a unique element $y \in D \setminus K$ and a unique $z \in (D + a) \setminus K$. We have $y \neq z$ as otherwise $D = D + a$. Consider the arithmetic progression starting at y. Assume $y + ia \in K$ for all $i > 0$. We must have $y + ia = y + ja$ for some $i > j$, so $(i - j)a = 0$. This yields the contradiction $y = y + (i - j)a \in K$. Let now $i > 0$ be minimal such that $y + ia \notin K$. As $y + (i-1)a \in K$ we have $y + ia \in D + a$, hence $y + ia = z$. We have an arithmetic progression of stepwidth a, which starts at y, ends at $z = y + ia$ and all of whose intermediate elements are in K.

Let now $x \in K$. If $x + ja \in K$ for all $j > 0$ we obtain a coset of H. Assume this is not the case, let j minimal such that $x + ja \notin K$. Then $x + ja = z$. This shows that D is the union of $I = \{y, y + a, \ldots, y + (i-1)a\}$ (where $y + ia = z$) and of some cosets of H.

Vice versa, if D has the form as described, then $D \cap (D+a)$ is a maximal subset of D. Assume $D+c = D$. Because of the coset structure we must have $I + c = I$. $\square$

By Lemma 5 we have that a set D not of type $\mathcal{A}, \mathcal{B}$ or $\mathcal{C}$ is a union of $m \geq 0$ cosets of $H = \langle a \rangle$ and of an interval I of stepwidth a. Let $|I| = r$. As D is in a long orbit we have $r \leq t-1$. If $r = 1$, then we have type $\mathcal{B}$ or $\mathcal{C}$. Assume this is not the case. Then $2 \leq r \leq t-1$. A set of this form cannot be of type $\mathcal{A}$ or $\mathcal{B}$.

Lemma 6. *Let $I \subset G$ be an ordinary interval in a cyclic group G. The maximal subsets of I come from precisely $|I| - 1$ different orbits (the two endpieces in one orbit, all others unique in their orbit). All those orbits are long.*

Proof. Let $I = \{x, x+a. \ldots, x+(d-1)a\} \subseteq G$ be an interval. We want to see how the d maximal subsets of I are distributed on the orbits. Clearly the left end and the right end subsets are in the same orbit. Without restriction $x = 0$. Denote $I_i = I \setminus \{ia\}$ for $0 \leq i \leq d-1$. Let $g = r/gcd(a, r)$. We have $ga = 0$ and g is the smallest positive such number. As $|I| = d$ it follows $d \leq g$. As I is an ordinary interval we have $d < g$. In particular $da \notin I$. Assume $I_{d-1} - c = I_u$ for $u \neq 0$. The presence of 0 in I_u shows $c = ia \in I$. Clearly $i \geq 2$. It follows that both $(d-1)a$ and da are outside I_{d-1} but $\{(d-1-i)a, (d-i)a\} \subset$. Both must equal u, contradiction. This shows that the orbit containing I_0 and I_{d-1} does not contain a third subset of I and that it is a long orbit.

Assume now $I_x + c = I_y$ for some $0 < x, y < d-1$. The presence of 0 shows $c = za \in I$ for $1 \leq z \leq d-1$. As $(d-z)a \in I$ and $(d-z)a + c = da \notin I$ it follows $d - z = x$. As $x < d-1$ it follows $z \geq 2$. It follows $(d+1-z)a \in I$. As $(d+1-z)a + c = (d+1)a$ we must have $(d+1)a \in I$, hence $(d+1)a = 0$ and $g = d+1$. This shows that I is a punctured subgroup. $\square$

Lemma 7. *Let $I \subset G$ be the puncturing of a coset of a subgroup of order $t > 2$. If t is even, then the maximal subsets of I belong to $t/2$ different orbits, one short orbit and $(t-2)/2$ long orbits with two representatives each. If t is odd, then the maximal subsets of I are from $(t-1)/2$ long orbits, each with two representatives.*

Proof. Let $H = \{0, s, 2s, \ldots, (t-1)s\}$ the subgroup of order t, where $r = st$, and $I = H \setminus \{0\}$. Then $H \setminus \{0, is\}$ and $H \setminus \{0, -is\}$ belong to the same orbit. $\square$

D is of type $\mathcal{D}$ if it satisfies $i(D) = l - 2,\ j(D) = 1$. The numbers show that it is not of type $\mathcal{A}, \mathcal{B}$ or $\mathcal{C}$ then. Lemmas 6 and 7 show that D can be of type $\mathcal{D}$ only if in the description of Lemma 5 the interval I is ordinary.

The only situation yet to be considered is when I is a punctured coset, equivalently if D is the puncturing of a periodic set. If the stabilizer of this periodic set has even order > 2 then D has type $\mathcal{C}$ as we know. We speak of type $\mathcal{E}$ if D is the puncturing of a periodic set whose full stabilizer has odd order.

Theorem 3. *Let $D \subset G$ be a subset of the cyclic group G of order r such that D is in a long orbit. Then D is of precisely one of the types $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ or $\mathcal{E}$. The following table describes the basic parameters:*

type	$\lvert D\rvert = l$	$i(D)$	$j(D)$
$\mathcal{A}$		l	0
$\mathcal{B}$		$l-1$	0
$\mathcal{C}$	$2mg+2g-1, g>1$	$2mg$	$g-1$
$\mathcal{D}$	$mt+r, 2 \le r \le t-2$	$l-2$	1
$\mathcal{E}$	$mt+t-1$	$mt = l-t+1$	$(t-1)/2$

In particular a puncturing of a t-periodic set for even $t > 2$ has type $\mathcal{C}$. It has type $\mathcal{E}$ if the order of the stabilizer of the periodic set is odd. If the full stabilizer has order 2 then the puncturing has type $\mathcal{B}$. Ordinary intervals have type $\mathcal{D}$.

More properties of orbits

Theorem 4 (K-lemma). *Let $D \subset G$ be in a long orbit and $|D| > 2$. If $i(D) = 0$, then D is a punctured coset.*

Proof. The proof of this lemma from [7] follows directly from Theorem 3. $\square$

Lemma 8. *Let G be cyclic of order r. An interval $I \subseteq G$ is in a short orbit if and only if it is a coset of a subgroup.*

Proof. Let $I = \{0, a, \ldots, (d-1)a\} \subseteq G$ and $c \neq 0$ such that $I + c = I$. The presence of 0 shows that there is $1 \le i \le d-1$ such that $c + ia = 0$. Then $c + da = (d-i)a \in I$. It follows $d \in I$ and $da = 0$. $\square$

Lemma 9. *Let G be cyclic of order r and $I = \{0, a, \dots, (l-1)a\} \subseteq G$ an interval of l points. Let $s = ord(a)$. Then $I_j = I \setminus \{ja\}$ for $0 < j < l-1$ is itself an interval if and only if one of the following hold:*

1. *I is a subgroup ($s = l$).*
2. *I is a punctured subgroup ($s = l+1$), and $j+1$ is coprime with s.*
3. *I is a doubly punctured subgroup ($s = l+2$), l is odd and $j = (l-1)/2$.*

Proof. Write

$$I \setminus \{ja\} = \{x, x+c, \dots, x+(l-2)c\}.$$

Clearly subgroups have the property in question. We can assume $la \neq 0$. If $(l+1)a = 0$, then I is a punctured subgroup and we have the situation that $Z_{l+1} \setminus \{j, l\}$ is an interval. This is certainly satisfied if $j+1, l+1$ are coprime, and it is not satisfied in the contrary case.

We can assume $la \neq 0$, $(l+1)a \neq 0$. Assume $0 \neq x + (l-2)c$. Then $c \in I_j$. Assume to the contrary $0 = x + (l-2)c$. Then $I_j = \{0, -c, \dots\}$. Again the stepwidth $-c$ is in I_j. It follows that we can assume $c = ia$ for some $2 \leq i \leq l-1$.

Assume $i = 2$. The elements $y \in I_j$ different from its right endpoint satisfy $y + c \in I$. In particular there must be $ra \in I_j$, where $l-3 \leq r \leq l-1$ such that $(r+2)a \in I$. This forces $r = l-3$ and $\{ja, x+(l-2)c\} = \{(l-2)a, (l-1)a\}$, hence $j = l-2$, $x+(l-2)c = (l-1)a$. Start from this right endpoint and keep subtracting $c = 2a$. It follows that either $-a \in I$ or $-2a \in I$, contradiction.

We have $3 \leq i \leq l-1$. As $la, (l+1)a, (l+2)a$ cannot all be one of $ja, x+(l-2)a$ and as $\{(l-l)a, (l+1-i)a, (l+2-i)a\} \subset I$ we must have that one of $la, (l+1)a, (l+2)a$ is in I. It follows $(l+2)a = 0$. We have a subgroup Z_s such that $Z_s \setminus \{j, s-2, s-1\}$ is an interval. It follows that $\{j, s-2, s-1\} = \{j, -2, -1\}$ is an interval mod s. Equivalently $\{0, -1, j+1\}$ is an interval. It is impossible that 0 is in the middle of the interval: $(-1, 0, j+1)$ as this would force $j+1 = 1$ and $j = 0$. Also, $(0, -1, j+1 = -2)$ yields $j = -3 = s-3 = l-1$, which corresponds to an end segment, contradiction. The final choice is $(0, j+1, 2(j+1) = -1)$. It is impossible that l is even as the generator -1 cannot be a double. Let l be odd. Then $j = (l-1)/2$. $\square$

Lemma 10. *Let G be cyclic of order r and $I = \{0, a, \dots, (l-2)a\} \subseteq G$ an interval of $l-1$ points, where $l \geq 5$. Let $s = ord(a), 0 < j < l-2$ and $w \notin I$ such that $(I \setminus \{ja\}) \cup \{w\}$ is an interval. Assume $l-1 \leq s/2$.*

If $w \notin \{(l-1)a, -a\}$, then we are in one of the following orbits:

- $s = 8, I = a\{0, 1, 2, 3\}, j = 2, w = 6a$,
- $s = 10, I = a\{0, 1, 2, 3, 4\}, j = 2, w = 7$.

Let $w \in \{(l-1)a, -a\}$. Assume $w = (l-1)a$. Then one of the following hold:

1. *$s = l$ and I is a punctured interval.*
2. *$s = l + 1$, $gcd(j + 1, s) = 1$.*
3. *$s = l + 2$ is odd and $j = (l - 1)/2$.*

Proof. Assume $w \in \{(l-1)a, -a\}$. By symmetry we can assume $w = (l-1)a$. Then $I \cup \{w\}$ satisfies the hypothesis of Lemma 9 and we are done.

Assume now $w \notin \{(l-1)a, -a\}$. Let

$$(I \setminus \{ja\}) \cup \{w\} = \{x, x + c, \dots, x + (l-2)c = y\}.$$

It is clear that $w = ra$ for some r and that $s = ord(a) = ord(c)$. The complement of I in the subgroup generated by a satisfies the same conditions as I itself. It can therefore be assumed that $|I| = l - 1 \leq s/2$.

By a slight change of notation we work in Z_s and have $I = [0, l-2], I_j = I \setminus \{j\}$ and

$$I_j \cup \{w\} = x + c[0, l-2].$$

The isolated position of w shows $c \neq \pm 1$. Fix the ordering $0 < 1 < 2 < \cdots < s - 1$ and recall $s \geq 2l - 2$.

Recall that we are assuming $l \geq 5$. There is then $i \in I_j$ such that $i \neq y, w - c$. It follows $i + c \in I_j$. Replacinf if necessary c by $-c$ we can assume $2 \leq c \leq l - 2$. As $s \geq 2l - 2$ we must have that whenever $i, i + c$ are both in I then $i < i + c$. Those pairs $(i, i + c)$ are contained in

$$\{(0, c), (1, c + 1), \dots, (l - 2 - c, l - 2)\}.$$

There are therefore at most $l - 1 - c$ such pairs. On the other hand there are at least $l - 4$ such pairs (all elements of I_j aside of y and $w - c$ occur in the first coordinate). This shows $l - 4 \leq l - 1 - c$, hence $c \leq 3$.

Assume $c = 2$. Either $w+2 \in I$ or $w-2 \in I$, so $w \in \{l, -2\}$. By symmetry we can assume $w = l$. Then $w + 2 \notin I$, so $w = y$ and

$$I_j \cup \{w\} = \{l, l - 2, l - 4 \dots\},$$

clearly a contradiction.

Assume $c = 3, l \geq 7$. The first and second coordinates of the pairs above cover all of I. It follows that j must occur. Our counting argument improves by 1, contradiction. We have seen $l \leq 6$ if $c = 3$. Only cases $c = 3, l \leq 6$ remain.

Let $l = 6$. We have $I = \{0, 1, 2, 3, 4\}$ and $s \geq 10$. As no element of $\{2, 3, 4\} + c$ is in I we must have $\{2, 3, 4\} = \{y, w - 3, j\}$. As $1 - 3 = -2 \notin I \cup \{w\}$ we must have $x = 1$ and

$$I_j \cup \{w\} = \{1, 4, 7, 10, 13\}.$$

Consequently $s = 10, w = 7, j = 2$.

In case $l = 5$ a similar argument works. We have $I = \{0, 1, 2, 3\}$ and $s \geq 8$. For the same reason as above $\{1, 2, 3\} = \{j, y, w - 3\}$ and $\{0, 1, 2\} = \{j, x, w + 3\}$. These sets intersect in $\{1, 2\}$. It follows that either $w - 3 = x$ or $w + 3 = y$. In the first case we obtain $y = 3, w + 3 = 0, x = w = 6, s = 9$, which leads to a contradiction. It follows $w + 3 = y, w - 3 = 3, w = 6, x = 0, I_j \cup \{w\} = \{0, 3, 6, 9\}$ and therefore $s = 8, j = 2$. □

4 Same cardinality

For the purposes of the proof of Theorem 1 we use the notation that $f(x) = x^{n(D)} + ux^{n(E)}$ is a crooked function, where $0 \neq u \in F$ and $D, E \subseteq \Omega$ such that $|D|, |E| \geq 2$.

Lemma 11. *Either D or E is in a long orbit.*

Proof. Assume both D and E are in short orbits. Let the stabilizers of d, e in the Galois group have orders $i, j > 1$, respectively. Let $L_1 = GF(2^{r/i}), L_2 = GF(2^{r/j})$ be the smallest subfields containing the x^d and x^e, respectively. It follows $\delta_{f,a}(F) \subseteq L_1 + uL_2$. As $\delta_{f,a}$ is 2 to 1 we have $2^{r-1} \leq |L_1 + uL_2| \leq 2^{r/i+r/j}$, hence $r \leq 1 + r/i + r/j$.

Assume $i, j > 2$. Then $r \leq 3$ and $i = j = 1$, contradiction. Let $i = 2, j > 2$. It follows that r is even and ≤ 6. Clearly $r = 4$ yields the contradiction $j = 4$. Let $r = 6, i = 2, j = 3$. We have

$$f(x) = x^{9m} + ux^{21n}.$$

It follows $f(x) = f(\omega x) = f(\overline{\omega} x)$ for all x and because of equality in the basic equation we have $\delta_{f,a}(F) = L_1 + uL_2$ for all a. This shows that aside of $f(0) = 0$ the function f is 3 to 1 : each of the 21 nonzero elements of $L_1 + uL_2$ has precisely 3 preimages under f. This is impossible as u is not in the image of f.

The final case is $i = j = 2$. We have $r = 2s, q = 2^s, L_1 = L_2 = \mathbb{F}_q$ and $f(x)$ has the form

$$f(x) = N(x^i) + uN(x^j),$$

where $N(x) = x^{q+1}$. We have

$$\delta_{f,a}(x) = N((x + a)^i) + N(x^i) + u(N((x + a)^j) + N(x^j)).$$

Let $1 \neq w \in W$, where W is the subgroup of order $q+1$. Then $\delta_{f,a}(a/(w+1)) = 0$. It follows that 0 has $q > 2$ different preimages, contradiction. □

Choose notation such that D is in a long orbit.

Proposition 2. *If* $|D|, |E| > 1$, *then* $|D| = |E|$.

Proof. Recall that D is in a long orbit. Assume at first $|D| > |E|$ and $|D| \geq 3$. Observe that no translate of a maximal subset of D can be a proper subset of the smaller set E. Assume that D is not a punctured coset. There is a maximal subset $K_0 \subset D$ such that $K_0 + a \not\subset D$ for all $a \neq 0$ (Theorem 4). In particular K_0 is in a long orbit and we are done.

It follows that D can be chosen to be a punctured subgroup, more precisely $r = st$, $H = \{0, s, 2s, \ldots, (t-1)s\}$ is the subgroup of order t and $D = H \setminus \{0\}$. As $|D| = t - 1 \geq 3$ we have $t \geq 4$. Lemma 7 shows that the maximal subsets of D come in $\lfloor t/2 \rfloor$ orbits, and that with one exception in the even case those orbits are long . Choose $K = H \setminus \{0, s\} = D \setminus \{s\}$ to be such a representative. Then $K - s \subset D$ is the second representative of the same orbit and

$$0 = \beta_a(K) = \alpha g_s(a) + \alpha^{2^s} a.$$

This is equivalent with $\alpha/a \in L$, where $L = \mathbb{F}_q,\ q = 2^s$.

Assume $|E| \leq t - 3$. Let $M = H \setminus \{0, s, 2s\}$. Assume $M - c = M$ for $c \neq 0$. Clearly then $c \in H$ and $\{0, s, 2s\} - c = \{0, s, 2s\}$. It follows $t = 3$, contradiction. We conclude that M is in a long orbit. Assume $M - c \subset D$. Clearly $c \in H$ and $0 \in \{0, s, 2s\} - c$. It follows $c \in \{0, s, 2s\}$ and

$$0 = \beta_1(M) = \alpha + g_s(\alpha) + g_{2s}(\alpha) = \alpha + \alpha + \alpha = \alpha.$$

This shows $|E| = t - 2$. We use the same counting arguments as before. Assume at first t is divisible by 3. Among the $\binom{t-1}{2}$ second to maximal subsets

$H \setminus \{0, is, js\}$ of D one plays a special role (corresponding to the subgroup of order $3 : is = -js, 3is = 0$). The remaining subsets are in long orbits, each with 3 representatives in D. This yields $(\binom{t-1}{2} - 1)/3 = t(t-3)/3$ such orbits. If this number is $> (t-2)$, then there must be such an orbit which is not represented as a subset of E. This is indeed the case as $t \geq 6$. For such a subset $M = H \setminus \{0, is, js\}$ we have $M - c \subset D$ precisely for $c \in \{0, is, js\}$ and

$$0 = \beta_1(M) = \alpha + \alpha + \alpha.$$

Assume now t is not divisible by 3. This time the second to maximal subsets of D come in $\binom{t-1}{2}/3$ orbits, each with 3 representatives as subsets of D. The same argument as before works if $(t-1)(t-2)/6 > t-2$, equivalently $t > 7$. Only cases $t \in \{4, 5, 7\}$ remain.

Let $t = 7$. Each of the 5 orbits of second to maximal subsets of D must be represented as a subset of E as well, necessarily then exactly once. As $M_1 = \{3s, 4s, 5s, 6s\}$ is represented we have $E = \{x + 3s, x + 4s, x + 5s, x + 6s, y\}$. After replacing E by a translate we see that Z_7 must contain a 5-subset $\{3, 4, 5, 6, j\}$ which represents each of the 5 orbits of 4-subsets exactly once. Clearly $j \neq 2, j \neq 0$ as in each of these cases an interval is represented twice. We have $j = 1$. As in this case $\{1, 3, 5, 6\}$ and $\{1, 3, 4, 6\}$ are both represented and translates of one another a contradiction is obtained.

Let $t = 5$. As $M_1 = \{s, 2s\}$ and $M_2 = \{s, 3s\}$ are in different orbits of full length which are represented 3 times as subsets of D we must have that differences s and $2s$ are represented in E. It follows $E = \{x, x + s, y\}$, where we can choose y as either $x + 2s$ or as $x + 3s$. In the first case the translates of M_1 which are subsets of E are $M_1 - s + x,\ M_1 + x$. It follows

$$0 = \beta_1(M_1) = \alpha + g_{s-x}(u\alpha) + g_{-x}(u\alpha).$$

The unique translate of M_2 which is a subset of E is $M_2 - s + x$. This yields

$$0 = \beta_1(M_2) = \alpha + g_{s-x}(u\alpha).$$

Together with the M_1-equation the contradiction $\alpha = 0$ is obtained. We can assume $y = x + 3s$. Consider singletons now. We have

$$0 = \beta_1(\{0\}) = (u\alpha) + g_{-s}(u\alpha) + g_{-3s}(u\alpha) = u + g_{-s}(u) + g_{-3s}(u).$$

Applying g_{-s} twice again we obtain

$$u + g_{-2s}(u) + g_{-3s}(u) = 0.$$

Together with the equation above this yields $u = g_{-s}(u)$ which in turn shows $u = 0$.

The final case is $t = 4$. We have $r = 4s$,

$$D = \{s, 2s, 3s\},\ E = \{0, e\} - c.$$

Let $q = q^s$ and

$$K = GF(q) \subset L = GF(q^2) \subset F = GF(q^4).$$

Let $N(x) = x^{1+q+q^2+q^3}$ be the norm : $F \longrightarrow K$. The condition relative to subset $\{2s, 3s\}$ is $\alpha/a \in K$. The condition given by the short orbit containing $\{s, 3s\}$ is $\alpha\overline{a} \in L$. This is implied by the condition $\alpha/a \in K$. Only the singleton condition remains. It is

$$\alpha\overline{a}g_s(a) + \overline{\alpha}ag_s(a) + g_s(\alpha)a\overline{a} = g_{c+s}(\overline{u\alpha})g_{s+e}(\overline{a}) + g_{c-e+s}(\overline{u\alpha})g_{s-e}(\overline{a})$$

The first two terms on the left coincide. After taking conjugates and applying g_{3s} :

$$\overline{\alpha}g_s(a\overline{a}) = g_c(u\alpha)g_e(a) + g_{c-e}(u\alpha)g_{-e}(a)$$

Let $t = gcd(e, 4s)$ and $M = GF(2^t)$ the fixed field of g_e.

For any a and any element $\chi \in K$, which is also fix under g_c and under g_e, we have that $\alpha\chi$ also satisfies the hyperplane condition. As the hyperplane has to be uniquely determined it follows $gcd(c, e, s) = 1$. In case $a = 1$ the element α is determined by

$$\alpha \in K,\ g_{-c}(\alpha) = u\alpha + g_{-e}(u\alpha).$$

We use the second derivative. Let $\delta(x) = f(x) + f(x+1)$ be the first derivative at $a = 1$ and $e_b(x) = \delta(x) + \delta(x+b)$ the derivative of δ at $b \neq 1$. A contradiction is obtained if we find $b \neq 1$ and $x \in F$ such that $e_b(x) = 0$. Choose $b \in L \setminus K$. Then

$$\delta(x) = x^{q^3+q^2} + x^{q^3+q} + x^{q^2+q} + x^{q^3} + x^{q^2} + x^q + 1$$

and

$$e_b(x) = (x^{q^3} + x^q)(b + b^q) + b + b^{2q} + ug_{-c}(b + g_e(b)).$$

The value of $e_b(x)$ depends only on $x + \overline{x} = x + x^{q^2} = tr_{f|L}(x)$. Assume at first $M \not\subseteq K$. Choose $b \in (M \cap L) \setminus K$. Then

$$e_b(x) = (x^{q^3} + x^q)(b + b^q) + b + b^{2q}$$

and we can choose x such that $e_b(x) = 0$, contradiction. We have $M \subseteq K$. Consider α in case $a = 1$. We know $\alpha \in K$. As $M \subseteq K$ we have $tr_{L|M}(\alpha) = 0$. By Theorem 90 there exists $y_0 \in L$ such that

$$g_{-c}(\alpha) = y_0 + g_{-e}(y_0).$$

As $M \subseteq L$ it follows that all y satisfying this equation are in L. In particular $u\alpha \in L$. It follows $u \in L$. This shows that for $b \in L \setminus K$ we can find $x \in F$ such that $e_b(x) = 0$, contradiction.

Assume now $|E| > |D|$. By symmetry we can assume that E is in a short orbit. Let $|Z(E)| = s$, where $r = st$. We have $|E| = mt$ and E is the union of m cosets of the subgroup $H = \{0, s, \ldots, (t-1)s\}$. Let $T, N : F \longrightarrow L$ be the trace and norm from F to $L = \mathbb{F}_q$, where $q = 2^s$. Let K be a maximal subset of E. Then K is in a long orbit and $K - c \subset E$ if and only if $c \in H$. The powers of a in the definition of $\beta_a(K)$ are $n((E + c) \setminus K) = n(E \setminus K)$. It follows

$$0 = \beta_a(K) = \sum_{c \in H} (u\alpha)^{2^c} a^{n(E \setminus K)},$$

hence $T(u\alpha) = 0$.

Let M be in a long orbit. The set of all j satisfying $M - j \subset E$ is a union of cosets of H. Write it in the form $J_0 + H$. The second sum in the definition of $\beta_a(M)$, corresponding to representatives in E, is

$$\sum_{j,c} g_{j+c}(u\alpha) a^{n(E+j \setminus M)} = \sum_j g_j \Big(\sum_c g_c(u\alpha) a^{n(E+j \setminus M)}\Big) = 0,$$

where $j \in Y_0, c \in H$. In particular we obtain a contradiction if D is not a punctured coset.

Let D be a puncturing of the subgroup of order s'. We can choose $D = \{s', 2s', \ldots, (t'-1)s'\}$, where $r = st = s't'$. The argument used in the proof of the main theorem of [7] is based on maximal and second to maximal subsets of D. It gives a contradiction if $|D| > 2$. This shows that $D = \{s', 2s'\}$ is a puncturing of the subgroup of order $3 : r = 3s'$.

Let $q' = 2^{s'}$. Consider

$$\delta_{f,1}(x) = x^{q'} + x^{q'^2} + 1 + u(x^{n(E)} + (x+1)^{n(E)}) = x^{q'} + x^{q'^2} + 1 + u(N(x^i) + N((x+1)^i)$$

where N is the norm down to L. Let S be the space of elements whose trace to $GF(q')$ vanishes. We have $\delta_{f,1}(F) \subseteq S + 1 + uL$. Because of the APN condition we have $|\delta_{f,1}(F)| = 2^{r-1}$. This yields $r-1 \leq 2s'+s$, equivalently $s \geq s'-1$.

Assume at first $s = s'-1$. As s divides r we have $s=3, s'=4, r=12$. In that case $\delta_{f,1}$ is constant on $\mathbb{F}_{16}$, contradiction. Let next $s=s'$. Recall $r=3s$.

The condition $\beta_a(\{0\})=0$ reads $\alpha g_{2s}(a) = g_{-s}(\alpha)a$, equivalently $\alpha/a \in L$. Let $\alpha = \lambda a$. We have $0 = T(u\alpha) = T(ua\lambda) = \lambda T(ua)$ for all a. This leads to the contradiction $u=0$.

Assume now $s > s'$. We have $t=2$, hence $r = 6r_0, s = 3r_0, s' = 2r_0, D = \{2r_0, 4r_0\}$ and E is a union of cosets of $\{0, 3r_0\}$. Let $q_0 = 2^{r_0}$. The derivative $\sigma_{f,1}$ is constant on those $x \in GF(q_0^2)$ which also satisfy $N((x+1)/x) = 1$. As $N(x) = x^{q_0+1}$ for $x \in GF(q_0^2)$ the latter condition is satisfied when $(x+1)/x$ is a (q_0+1)-st root of unity. This leads to q_0 solutions x. It follows $q_0 = 2, r_0 = 1$, so we are working in $\mathbb{F}_{64}$. The condition $T(u\alpha) = 0$ is equivalent with $u\alpha \in \mathbb{F}_8$. The condition $\beta_a(\{0\}) = 0$ is equivalent with $\alpha a \in \mathbb{F}_4$. Choosing a as an element whose order does not divide 21 leads to a contradiction. $\square$

Lemma 12. *If D and E have the same cardinality, then they are in orbits of full length.*

Proof. Without restriction D is in a long orbit. Assume E is in a short orbit. Use the established terminology: $|E| = mt$, where $r = st$, the subgroup H of order t is the full stabilizer of E and E is the union of m cosets of H. Let $L = \mathbb{F}_{2^s}$.

Assume there is a maximal subset of E whose orbit is not represented by a subset of D. We saw in the proof of Proposition 2 that $T(u\alpha) = 0$ for all $\alpha = \alpha(a)$ in this case and D is a punctured coset. Just as in the proof of Proposition 2 a contradiction is obtained if $l > 2$.

We can therefore assume that the orbit of each maximal subset of E contains a (maximal) subset of D. It follows that D consists of $m-1$ cosets, one punctured coset and an isolated point (with respect to H). Assume $t > 2, m > 1$. There are m different orbits of maximal subsets of E, but only one of them can also be represented in D, contradiction. Assume $t > 2, m = 1:$ E is a coset of H and without restriction

$$D = (H \setminus \{0\}) \cup \{x\},\ x \neq 0.$$

Let $K = D \setminus \{s\}$. As K has an isolated point it is not represented in E. Also, its orbit has full length and has only one representative in D, contradiction.

We have $t = 2$. Let $b = -b$ be the involution. The maximal subsets of E come in m orbits. Each of these m orbits must be represented by a subset of D as well. As D has only two maximal subsets with precisely one isolated point we have $m = 2$, so $|D| = 4$.

Let $E = \{0, b\} \cup \{z, z + b\}$ and $D = \{x, x'\} \cup \{y, y + b\}$, where $x + x' \neq b$. We can choose notation such that

$$\{0, z, z + b\} + c = \{x, y, y + b\}$$

and

$$\{0, b, z\} + c' = \{x', y, y + b\}$$

Necessarily $c = x,\ c' = x' - z$. The first translate shows that we can choose $y = z + x$ (replacind if necessary z by $z + b$). The second translate shows that without restriction $y = x' - z$, hence $x' = x + 2z$. Consider the remaining maximal subsets of D :

$$K = \{x, x + z, x + 2z\}, K' = \{x, x + z + b, x + 2z\}.$$

They are from different orbits, at least one of which is long, contradiction. □

5 Same types

Proposition 3. *If $|D| = |E| = l \geq 4$, then D and E have the same type.*

Proof. Assume the types are different. The condition $i(D) \leq i(E) + j(E)$ shows that type $\mathcal{A}$ cannot be involved. Type $\mathcal{B}, \mathcal{C}$ is obviously impossible.

Types $\mathcal{B}, \mathcal{D}$

We have

$$D = U_1 \cup \cdots \cup U_m \cup \{x\}$$

where the U_i are cosets of the subgroup of order a, and

$$E = V_1 \cup \cdots \cup V_n \cup I$$

where the V_j are cosets of the subgroup of order b and I is an interval whose stepwidth is an element of order b such that $2 \leq |I| = r \leq b - 2$. In particular $l = ma + 1 = nb + r$. Observe that because of the basic condition the long orbits of maximal subsets are in bijection.

Assume at first $r > 2$. Denote the endpoints of I by L, R. Then $E \setminus \{L\}$ has type $\mathcal{D}$. It follows that a puncturing of D has type $\mathcal{D}$. Its distribution on the cosets of the subgroup of order a is $1, a-1, a \ldots$. In order to be of type $\mathcal{D}$ it must have two maximal subsets in the same orbit. This forces $a = 2$. Consider $E \setminus L$. As it is in the same orbit as a puncturing of D it follows that after removal of two more points a 2-periodic set is obtained. Let $E \setminus \{L, P, Q\}$ be 2-periodic. The same holds for $E \setminus R$. If $R \notin \{L, P, Q\}$ then two of the points of $\{L, P, Q\}$ form a conjugate pair. This shows that E has a maximal subset in a short orbit, contradicting the type. We have that $E \setminus \{L, R, Q\}$ is 2-periodic. Assume $r > 3$. Then $I \setminus \{L, R\}$ still has type $\mathcal{D}$. On the other hand it contains a 2-periodic maximal subset, contradiction. We conclude $r = 3$. Write $I = \{L, M, R\}$. Applying the same argument to M we see $Q = M$. It follows that $E \setminus I$ is 2-periodic, in other words b is even. As $r = 3 \leq b - 2$ we have $b \geq 6$. Pick $P \in V_1$. Then $E \setminus P$ contains precisely $(l-5)/2$ conjugate pairs. On the other hand, as it is in the same orbit as a puncturing of D it contains $(l-3)/2$ such pairs, contradiction. It follows $n = 0$, hence $l = 3$.

We have shown $r = 2, I = \{L, R\}$. It follows $b \geq 4$. As $E \setminus L$ is in the same orbit as a puncturing of D it follows that the b-periodic set $E \setminus I$ is in the same orbit as a double puncturing of D. The distribution of such a double puncturing on the cosets of the subgroup of order a is one of the following:

$$a-1, a, \ldots \text{ or } 1, a-2, a \ldots \text{ or } 1, a-1, a-1, a \ldots$$

The types involving 1 are impossible as $b \geq 4$. It follows that the b-periodic set $E \setminus I$ is a puncturing of an a-periodic set. This is impossible.

Types $\mathcal{B}, \mathcal{E}$

This is similar to the previous case. The counting condition implies that the subgroup underlying the set of type $\mathcal{E}$ has order 3. We have

$$D = U_1 \cup \cdots \cup U_m \cup \{x\}$$

as above, and

$$E = V_1 \cup \cdots \cup V_n \cup \{L, R\}$$

where the V_j are cosets of the subgroup of order 3. The sets $E \setminus L$ and $E \setminus R$ are in the orbit of a subset of D, and the 3-periodic set $E \setminus \{L, R\}$ therefore is in the same orbit as a double puncturing of D. The distribution of this double puncturing on the cosets of the subgroup of order a is one of

$$1, a-2, a \dots \text{ or } 1, a-1, a-1, a \dots$$

The only possibility is that $a = 2$.

It follows that there exist P, Q such that $E \setminus \{L, P, Q\}$ is 2-periodic. The same is true with R in the place of L. Comparison yields that without restriction $P = R$. It follows that $E \setminus \{L, R, Q\}$ is periodic, a periodic set which is the puncturing of a periodic set, contradiction as before.

Types $\mathcal{D}, \mathcal{C}$

The counting argument shows that the set of type $\mathcal{C}$ satisfies $g = 2$. It is therefore the puncturing of a 4-periodic set. Let D be the set of type $\mathcal{D}$ and L, R the endpoints of its interval. All points but one of the type $\mathcal{C}$ set E come in conjugate pairs. It follows that every $x \in D \setminus \{L, R\}$ satisfies the following: there are $P_x, Q_x \in D$ such that $D \setminus \{x, P_x, Q_x\}$ is 2-periodic. Fix x and choose $y \in D \setminus \{x, L, R\}$. This is possible if $l > 3$. If $y \notin \{x, P_x, Q_x\}$, then two of the three elements of this set form a conjugate pair and D therefore contains a 2-periodic maximal subset, contradiction. It follows $l \leq 5$. As l is 3 mod 4 we are back in case $l = 3$.

Types $\mathcal{D}, \mathcal{E}$

We have

$$D = U_1 \cup \dots \cup U_m \cup I$$

where the U_i are cosets of the group of order a and $I = \{l, \dots, r\}$,

$$E = V_1 \cup \dots \cup V_n \cup W$$

is a puncturing of a b-periodic set, where b is odd. The counting condition shows $b \leq 5$.

Consider the case when $b = 5$. We have $i(D) = l - 2, j(D) = 1$ and $i(E) = l - 4, j(E) = 2$. Let $w \in W$. Then $E \setminus w$ is conjugate to a puncturing of D. The distribution of this puncturing of D on the cosets of the group of order 5 is therefore $3, 5, 5, \dots$ The distribution of D itself cannot be $4, 5, 5 \dots$ as this would be type $\mathcal{E}$. It follows that D has type $1, 3, 5 \dots$ The isolated element in D corresponds to the orbit of $E \setminus w$. It follows that the second such orbit leads to a different isolated element in D, contradiction.

We have $b = 3, i(D) = l - 2, j(D) = 1, i(E) = l - 2, j(E) = 1$. Let $x \in D, x \neq l, r$. Then $D \setminus x$ is conjugate to a puncturing of E and therefore has type either $1, 3, 3 \dots$ or $2, 2, 3, , , , , , , \dots$ The type of D itself is therefore $1, 1, 3 \dots$ or $1, 2, 2, 3, \dots$ and x is an isolated point in D. This shows $D = I$ of length ≤ 4. On the other hand l is 2 mod 3, contradiction.

Types $\mathcal{C}, \mathcal{E}$

We have subsets $U = \cup_{i=1}^{m} U_i$ and $V = \cup_{j=1}^{n} V_j$ such that the U_i are cosets of the subgroup of order $a = 2g > 2$, the V_j are cosets of the group of odd order b. Moreover we assume that a and b are the full stabilizer orders. Then $D = U \setminus x_0$ and $E = V \setminus y_0$ where notation is chosen such that $x_0 \in U_m, y_0 \in V_n$. As the cardinalities are the same we have $am = bn = l + 1$. In particular n is even. Denote by $\overline{x}$ the partner of x which together with x forms a 2-periodic pair.

Let $y \in V \setminus V_n$. There is $x \in U \setminus U_m$ such that $U \setminus \{x_0, x\} \sim V \setminus \{y_0, y\}$. As we can take away two points from $U \setminus \{x_0, x\}$ and obtain a 2-periodic set, the same must be true of $V \setminus \{y_0, y\}$. Let $V \setminus \{y_0, y, y_1, y_2\}$ be 2-periodic. Choose now $y' \in V$ such that $y' \notin V_m$ and also $y' \notin \{y_0, y, y_1, y_2\}$. The same argument as above shows that we can take away 4 points from $V \setminus \{y_0, y'\}$ and obtain a 2-periodic set. This set of 4 points intersects $\{y_0, y, y_1, y_2\}$ in precisely 2 points. The remaining two points of this set form a pair. This shows that E contains a maximal subset in a short orbit, contradiction. The choice of y' will be possible if $b > 3$ or $b = 3, n > 2$. Assume $b = 3, n = 2$. Then $m = 1, a = 6$. As $i(E) = 3, i(D) = 0, j(D) = 2$ we reach a contradiction. $\square$

6 Small cardinalities

Case $|D| = |E| = 2$ is special as the derivatives are linear functions. The function is crooked if and only if it is APN. Let $D = \{0, i\},\ E = \{j, k\}$. We have

$$\delta_{f,a}(x) = (x + a)g_i(x + a) + xg_i(x) + ug_j(x + a)g_k(x + a) + ug_j(x)g_k(x).$$

After forgetting constants we obtain

$$d_a(x) = xg_i(a) + ag_i(x) + u(g_j(x)g_k(a) + g_j(a)g_k(x),$$

a linear function. Write $x = ay$. Then

$$d_a(y) = yag_i(a) + g_i(y)ag_i(a) + u(g_j(a)g_k(a)g_j(y) + g_j(a)g_k(a)g_k(y)).$$

We collect terms and see $a = x$ as a variable:

$$d(x, y) = xg_i(x)(y + g_i(y)) + ug_j(x)g_k(x)(g_j(y) + g_k(y)).$$

Our function is crooked if for every $x \neq 0$ this function as a function of y alone has rank $r-1$. As $d(x, 1) = 0$ the condition is that $d(x, y) \neq 0$ whenever $xy \neq 0$ and $y \neq 1$. Equivalently: the equation

$$xg_i(x)(y + g_i(y)) = ug_j(x)g_k(x)(g_j(y) + g_k(y))$$

is satisfied only when $xy = 0$ or $y = 1$. An obvious condition is that the fixed field of g_i and g_{j-k} is $\mathbb{F}_2$.

Lemma 13. *The function $f(x) = xg_i(x) + ug_j(x)g_k(x)$ is APN (crooked) if and only if the following hold: $i, j-k, r$ do not have a common divisor and u is not representable in the form*

$$u = \frac{xg_i(x)}{g_j(x)g_k(x)} \frac{y + g_i(y)}{g_j(y) + g_k(y)}$$

where y not in the fixed field of g_i or of g_{j-k}.

Substituting λx for x the right side picks up a factor $\lambda g_i(\lambda)/(g_j(\lambda)g_k(\lambda)$. A contradiction is obtained if this mapping has all of F^* as its image. We must have $d = (2^r - 1, 1 + 2^i - 2^j - 2^k) \neq 1$. Let U be the subgroup of order $(2^r - 1)/d$. The condition is that the image of the mapping $y \mapsto \frac{y+g_i(y)}{g_j(y)+g_k(y)}$ together with U does not generate all of F^*.

Let now $|D| = |E| = 3$. Type $\mathcal{E}$ does not occur. Here are the possible types:

type	$i(D)$	$j(D)$	representative
$\mathcal{A}$	3	0	
$\mathcal{B}$	2	0	$\{0, r/2, d\}, 2d \neq r/2$
$\mathcal{C}$	0	1	$\{0, r/4, r/2\}$
$\mathcal{D}$	1	1	$\{0, d, 2d\}, 2d \neq r/2.$

Consider at first the mixed types. The only possibilities are $\{\mathcal{B}, \mathcal{D}\}$ and $\{\mathcal{C}, \mathcal{D}\}$.

Types $\{\mathcal{C},\mathcal{D}\}$.

$$D=\{0,r/4,r/2\},\ E=\{0,e,2e\}-c.$$

Here $2e\neq r/2$. As $\{0,2e\}\sim\{0,r/4\}$ it follows $2e=\pm r/4$ and $ord(e)=8$. As $r/4$ is determined only up to a sign we can choose notation such that $2e=r/4$. We have

$$D=\{0,2e,4e\},\ E=\{0,e,2e\}-c$$

where $ord(e)=8$. Denote $\overline{x}=g_{4e}(x), L=\mathbb{F}_q$, where $q=2^e$, and $K=\mathbb{F}_{q^4}$. We use only $a=1$.

With $M_1=\{2e,4e\}$ we have

$$\alpha+g_{2e}(\alpha)=g_{2e+c}(u\alpha).$$

The condition arising from $\{0,4e\}$ is

$$\alpha\in K.$$

The only remaining orbit of maximal subsets corresponds to $M_2=\{e,2e\}-c$. It reads

$$u\alpha=g_e(u\alpha).$$

This implies $u\alpha\in L$, the $\{0,4e\}$-condition yields $\alpha=\overline{\alpha}\in K$, and because of the M_1-condition

$$u\alpha=g_{-c}(\alpha)+g_{2e-c}(\alpha).$$

The singleton $\{4e\}$ shows

$$\alpha+g_{2e}(\alpha)+g_{4e}(\alpha)=g_c(u\alpha),$$

which by the above equation equals $\alpha+g_{2e}(\alpha)$, hence $\alpha=0$, contradiction.

Types $\{\mathcal{B},\mathcal{D}\}$

Assume D has type $\mathcal{B}$ and E has type $\mathcal{D}$:

$$D=\{0,r/2,d\},\ E=\{0,e,2e\}-c.$$

If $\{0,d\}$ is matched with $\{0,e\}$ and $\{r/2,d\}$ with $\{0,2e\}$ two solutions come up, either $d=e,3d=r/2$ or $e=-d,3d=r/2$. Similarly, when $\{0,d\}$ is matched with $\{0, 2e\}$ and $\{r/2, d\}$ with $\{0, e\}$ there are two more possibilities: $d = 2e, 3e = r/2$ or $d = -2e, 3e = r/2$. However all four possibilities are equivalent:

$$D = \{0, 3d, d\},\ E = \{0, d, 2d\} - c,$$

where $r = 6d$. Let $L = \mathbb{F}_{q^3}$, where $q = 2^d$. We use only $a = 1$. Subset $M_1 = \{r/2, d\}$ shows $\alpha = g_{c+d}(u\alpha)$. Likewise $M_2 = \{0, d\}$ yields

$$\alpha = g_c(u\alpha) + g_{c-d}(u\alpha).$$

Finally the singleton yields

$$\alpha + \overline{\alpha} + g_{-d}(\alpha) = g_c(u\alpha) + g_{c-d}(u\alpha) + g_{c-2d}(u\alpha).$$

Here $\overline{a} = g_{3d}(a)$. Comparison of the first two equations yields

$$u\alpha + g_d(u\alpha) + g_{-d}(u\alpha) = 0.$$

Using this in the last equation we obtain

$$\alpha + \overline{\alpha} + g_{-d}(\alpha) = g_{c+d}(u\alpha + \overline{u\alpha}).$$

This implies $\alpha \in L$. The first equation shows now $u \in L$. Back to the last equation the contradiction $\alpha = 0$ is obtained.

We come to the pure types.

Types $\{\mathcal{A}, \mathcal{A}\}$

Let

$$D = \{0, d_1, d_2\},\ E = \{0, e_1, e_2\} - c.$$

We can choose $e_1 = d_1 = i, d_2 = j$. Assume

$$\{0, j\} + c_1 = \{0, e_2\}, \{i, j\} + c_2 = \{i, e_2\}.$$

If $c_1 = 0$ or $c_2 = 0$ then $j = e_2$ and D, E are conjugates. The remaining possibility shows $c_1 = e_2 = -j,\ c_2 = e_2 - i = i - j$ which implies $2i = 0$ and the contradiction that $\{0, i\}$ is in a short orbit. Assume

$$\{0, j\} + c_1 = \{i, e_2\}, \{i, j\} + c_2 = \{0, e_2\}$$

All cases but one lead to the usual contradiction: either $2i = 0$ or $2j = 0$ or $2(i - j) = 0$, implying a short orbit. The remaining case is $c_1 = e_2, c_2 = -j$.

It follows $e_2 = i - j$. We have $E - i = \{0, -i, -j\} - c$. After a slight change of notation we are in case

$$D = \{0, i, j\},\ E = \{0, -i, -j\} - c.$$

Here $j \neq -i$ as D, E are not conjugate. Let $M_1 = \{0, i\},\ M_2 = \{0, j\},\ M_3 = \{i, j\}$. We have $\beta_a(M_k) = 0$. This yields the equations

$$\alpha g_j(a) = g_{i+c}(u\alpha)g_{i-j}(a)$$

$$\alpha g_i(a) = g_{j+c}(u\alpha)g_{j-i}(a)$$

$$\alpha a = g_{i+j+c}(u\alpha)g_{i+j}(a)$$

In case $a = 1$ this yields

$$\alpha = g_{i+c}(u\alpha) = g_{j+c}(u\alpha) = g_{i+j+c}(u\alpha)$$

which implies that $u\alpha$ is fix under g_i and g_j. We have $\alpha = g_c(u\alpha)$ in this case. Let K be the fixed field of g_i and g_j. We have $u\alpha \in K$, therefore $\alpha \in K$ and finally $u \in K$.

We continue with general a. In order to get rid of g_c apply g_j to the first equation above, g_i to the second and solve for the common term $g_{i+j+c}(u\alpha)$. This yields

$$g_{i+j+c}(u\alpha) = g_j(\alpha)\frac{g_{2j}(a)}{g_i(a)} = g_i(\alpha)\frac{g_{2i}(a)}{g_j(a)} = \alpha\frac{a}{g_{i+j}(a)}. \tag{1}$$

The first identity on the right can be written as

$$\frac{g_j(\alpha)}{g_i(\alpha)} = \frac{g_i(a)g_{2i}(a)}{g_j(a)g_{2j}(a)}$$

Written out this becomes

$$1 = (\alpha a^{1+2^i+2^j})^{2^j-2^i}.$$

This shows that $\lambda = \alpha a^{1+2^i+2^j}$ is in the fixed field of g_{j-i}. Analogously the second equation simplifies to $g_j(\lambda) = \lambda$. We have $\lambda \in K$.

Back to the special case $a = 1$. The hyperplane condition is satisfied by α if and only if $\alpha = g_c(u\alpha) \in K$. Because of the APN condition there must exactly one solution α. This shows k and c are coprime.

Restrict f to K. We have

$$f(x) = x^3 + ux^{32^c}$$

for $x \in K$, and

$$f(x+a) + f(x) = ax^2 + a^2x + a^3 + ug_c(ax^2 + a^2x + a^3) =$$

$$= ax(x+a)(1 + u(ax(x+a)^{2^c-1}) + a^3 + g_c(a^3).$$

Let $y = ax(x+a)$ and $V \subset K$ the hyperplane consisting of the elements of absolute trace 0. Then $y \in a^3V$. We have $f(x) + f(x+a) = y + ug_c(y) + a^3 + uG_c(a^3)$. Consider the function $d(y) = y + ug_c(y)$. Assume $k > 2$. There is a uniquely determined $y \neq 0$ such that $d(y) = 0$. As $k > 2$ we can find $a \in K$ such that $y = a^3v$, where $v \in V$. We can find x such that $y/a^3 = (x/a) + (x/a)^2$. For this choice of x, a we have $f(x+a) + f(x) = f(0)$, contradiction. We conclude that K is either $\mathbb{F}_2$ or $\mathbb{F}_4$.

Assume $K = \mathbb{F}_2$. In particular $u = 1$ and $\lambda = 1$ for all a. Expressing α in terms of a and using Equation 1 we obtain

$$g_{i+j+c}(a)g_{2i+j+c}(a)g_{i+2j+c}(a) = g_i(a)g_j(a)g_{i+j}(a)$$

for all a. It follows that the sets $\{i+j, i+2j, 2i+j\}$ and $\{i, j, i+j\}$ are in the same orbit. This implies that either $j = 2i$ or $i = 2j$ or $\{i, j\} = \{-i, -j\}$, contradiction in each case.

We have $K = \mathbb{F}_4$. In particular r is even. The same equation as before shows that $g_{c+i+j}(a)g_{c+2i+j}(a)g_{c+i+2j}(a)$ and $g_i(a)g_j(a)g_{i+j}(a)$ have the same third powers, equivalently

$$g_{c+i+j}(a)g_{c+2i+j}(a)g_{c+i+2j}(a)g_{c+i+j+1}(a)g_{c+2i+j+1}(a)g_{c+i+2j+1}(a) =$$

$$= g_i(a)g_j(a)g_{i+j}(a)g_{i+1}(a)g_{j+1}(a)g_{i+j+1}(a)$$

for all a. Assume the 2-weight is 6 on both sides, equivalently no two of the indices are identical (mod r) on either side. Then the sets $\{i+j, 2i+j, i+2j, i+j+1, 2i+j+1, i+2j+1\}$ and $\{i, j, i+j, i+1, j+1, i+j+1\}$ are in the same orbit. A case by case analysis shows that this is not true. So the 2-weight is < 6. As i is different from $j, i+j, i+1$ it can only equal $j+1$ or $i+j+1$. As i and j occur in symmetric positions we only need to consider the cases $i = 1$ and $i = j+1$. Consider at first case $i = 1$. The first set of exponents is $\{1, j, j+1, 2, j+1, j+2\}$, equivalent to $\{1, 2, j, j+3\}$, The second is $\{j+1, j+2, 2j+1, j+2, j+3, 2j+2\}$, which is equivalent to $\{j+1, j+4, 2j+1, 2j+2\}$. It is easy to see that the weight cannot be smaller: as $1, 2, j$ are pairwise different and $j \neq 2, -1$, the only possibility for the first set to have smaller weight is when $j = -2$, but then the weight of the second set is still 4, contradiction. As the weight is 4 these two sets must be translates of one another:

$$\{j+1, j+4, 2j+1, 2j+2\} = \{1, 2, j, j+3\} + c.$$

This is excluded by a case by case analysis. The second case $i = j+1$ is handled in a similar way. Type $\mathcal{A}$ does not occur.

If both exponents are of type $\mathcal{C}$, then they are in the same orbit.

Types $\{\mathcal{B}, \mathcal{B}\}$

We can choose

$$D = \{0, r/2, d\}, E = \{0, r/2, e\} - c.$$

Let $s = r/2$ and L be the field of order 2^s. The usual argument shows that we can choose $e = -d$. Let $M_1 = \{0, d\}$: the condition $0 = \beta_a(M_1)$ reads

$$\alpha\overline{a} = g_{c+d}(u\alpha)g_d(\overline{a}).$$

In the same way $M_2 = \{r/2, d\}$ yields

$$\alpha a = g_{c+d}(\overline{u\alpha})g_d(\overline{a}).$$

Comparison of the two conditions shows $g_d(\overline{a})/\alpha \in L$, In particular, if $a \in L$, then $\alpha \in L$ and also $u\alpha \in L$. This shows that we have $u \in L$. The condition derived from the short orbit is

$$\alpha g_d(a) + g_c(u\alpha)g_{-d}(a) \in L.$$

The final hyperplane condition is

$$0 = \beta_a(\{0\}) = \alpha\overline{a}g_d(a) + \overline{\alpha a}g_d(\overline{a}) + g_{-d}(\alpha)g_{-d}(a\overline{a}) +$$

$$+ g_c(u\alpha)\overline{a}g_{-d}(a) + g_c(\overline{u\alpha})\overline{a}g_{-d}(\overline{a}) + g_{c+d}(u\alpha)g_d(a\overline{a})$$

This simplifies: the first and last summand coincide by the M_1-condition. Also, the terms by the equality signs coincide. It follows that the remaining terms are identical. After eliminating a common factor and taking conjugates the (0)-condition becomes

$$\alpha g_d(a) = g_c(u\alpha) g_{-d}(a).$$

Let $a \in K = L \cap Fix(g_d) = \mathbb{F}_{2^k}$. We have $\alpha = g_{c+d}(u\alpha) = g_c(u\alpha) = \overline{\alpha} \in K$ which implies $u \in K$. The hyperplane condition in case $a \in K$ is then satisfied precisely for $\alpha \in K, \alpha = g_c(u\alpha)$. If α satisfies this condition, then also $\chi\alpha$ is a solution for $\chi \in K \cap Fix(g_c)$. As because of the APN condition there is only one solution α we must have $gcd(c, d, s) = 1$.

Apply g_d to the (0)-equation, solve both our equations for the term involving u :

$$g_{c+d}(u\alpha) = \alpha\overline{a}/g_d(\overline{a}) = g_d(\alpha)g_{2d}(a)/a.$$

The last equality yields after simplification

$$(\alpha a g_d(a)\overline{a})^{2^d-1} = 1,$$

equivalently $\alpha a^{2^d+1}\overline{a} \in Fix(g_d)$.

Consider now the restriction of f to K. It is

$$f(x) = x^3 + ug_{-c}(x^3).$$

The corresponding restriction of $\delta_a, a \in K$ yields after removal of constants

$$d_a(x) = y + ug_{-c}(y),$$

where $y = ax(x + a) \in a^3V$ and $V \subset K$ is the hyperplane of K consisting of the elements of absolute trace 0.

Assume $k > 2$. As $gcd(k, c) = 1$ there is a unique nonzero solution y of $y + ug_{-c}(y) = 0$. As $k > 2$ we can express y in the form $y = a^3v$, for some a, where $v \in V$. As $v = z + z^2$ for some z we can write $z = x/a$ and obtain $y = ax(x + a)$ for this choice of a, x. This contradicts the APN property of d_a. The exceptional situations correspond to $k = 1$ and $k = 2$.

Case $k = 1$.

Restrict to $a \in L$. As $k = gcd(d, s) = 1$ we have $\alpha a^{2^d+2} = 1$, hence $\alpha = 1/a^{2^d+2}$. An immediate consequence is $u = 1$. Using these values in the M_1-equation yields

$$2^{c+2d} + 2^{c+d+1} \equiv 2^{d+1} + 1 \bmod 2^s - 1.$$

Here we take exponents mod s, in the range between 0 and $s-1$. Assume both expressions have 2-weight 1. This means $d=s-1$ and $2^{c-2}+2^c\equiv 2$, contradiction. The 2-weights are 2. Considering differences mod s we see $d+1\in\{d-1,s-d+1\}$. This shows $2d=s$, contradicting the fact that $gcd(d,s)=1$.

Case $k=2$.

In particular s and d are even, c is odd. The assumption $u=1$ leads to the same contradiction as in case $k>2$. It follows $u\in\mathbb{F}_4\setminus\mathbb{F}_2$. The field $Fix(g_d)$ contains $\mathbb{F}_4$. The restriction of f to $Fix(g_d)$ has the form considered in Theorem 2. If its order were larger than 4, then Theorem 2 would imply $gcd(c,d,2s)>1$, which is not the case. We have $gcd(d,2s)=2$, equivalently $Fix(g_d)=GF(4)$. The same procedure as in case $k=1$ shows

$$2^{c+2d}+2^{c+d+1}+2^{d+2}+1\equiv 2^{c+2d+1}+2^{c+d+2}+2^{d+1}+1 \bmod 2^s-1.$$

A case by case analysis yields a contradiction.

Types $\{\mathcal{D},\mathcal{D}\}$

The last case is that both exponents are of type $\mathcal{D}$:

$$D=\{0,d,2d\},\ E=\{0,e,2e\}-c.$$

The first subcase is when $\{0,2d\}\sim\{0,e\}$ and $\{0,2e\}\sim\{0,d\}$. Without restriction then $5d=0$ and

$$D=\{0,d,2d\},\ E=\{0,2d,4d\}-c.$$

We will need only the equations relative to $a=1$. Subset $\{0,2d\}$ yields

$$\alpha=g_c(u\alpha)+g_{c-2d}(u\alpha),$$

$\{0,d\}$ shows

$$\alpha+g_{-d}(\alpha)=g_{c+d}(u\alpha)$$

and the singleton shows

$$\alpha+g_{-d}(\alpha)+g_{-2d}(\alpha)=g_c(u\alpha+g_{-2d}(u\alpha)+g_d(u\alpha)).$$

Comparison shows $u\alpha = g_{-d}(u\alpha)$, which contradicts the first equation.

The second subcase is when $\{0, 2d\}$ and $\{0, 2e\}$ are in the same orbit. This leads to

$$D = \{0, d, 2d\},\ E = \{0, d + b, 2d\} - c,$$

where $b = r/2$ is the involution. The maximal subsets $\{0, 2d\},\ \{d, 2d\},\ \{d + b, 2d\}$ lead to the following equations:

$$\alpha g_d(a) = g_c(u\alpha) g_d(\overline{a}).$$

$$\alpha a = g_d(\alpha) g_{3d}(a)$$

$$g_c(u\alpha)a = g_{c+d}(\overline{u\alpha}) g_{3d}(\overline{a}).$$

Miraculously the singleton equation is a formal consequence of those three equations.

Choose $a = 1$. Then

$$\alpha = g_c(u\alpha) = g_d(\alpha) = g_{c+d}(\overline{u\alpha})$$

and $\alpha = g_d(\overline{\alpha}) = \overline{\alpha} \in K$. It follows $u \in K$. Let h be the restriction of f to K. Clearly h is APN. Let $a \in K$. The equations show that $g_d(\alpha)/\alpha = a/g_{3d}(a)$ and also $g_d(\alpha)/\alpha = a/g_{3d}(a)$. By comparison $\alpha \in K$. We conclude that h itself is crooked. It is described by the exponent sets $D' = \{0, d, 2d\}, E' = \{0, d, 2d\} - c \sim D'$. Theorem 2 and [7] show that D' must have cardinality 2.

Let $r = 2s$. Two of the exponents $0, d, 2d$ must be identical mod s. If d is a multiple of s, then $2d = 0 \pmod r$, contradiction. It follows that $2d$ must be a multiple of s. If $d < s$, then $2d = s$ and D is a punctured subgroup, contradiction. The same happens when $s < d < r$. This type is out as well.

In the sequel it can be assumed that $l = |D| = |E| > 3$.

7 An upper bound on incidences

Definition 5. *Let $|D| = |E| = l$. The incidence number $m(D, E)$ is the maximum number i such that there exist different maximal subsets $K_1, \ldots, K_i$ of D and different maximal subsets $L_1, \ldots, L_i$ of E with $K_j \sim L_j$ for all j.*

Clearly $m(D, E) = l$ if $D \sim E$. We assume that D and E are not in the same orbit. What is the maximum $m(D, E)$ then? The following examples show that $m(D, E)$ may be arbitrarily large:

Definition 6. *Let D, E be representatives of different orbits. The orbits form an* **extraspecial pair** *if D, E can be chosen as follows:*

Let T be the stabilizer of a periodic set P consisting of more than one T-orbit, choose $a, b \in P$ from different orbits and

$$D = P \setminus \{b\},\ E = P \setminus \{a\}.$$

They form a **special pair** *if D, E may be chosen as follows: P is a $2t$-periodic set containing the subgroup H of order $2t$, $ord(c) = t, y \in H \setminus \langle c \rangle$ such that $2y \neq c$. Let*

$$D = P \setminus \{-c, y - c\},\ E = P \setminus \{0, y - c\}.$$

As $m(D, E)$ is unchanged when D, E are replaced by elements of the same orbit the incidence number m really is defined on pairs of orbits. If $m \geq 1$ we can choose $D = M \cup \{a\}, E = M \cup \{b\}$. Assume $m \geq 2$. This means there are $x, y \in M$ and some $c \in G$ such that

$$(D \setminus \{x\}) + c = E \setminus \{y\}.$$

Let $t = ord(c)$ and denote by $C_t(u)$ the orbit of u under the subgroup of order t. We will consider this situation, where $l \geq 4$.

Lemma 14. *Consider the intervals of stepwidth c starting at a, y and ending at the first entry different from the starting point which is not contained in $M \setminus \{x\}$. These end points are b, x.*

Proof. Assume at first $x \neq y$. The claim is obvious. By definition of c we have that $a + ic \in (M \setminus \{y\}) \cup b$ as long as $a + (i-1)c \in (M \setminus \{x\}) \cup a$, analogously for y as starting point. It is impossible that this is always satisfied as the orbit would never come to an end. The first time the condition is not satisfied is when one of the endpoints b or x is reached. Case $x = y$ is the special case when one of the intervals is reduced to one point x. □

It follows from the preceding lemma that one of two situations arise. Either there are intervals $I_c(a, b)$ and $I_c(y, x)$ of stepwidth c, the first with starting point a and endpoint b, the second with starting point y and endpoint x, or there are intervals $I_c(a, x)$ and $I_c(y, b)$. All intermediate points of these intervals are in $M \setminus \{x, y\}$. It is also clear that each of those choices leads to sets which satisfy the requirement

$$(D \setminus \{x\}) + c = E \setminus \{y\}.$$

We consider the distribution of the points from $M \cup \{a, b\}$ on the orbits of the group of order t (generated by c). We have that the elements of the basic intervals are on an orbit each. The remaining elements of M come in full orbits. Assume now $m(D, E) \geq 3$. This means there are $u \in M \setminus \{x\}$ and $v \in M \setminus \{y\}$ and there is $c' \in G$ such that

$$(D \setminus \{u\}) + c' = E \setminus \{v\}.$$

In the first case the basic intervals are $I_1 = I_c(a, b)$ and $I_2 = I_c(y, x)$. Let k, k' be the sizes of those intervals. It follows that the distribution of the points of $M \cup \{a, b\}$ on orbits is either $(k + k', t, \dots)$ (if the basic intervals are on the same orbit) or $(k, k', t, \dots)$ (if they are on different orbits). These are cases (1,1) and (1,2), respectively.

Type (1,1)

We have $k + k' < t$ as otherwise D, E are in the same orbit. If u is periodic then also v is and we have the same contradiction as before. We have that $u, v \in C(a)$. The relevant points on $C(a)$ form the union of two intervals of stepwidth c. There are several cases where u, v are positioned. Clearly c' is a multiple of c. In each case c' maps D to E. It follows that in case (1,1) the assumption $m(D, E) > 2$ leads to a contradiction.

Here are the details: let g, g' be the sizes of the gaps between I_1, I_2. In particular $k + g + k' + g' = r$. If $u \in I_1$ the distribution of $D \setminus u$ is $(X, 1, k-X-2, g+1, k', g')$, if $u \in I_2$, then it is $(k-1, g+1, Y, 1, k'-Y-1, g')$. Here each distribution starts with a segment of I_1. Analogously $v \in I_1$ leads to distribution $(Z-1, 1, k-Z-1, g, k', g'+1)$ of $E \setminus v$ and $v \in I_2$ to distribution $(k-1, g, W, 1, k'-W-1, g'+1)$. Here the parameters in capital letters are the lengths of the leading segments in I_1, I_2, respectively. Denote the cases by those capital letters. Consider the case when u is of X-type and v of Z-type. In the first subcase we have $X = Z - 1, \dots, g = g + 1$, an obvious contradiction. In the second subcase $g = g' = 1$ and $k' = Z - 1$, a contradiction. The last subcase implies $g = g' = 0$, hence $k + k' = t$, contradiction. The situation is similar in the remaining three cases.

Type (1,2)

This time I_1, I_2 are in different c-orbits. We have $k' < t$ as otherwise $D \sim E$. If u is in the periodic part, then also v is and c' maps u to v, which implies as usual that $E \sim D$.

Lemma 15. *c' maps $C_t(a)$ to $C_t(y)$ and vise versa.*

Proof. The only other possibility is that c' is a multiple of c. Assume this is the case. We have seen that u is not in the periodic part. Let $u \in C_t(a)$. The same is true of v. It follows that c' maps I_2 into itself, so $c' = 0$, contradiction. Assume $u \in C_t(y)$. Then $C_t(a)$ shows $c' = c$ and we have $u = x, v = y$. $\square$

In particular we can choose notation such that $C(a) \cup C(y)$ is the subgroup of order $2t$. There are now four possibilities where u, v can be situated. If both are in $C_t(a)$, then $D \setminus u$ has distribution $(k-2, k', t, \dots)$ which implies $k' = k-2$. If both are in I_2, then $D \setminus u$ has distribution $(k-1, k'-1, t, \dots)$. This implies $k' = k$. For the two remaining possibilities we have necessarily $k' = k-1$. It follows that $k' \in \{k, k-1, k-2\}$ if there is a third incidence between maximal subsets of D and E.

Also, the cases $k' = k$ and $k' = k-2$ are equivalent, for the following reason: the two incidences we start from have the form

$$(D \setminus a) + 0 = E \setminus b, \ (D \setminus x) + c = E \setminus y.$$

Instead of D, E work with $D, E - c$. Then the roles of c, a, b, x, y are taken by $-c, x, y-c, a, b-c$. The type is still 1 but the basic intervals are changed, of lengths $k'+1, k-1$ instead of k, k'.

Consider case $k' = k-2$ corresponding to $u, v \in I_1$. We have

$$c' : I_1 \setminus \{b, u\} \longrightarrow I_2 \longrightarrow I_1 \setminus \{0, v\}.$$

Assume $k = t$. Then b, u is mapped to a pair of neighbours. They must be neighbours themselves. $u = 0 = a$ is impossible, so $u = b - c = -2c$ is mapped to $y - 2c$. This shows $c' = -y$, which contradicts the second mapping. We have $k < t$. As $I_1 \setminus \{b\}$ is an interval of size $\leq t-3$ and $I_1 \setminus \{b, u\}$ is an interval it follows from Lemma 9 sthat $u = b - c = (k-2)c$. The same argument applies to $I_1 \setminus \{0, v\}$. Assume v is not an endpoint of $I_1 \setminus \{0\}$. Then $|I_1 \setminus 0| = k - 1 \geq t - 2$, so $k = t - 1$. We have

$$c' : \{u = -3c, b = -2c, B = -c\{ \longrightarrow y - \{-3c, -2c, -c\} \longrightarrow \{0, -c, v\}.$$

The first mapping shows $c' = -y$, which contradicts the second mapping. We have $k < t-1$ and $v = c$. Here are the mappings afforded by c' :

$$\{0, \dots, (k-3)c\} \longrightarrow y + \{0, \dots, (k-3)c\} \longrightarrow \{2c, \dots, (k-1)c\}.$$

It follows $c' = y, 2y = 2c$. As $y - c = \omega$ is the involution we have that t is odd, and y generates the group of order $2t$. This is our first exceptional situation: t is odd, $k \leq t-2$,

$$I_1 = \{a = 0, v = c, \ldots, u = (k-2)c, b = (k-1)c\}, I_2 = \{y, \ldots, x = y + (k-3)c\}$$

and $D = (I_1 \setminus b) \cup I_2 \cup P, E = (I_1 \setminus 0) \cup I_2 \cup P$. Here P is a union of cosets of the subgroup of order $2t$ and $2y = 2c$. As u, v are uniquely determined we have $m(D, E) = 3$ in this case.

The last case that remains to be considered is $k' = k - 1$. We have that u, v are in different basic intervals.

Consider the case $k = t$. We have

$$C(0) = I_1 = \{a = 0, c, \ldots, b = (t-1)c = -c\},$$

$$C(y) = \{y, y + c, \ldots, x = y - 2c, A = y - c\},$$

where A is the unique element in $C(y) \setminus I_2$. There are two subcases, either $u \in I_1, v \in I_2$ or vice versa. In the first situation by definition c' maps $I_1 \setminus \{b, u\} \longrightarrow I_2 \setminus \{v\}$ and $I_2 \longrightarrow I_1 \setminus \{a\}$. The second mapping shows $c' = -A$. The first mapping implies that $\{b, u\} + c' = \{v, A\}$. As u is not mapped to v we obtain a unique solution: $u = 2A = 2y - 2c, v = -y$. In the second situation, when $u \in I_2, v \in I_1$ the situation is analogous. We have $c' = y, u = -y, v = A + y = 2y - c$. It follows $m \leq 4$ in this case and we observe that $m = 4$ really happens. Observe that in this exceptional case both D and E have type $(t-1, t-1, t \ldots)$ in their distribution on t-cosets and both arise from a $2t$-periodic set by double puncturing the subgroup of order $2t$. The condition that D, E are not in the same orbit is $2y \neq c$.

We also consider the special case $k = t - 1$. The situation is

$$C(0) = \{c = a, 2c, \ldots, (t-1)c = b, 0\},$$

$$C(y) = \{y, y + c, \ldots, y - 3c, y - 2c, y - c\}$$

where 0 is the element of $C(0)$ outside I_1 and $y - 2c, y - c$ the elements of $C(y) \setminus I_2$.

The first subcase is $u \in I_1, v \in I_2$. We have that c' maps

$$I_1 \setminus \{b, u\} \longrightarrow I_2 \setminus \{v\}, I_2 \longrightarrow I_1 \setminus \{a\}.$$

Taking complements this means

$$c' : \{y - 2c, y - c\} \longrightarrow \{0, c\}, \{0, -c, u\} \longrightarrow \{y - 2c, y - c, v\}.$$

The first arrow shows $c' = -y+2c$. Assume $0 \mapsto y-2c$. Then $\omega = y-2c = c'$ is the involution. We must have $u+\omega = y-c$, equivalently $u = y-c-\omega = c = a$, contradiction. Assume $0 \mapsto y-c$. Equivalently $2y = 3c$. It follows $u+c' = y-2c$, which implies $u = -c = b$, contradiction. The final subcase is $0 \mapsto v$, hence $v = c' = -y+2c$. As $u \neq 0$ we must have $u = -2c$ and $-c+c' = y-c$. It follows $c' = y = -y+2c$. This shows that $y-c$ is the involution and $v = y$, contradiction.

The second subcase is $u \in I_2, v \in I_1$. The same arguments as before show that c' maps

$$c' : \{u, y-2c, y-c\} \longrightarrow \{0, c, v\}, \{0, -c\} \longrightarrow \{y-2c, y-c\}.$$

The second implies $c' = y-c$. Assume $u \mapsto 0$. Then $u = -c' = -y+c$. As $\{y-2c, y-c\} \longrightarrow \{c, v\}$ we get $v = 2c$ and $y-2c+c' = c$. This shows $2y = 4c$ and finally $u = -y+c = y-3c = x$, contradiction. It follows $u \mapsto c$, so $u = -y+2c$. As $\{y-2c, y-c\} \longrightarrow \{0, v\}$ it follows $v = \pm c \in \{a, b\}$, contradiction. We conclude that $m \leq 4$ if $k = t$ and $m \leq 2$ if $k = t-1$.

We are still in case $k' = k-1$ and we can assume $k' \leq t-3$. Let at first $u \in I_1, v \in I_2$. We have

$$c' : I_1 \setminus \{b, u\} \longrightarrow I_2 \setminus \{v\}, I_2 \longrightarrow I_1 \setminus \{a\}.$$

Assume $u \neq b-c$ (not an endpoint of $I_1 \setminus \{b\}$. If u is the only point complementing $I_1 \setminus \{b, u\}$ to an interval, then $c' : u \mapsto v$ and $D \sim E$, contradiction. This situation is studied in Lemma 10. As we know already that $k-1 \leq t-3$ this leaves only the exceptional situations in cases $t = 8$ and $t = 10$ of Lemma 10. Let at first

$$t = 8, I_1 = \{a = 0, c, 2c, 3c, 4c\}, I_2 = \{y, y+c, y+2c, x = y+3c\}.$$

Assume $u = 2c$. We have $c' \in I_2$. Necessarily $c' = y$. We see $v = y+2c$. As $I_2 + y = 2y + \{0, c, 2c, 3c\} = \{c, 2c, 3c, 4c\}$ it follows $2y = c$, which implies the contradiction $D \sim E$. The same holds when $u = c$. Let now

$$t = 10, I_1 = \{a = 0, c, 2c, 3c, 4c.5c = b\{, I_2 = \{y, y+c, y+2c, y+3c, y+4c = x\}.$$

We also have $u = 2c$. As before the image of $I_1 \setminus \{b, u\}$ shows $c' = y, v = y+2c$ and the image of I_2 then shows $2y = c$, which implies $D + y = E$, contradiction. We have shown $u = b-c$ if $u \in I_1$. Let

$$I_1 = \{a = 0, c, \ldots, u = (k-2)c, b = (k-1)c\}, I_2 = y + \{0, \ldots, (k-2)c\}.$$

As $I_1 \setminus \{b,u\}$ is an interval we have that $I_2 \setminus \{v\}$ is an interval. By Lemma 9 v cannot be in the open part of I_2, so $v = x = y + (k-2)c$. The image of $I_1 \setminus \{b,u\}$ shows $c' = y$, and the image of I_2 shows $2y = c$, which implies $D \sim E$ as before.

We have shown $u \notin I_1$. The case $u \in I_2, v \in I_1$ is symmetric to the one considered, which is seen replacing D by $D + c$.

Type (2,1)

Type 2 occurs when the c-interval starting at a ends at x and the interval starting at y ends at b. Consider those intervals $I_1 = I_c(a,x)$ of length k and $I_2 = I_c(y,b)$ of length k'. Type $(2,1)$ means that those basic intervals are in the same c-orbit. It follows that $D \cup E$ has distribution $(k+k', t, \dots)$. We have $k+k' < t$ as otherwise $D \sim E$. With the usual notation (u,v,c') we have that u cannot be in the periodic part as v would have to be there too and c' would map u to v. There are four cases relative to the positioning of u,v. Let g,g' be the sizes of the gaps between I_1 and I_2 on $C_t(a)$, so $k+k'+g+g' = t$. If $u \in I_1$, then $D \setminus u$ has type $(X,1,k-X-1,g,k'-1,g'+1)$. If $u \in I_2$, then $D \setminus u$ has type $(k,g,Y,1,k'-Y-2,g'+1)$. The type of $E \setminus v$ is $(Z-1,1,k-Z-1,g,k',g'+1)$ if $v \in I_1$, it is $(k-1,g,W,1,k'-W-1,g'+1)$ in the remaining case. There are four possible combinations, each with 3 subcases.

Combination (X,Z) leads in the first subcase to $X = Z-1 = Z$, contradiction, in the second to $k' = Z$, contradiction. The third case is more interesting: $X = k', g' = 0, g = 1, Z = k-k'$. This is a third incidence and it is uniquely determined. Take a closer look at this exceptional situation:

$$C(0) = \{a = 0, .., x = (k-1)c, L = kc, y = (k+1)c, .., b = -c\}$$

and $u = k'c, v = (k-k')c, c' = -k'c$. Both D,E have type $(t-2, t \dots)$ Their complements are $\{-c, kc\}$ and $\{0, kc\}$, respectively. They are in the same orbit if and only if $(2k+1)c = 0$ which is impossible.

Combination (X,W) leads in the first subcase to $X = k-1, g = 1, W = k-X-1 = 0$, which is the known incidence arising from $v = y$. The third subcase $X = k'-W-1$ leads to $u = a$, another known incidence. The second subcase has $X = W$. It follows $u + c' = v$ and D,E are in the same orbit.

Combination (Y,Z) leads to $k = Z-1, g = 1, Y = k-Z-1 < 0$ in the first subcase, to $k = k-Z-1$ in the second subcase. The third subcase has $k = k', g = g' + 1, Y = Z - 1$. Once again u is mapped to v. Finally there is combination (Y, W). The first subcase is $k = k - 1$. In the second subcase we have $g' = 0, g = 1, W = k, Y = k' - k - 1$. The third subcase is similar: $g' = 0, g = 1, Y = k - 1, W = k' - k - 1$. We conclude that in all cases $m(D, E) \leq 3$.

Type (2,2)

I_1 and I_2 are on different c-orbits, lengths k and k'. It follows that $D \cup E$ has distribution $(k, k', t \dots)$, the distributions of D, E are respectively $(k, k' - 1, t, \dots)$ and $(k - 1, k', t, \dots)$.

Assume $u, v \in C_t(a) \cup C_t(b)$. Obviously there are four subcases. A limitation is obtained by comparing the distributions as usual. When $u, v \in C_t(a)$ we have $\{k - 1, k' - 1\} = \{k - 2, k'\}$ hence $k' = k - 1$. We must have

$$c' : C_t(a) \leftrightarrow C_t(b)$$

and more precisely

$$c' : I_1 \setminus u \mapsto I_2, I_2 \setminus b \mapsto I_1 \setminus \{a, v\}$$

where u is different from a, x. We can choose $a = 0$ and $C(a) \cup C(b)$ as the subgroup of order $2t$. Also c' shows that the periodic set $D \cup E$ has the group of order $2t$ in its stabilizer. This shows $k < t$ as in case $k = t$ we would have $D \sim E$. As $I_1 \setminus u$ must be an interval and u is different from $0, x$ it follows from Lemma 9 that $k \geq t - 2$. We know already $k < t$. In case $k = t - 1$ we would have $\{u, -c\} + c' = \{y - 2c, y - c\}$. This forces the contradiction $u \in \{0, -2c\} = \{a, x\}$. In case $k = t - 2$ a similar contradiction is obtained.

The second case is when $u \in I_1, v \in I_2$. The distribution of $D \setminus u$ and of $E \setminus v$ is $(k-1, k'-1, t, \dots)$ Assume $k \neq k'$. Then c' is a multiple of c. It maps $I_1 \setminus u$ to $I_1 \setminus a$, which is not possible. We have $k = k'$ and $c' : C_t(a) \leftrightarrow C_t(b)$. In particular c' maps $I_1 \setminus u \mapsto I_2 \setminus v$ and $I_2 \setminus b \mapsto I_1 \setminus a$. We have that $r \geq 8$ is even. The generic case that u is the unique element completing $I_1 \setminus u$ to an interval is not possible as in that case u would be mapped to v. The same would happen if $k = t$. We have $k = k' < t$. Lemma 10 shows that either $k \geq t - 2$ or we are in the special cases for $t = 8, t = 10$. Assume $k = t - 2$. Considering complements and using the standard terminology (in particular $a = 0$) we have that

$$c' : \{u, -2c, -c\} \longrightarrow \{v, y - 2c, y - c\}.$$

As $u \neq 0, -3c = x$ we have that $c' : u \mapsto v$, contradiction. In the same way the exceptional cases $t = 8, t = 10$ lead to contradictions. Consider $t = 8$. We have

$$I_1 = \{a = 0, c, 2c, x = 3c\}, I_2 = \{y, y + c, y + 2c, b = y + 3c\}.$$

We have $u \in \{c, 2c\}, v \in \{y + c, y + 2c\}$. Assume $u = c, v = y + c$. The two elements complementing $I_1 \setminus c$ to an interval are $c, 5c$, analogously for $I_2 \setminus \{y + c\}$. We must have $c' : u \mapsto y + 5c, c' = y + 4c = y - 4c$. This is impossible as $x + c' \notin I_2$. All cases lead to similar contradictions, both for $t = 8$ and $t = 10$. Only case $k = t - 1$ survives. We have

$$C(a) = \{a = 0, c, \dots, x = -2c, A = -c\{, C(b) = \{y, \dots, b = y-2c, B = y-c\}.$$

We have

$$c' : u \mapsto B, A \mapsto v, B \mapsto a = 0.$$

This implies $c' = -B = -y + c, v = -y, u = 2(y - c)$. In particular those elements are uniquely determined in the present subcase. Observe also that for type reasons the choice $u \in I_2, v \in I_1$ is not possible in this subcase. The two remaining subcases for $u, v \in C(a) \cup C(b)$ are symmetric to the cases we just discussed. We have that a third incidence with $u, v \in C(a) \cup C(b)$ is possible only in one subcase corresponding to D of type $(t - 1, t - 2, t, \dots)$ and E of type $(t - 2, t - 1, t \dots)$, where the t-periodic hull of $D \cup E$ is the subgroup of order $2t$.

Assume u, v are both in the periodic part. Then $\{k, k' - 1\} = \{k - 1, k'\}$ and consequently $k = k'$. If $k < t-1$, then necessarily c' maps u to v and D, E are in the same orbit. Assume $k = t - 1$. In order to avoid the contradiction above we must have $c' : C(u) \longrightarrow C(b) \longrightarrow C(a) \longrightarrow C(v)$. Write

$$C(a) = \{a = 0, \dots, x = (t-2)c, A = -c\}, C(b) = \{y, \dots, b = y+(t-2)c, B = y-c\}.$$

We have that c' maps

$$u \mapsto B, \{b, B\} \longrightarrow \{a, A\}, A \mapsto v.$$

Assume $c' : B \mapsto A$. Then $c' = -y$ maps $b \mapsto x$, contradiction. It follows $c' : B \mapsto a, c' = -B = -y + c$. We have $u = 2(y - c), v = -y$. Observe that y is contained in the stabilizer of the t-periodic hull of $D \cup E$. The values of u, v are uniquely determined and yield a third incidence. Also, the value

$v = -y$ shows that the t-periodic hull of $D \cup E$ is not the subgroup of order $2t$. It follows that this case is different from the one considered above.

Let $k = k' = t$. In particular D, E are obtained by puncturing a t-periodic set, and c' maps $C_t(u) \mapsto C_t(a), C_t(b) \mapsto C_t(v)$. Let

$$C(a) = \{a = 0, c, \ldots, x = -c\}, C(b) = \{y, \ldots, y - c = b\}.$$

As $c' : u \mapsto 0$ we have $c' = -u$ and $b - u = v$. The stabilizer of the periodic set $P = D \cup E$ contains u as well. We see that in this case $m(D, E)$ may be arbitrarily large: start from a periodic set P whose stabilizer T has more than one orbit on P. Let $a = 0 \in T, b \notin T$. Then $D = P \setminus \{b\}$ and $E = P \setminus \{0\}$ are in different orbits. Let $0 \neq u \in P$ and $v \in E$ such that $P \setminus \{b, u\} \sim P \setminus \{0, v\}$. Necessarily then $c' : b \mapsto v, u \mapsto 0$, hence $c' = -u \in T, v = b - u$. Each such choice of $u \in T$ yields such an incidence. However, unless $u = -u$ is the involution the corresponding maximal subset $D \setminus \{u\}$ is not the unique representative of its orbit as a subset of D, a second representative being $D \setminus \{-u\}$.

Assume now u is in the periodic part but v is not. Comparing the types of $D \setminus u$ and $E \setminus v$ we see that necessarily $k = t$ and $\{k' - 1, t - 1\}$ is obtained by taking 1 off from one of the parts of $\{k - 1, k'\}$.

Assume $v \in C_t(b)$. We have $k = t$ and at this point k' is unrestricted. The distributions of $D \setminus u$ and $E \setminus v$ are $(t, k'-1, t-1, t \ldots)$ and $(t-1, k'-1, t \ldots)$. Assume $k' < t$. Then c' maps $C_t(b)$ to itself, so c' is a multiple of c, which on the other hand is not the case. We have $k' = t$ and

$$c' : C_t(u) \mapsto C_t(b) \mapsto C_t(a).$$

However this implies that u is mapped to v, contradiction.

The last case is $v \in C_t(a)$. It follows $k' = t-1$. We have $k = t, k' = t-1, u$ in the periodic part, $v \in C_t(a)$. The distributions of D, E are different, so they canot be in the same orbit. The distributions of $D \setminus u$ and $E \setminus v$ are $(t, t-2, t-1, \ldots)$ and $(t-2, t-1, t, \ldots)$. It follows that $c' : C_t(u) \mapsto C_t(b) \mapsto C_t(a)$. This shows $u \in 2y + \langle c \rangle$. We have

$$C_t(a) = \{a = 0, c, \ldots, -c = x\}, C(b) = \{y, y + c, \ldots, y - 2c = b, y - c = B\},$$

where B is the element of $C_t(b)$ not in $D \cup E$. We have $c' : u \mapsto B$, hence $c' = y - c - u$ and $c' : \{B, b\} \mapsto \{0, v\}$. As B, b are neighbours on $C_t(b)$ it follows that v is a neighbour of 0 on $C_t(a)$, so $v = \pm c$. Let P be the t-periodic hull of $D \cup E$. Then the complements of D, E in P are $\overline{D} = y-2c, y-c\}, \overline{E} = \{0, y-c\}$. Also y is in the stabilizer of P, so this stabilizer has order Consider the choice $v_1 = c$. Then $c_1' = -b = 2c-y = y-c-u$, so $u_1 = 2y-3c$. Replacing the pair (x, y) by (u, v) we see that we land in type 1, which has already been considered. The remaining possibility is $v_2 = -c, u_2 = 2(y-c), c_2' = -y+c$. We need not consider this subcase as it is equivalent to one of type 1.

By collecting the results a classification of all pairs of orbits with more than two incidences may be obtained. For the purposes of the proof of the main theorem the following is sufficient:

Corollary 1. *Let D, E be of same cardinality $l \geq 4$ and from different orbits. If $m = m(D, E) > 3$, then the pair of orbits is either extraspecial or special in the sense of Definition 6. It is extraspecial if $m > 4$.*

8 Completion of the proof

The extraspecial case

Assume we are in the extraspecial case of Definition 6: P is a set whose stabilizer H has order t and P consists of more than one coset of H. The sets D, E are obtained by puncturing P at elements from different cosets of $H : D = P \setminus a, E = P \setminus b$, where $a \in H, b \notin H$. Assume P contains a third coset C. Let $x \in C$. Then $P \setminus \{a, x\}$ must be in the same orbit as $P \setminus \{b, y\}$ for some y. However, P is the t-hull of both sets, so elements achieving the translation must be in H. It cannot map a to b or to y, contradiction. We have $P = H \cup (b + H)$. Let $a = 0$. Then

$$D = P \setminus 0,\ E = (P \setminus b) - c.$$

Consider $M = P \setminus 0, h \subset D$. We have $M - h \subset D$ and there is no further representative of this orbit in D or E. If $h \neq -h$, then these are different and they are in a long orbit. The fact that $\beta_a(M) = 0$ is equivalent with $\alpha g_h(a) = g_h(\alpha)a$ for all a, equivalently $g_h(\alpha/a) = \alpha/a$ for all $a \neq 0$ and $h \in H$ such that h is different from 0 and from the involution. Choosing h to be a generator of H we see that $\alpha/a \in K = Fix(H)$. Let $r = st$. Then $K = \mathbb{F}_{2^s}$.

Choose now $N = P \setminus \{0, b+h\} \subset D$. It is in a long orbit. Its partner in E is $N - h - c = (P \setminus \{-h, b\}) - c$. The condition $\beta_a(N) = 0$ reads

$$\alpha g_{b+h}(a) = g_{h+c}(u\alpha)a.$$

Choosing $a \in K$ we know $\alpha \in K$ and conclude $u \in K$. Also, isolating α/a on one side we see $g_c(u\alpha)/g_b(a) \in K$, equivalently $g_{b-c}(a)/a \in K$. We claim that this forces $b = c$. In fact, assume $g_i(a)/a \in K$ for all a. As we can replace i by $-i$ it can be assumed $0 \leq i \leq r/2$. Raising to power $q-1$, where $q = 2^s$, shows that $2^r - 1 = q^t - 1$ divides $(q-1)(2^i - 1)$, which yields the contradiction $t < 2$. We have $b = c$ and the situation is the following:

$$D = P \setminus 0, \;\; E = (P - b) \setminus 0.$$

Consider now the second to maximal subset $S = P \setminus \{0, b, b+h\}$ for some $h \neq 0$. It is in a long orbit and has two partners as subsets of $E : S - b = (P - b) \setminus \{0, h, -b\}$ and $S - b - h = (P - b) \setminus \{0, -h, -b - h\}$. Let $a = 1$. The condition $\beta_1(S) = 0$ reads

$$\alpha = g_b(u\alpha) + g_{b+h}(u\alpha) = 0,$$

contradiction.

The special case

D, E arise from a $2t$-periodic set P by double puncturing the subgroup of order $2t$:

$$C(0) = \{a = 0, c, \dots, b = -c\},$$
$$C(y) = \{y, y + c, \dots, x = y - 2c, A = y - c\},$$
$$u_1 = 2y - 2c, v_1 = -y, c_1' = -y + c, u_2 = -y, v_2 = 2y - c, c_2' = y.$$

Here $C(0) \cup C(y) = T$ is the subgroup of order $2t$ and $2y \neq c$ as D, E are not in the same orbit. This shows that $t > 2$ as in case $t = 2$ we would have $2y = c$. Also we must have that a, x, u_1, u_2 are pairwise different, likewise b, y, v_1, v_2. The conditions are $2y \notin \{0, c, 2c\}$. We claim that D and E have type $\mathcal{D}$. In fact, the distribution on cosets of the subgroups of order $2t$ and t shows that D, E do not contain a maximal subset in a short orbit. Let $D \setminus e \sim D \setminus f$. One of e, f must be in $C(0)$, the other in $C(y)$. Choose notation such that $e \in C(0)$. Considering complements we have $\{b, A, e\} + s = \{b, A, f\}$. If $s \in C(0)$, then $b + s = b$, hence $s = 0$, contradiction. It follows that $s : C(0) \leftrightarrow C(y)$. We must have $A + s = b$. As $b + s = A$ is impossible (or D would be in a short orbit), we have $b + s = f, e + s = A$. In coordinates: $s = -y, e = 2y - c, f = -y - c$. As indeed $e, f \in D$ we see that $i(D) = l - 2$. The same argument holds for the other set: $i(E) = l - 2$. As $4 = m(D, E) \geq i(D) = l - 2$ we have $l \leq 6$. Assume P is larger than the subgroup of order $2t$. Then $l \geq 4t - 2$. As $l \leq 6$ this shows $t = 2$, contradiction. We have $l = 2t - 2$. It follows $t \in \{3, 4\}$. $t = 3$ is impossible as the condition $2y \notin \{0, c, 2c\}$ cannot be satisfied. We have $t = 4$. In this case $2y = -c$ is the only choice. This entails $-y = y + c = A \notin E$. As $v_1 = -y$ this is impossible.

Continuing with case $m \leq 3$

We have shown $m(D, E) \leq 3$. This implies that both $i(D)$ and $i(E)$ are bounded by 3. Recall that we know already that D, E have the same type and that $l \geq 4$. The type cannot be $\mathcal{A}$.

If the type is $\mathcal{B}$, then $l = 4$ and $m(D, E) = 3$. We can choose both D and E to contain the subgroup T of order 3. This gives us a fourth incidence: $m(D, E) = 4$, contradiction.

Assume the type is $\mathcal{D}$. As $i(D) = l - 2 \leq m(D, E) \leq 3$ we have $l \leq 5$. We know from Lemma 5 that there is a subgroup of some order t such that D is the union of a t-periodic part P and an interval I of stepwidth of order t. Here I is not a complete coset (as D is in a long orbit) and I has more than one point as D does not contain a maximal subset in a short orbit. These conditions show $t \geq 3$. If $t = 3$, then $l = 5$ and D is the puncturing of a 3-periodic set, which we count as type $\mathcal{E}$. As $t \geq 4$ the periodic part is absent. It follows that both D, E are intervals. Obviously the stepwidth of D and of E are multiples of one another. It follows that they both generate the same subgroup. We can choose D, E to be intervals contained in the subgroup of order t, where $t \geq l + 2$.

Consider at first $l = 4$:

$$D = \{0, c, 2c, 3c\}, E = \{0, d, 2d, 3d\}.$$

As $D \setminus c$ is in the same orbit as either $E \setminus d$ or $E \setminus 2d$ it follows, by considering differences, that $\pm\{c, 2c, 3c\} = \pm\{d, 2d, 3d\}$. We can also replace d by $-d$. In case $d = c$ clearly $E \sim D$. It follows that we can choose $d \in \{2c, 3c\}$. Assume $d = 2c$. Then $t \geq 7$ odd. The only choice is $t = 7$. We have

$$D = \{0, c, 2c, 3c\}, E = \{0, 2c, 4c, -c\}.$$

The required incidences are

$$(D \setminus 2c) - c = E \setminus (4c),\ (D \setminus c) - 3c = E \setminus 2c.$$

This case survives at this stage. Let $d = 3c$. Then $\pm\{c, 2c\} = \pm\{6c, 9c\}$. Case $t = 7$ leads to

$$D = \{0, c, 2c, 3c\}, E = \{0, 3c, -c, 2c\}.$$

They intersect in a maximal subset and the second incidence is $\{0, c, 3c\} - c = \{0, -c, 2c\}$. This is the second survivor. The remaining case is $t = 8$. It leads to

$$D = \{0, c, 2c, 3c\}, E = \{0, 3c, 6c, c\}.$$

Again they intersect in a maximal subset, and $\{0, 2c, 3c\} + 6c = \{0, 6c, c\}$. This is the third survivor.

Let $l = 5$.

$$D = \{0, c, 2c, 3c, 4c\}, E = \{0, d, 2d, 3d, 4d\}.$$

As $D \setminus c$ is in the same orbit as a maximal subset of E it cannot be that c is the only point completing $D \setminus c$ to an interval. The same is true of $D \setminus 2c$ and $D \setminus 3c$. As usual Lemma 10 yields a contradiction.

Assume D and E have type $\mathcal{C}$. As $i(D) = 2mg$ the periodic part must be absent: $m = 0$. It follows that both D and E are puncturings of the subgroup of (even) order $2g$. This shows that they are in the same orbit.

The final case is when D, E are of type $\mathcal{E}$. As $i(D) = mt \leq 3$ it follows that $m \leq 1$. It cannot be that $m = 0$ for both D and E as in this case we would have $D \sim E$. Assume $m = 0$ for D. Then D is the puncturing of a subgroup of odd order $l + 1$. In particular l is even. As $m = 1$ in the case of E we have that l is odd, contradiction. It follows $m = 1, t = 3$ for both D and E. Both sets are puncturings of a union of two cosets of the subgroup of order 3. Let $H = \{0, \alpha, 2\alpha = -\alpha\}$ be this subgroup and

$$D = H \cup \{y, y + \alpha\},\ E = H \cup \{z, z + \alpha\}.$$

Puncturings with respect to elements of H have a different distribution type on cosets as the others. It follows that $D \setminus 0, D \setminus \alpha, D \setminus 2\alpha$ must be in the same orbits as the $E \setminus 0, E \setminus \alpha, E \setminus 2\alpha$, in some order. It follows $z \in -y + H$. In particular $y + H \neq -y + H$ as otherwise $D \sim E$. Replacing D by a shift such that $D \cap E$ has size 4 we arrive at the following situation: $P = D \cup E = H \cup (y + H)$ where $-y \notin y + H$ and

$$D = P \setminus 0,\ E = P \setminus y.$$

In particular P is not a subgroup. We recognize a special case of the situation excludes in the first section.

Only the three surviving cases for $l = 4$ remain to be considered. Here is the first of those cases, with fresh notation: $r = 7s, ord(d) = 7, K = \mathbb{F}_q$, where $q = 2^s$ and

$$D = \{0, d, 2d, 3d\},\ E = \{0, 2d, 4d, 6d\} - c.$$

Let $A_1 = \{0, 2d, 3d \subset D$ with partner $A_1 - 3d - c = \{0, 4d, 6d\} - c \subset E$. The corresponding condition A_1 is

$$\alpha g_d(a) = g_{3d+c}(u\alpha) g_{5d}(a).$$

Similarly $A_2 = \{0, d, 3d \subset$ with $A_2 - d - c = \{0, 2d, 6d\} - c \subset E$ yields equation A_2

$$\alpha g_{2d}(a) = g_{d+c}(u\alpha) g_{5d}(a).$$

Subset $A_3 = \{d, 2d, 3d\}$ with $A_3 - d \subset D$ yields condition A_3 :

$$\alpha a = g_d(\alpha) g_{4d}(a)$$

and finally $A_4 = \{2d, 4d, 6d\} - c$ with its partner $A_4 - 2d$ yields

$$u\alpha g_{-c}(a) = g_{2d}(u\alpha) g_{d-c}(a).$$

Choose $a \in K$. Then A_3 shows $\alpha \in K$ and one of the first conditions yields $u \in K$. The only remaining condition for the choice $a \in K$ is $\alpha = g_c(u\alpha)$. Consider the subset $V = \{0, 3d \subset D$. Its partners are $V - 3d - c$ and $V - d - c$, both in E. The corresponding condition for $a = 1$ is $\alpha = g_{3d+c}(u\alpha) + g_{d+c}(u\alpha) = 0$, contradiction.

The second survivor has, with the same notation for the fields as before,

$$D = \{0, d, 2d, 3d\},\ E = \{0, 3d, 6d, 2d\} - c.$$

The same arguments using maximal subsets as before show that for $a \in K$ we have $\alpha \in K$, and as a consequence $u \in K$. Not let $S = \{0, 2d\}$. We have $\beta_1(S) = 0$. The different representatives of the orbit of S in our subsets are $S \subset D, S + d \subset D, S - c \subset E$. It follows $g_c(u\alpha) = \alpha + g_{-d}(\alpha) = 0$. The very last exceptional case has $t = ord(d) = 8, r = 8s$ and

$$D = \{0, d, 2d, 3d\},\ E = \{0, 3d, 6d, d\} - c.$$

The usual arguments show that for $a \in L = \mathbb{F}_{q^4}$ we have $\alpha \in K = \mathbb{F}_q$, from which it follows that $u \in K$. Consider the restriction h of f to L. It is

$$h(x) = N(x) + ug(N(x)).$$

Here the norm $N(x)$ is described by exponents $\{0, d, 2d, 3d\}$ and $g(x) = g_{-c}(x)$. This restriction must be crooked, which is not the case because of Theorem 2.

References

[1] J. Bierbrauer: *Introduction to Coding Theory,* Chapman and Hall, CRC Press 2004.

[2] A. E. Brouwer and L. Tolhuizen: *A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters, Designs, Codes and Cryptography* **3** (1993), 95-98.

[3] L. Budaghyan, C. Carlet, P. Felke, G. Leander: *An infinite class of quadratic APN functions which are not equivalent to power mappings,* manuscript.

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

[5] E.R. van Dam and D. Fon-Der-Flaass: *Codes, graphs, and schemes from nonlinear functions,* *European Journal of Combinatorics* **24** (2003), 85-98.

[6] Y. Edel, G. Kyureghyan and A. Pott: *A new APN function which is not equivalent to a power mapping,* manuscript.

[7] G. M. Kyureghyan: *Crooked maps in* $\mathbb{F}_{2^n}$, *Finite Fields and Their Applications,* in press.