Available online at www.sciencedirect.com
SCIENCE DIRECT®
European Journal of Combinatorics 25 (2004) 1123–1133
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Addendum

Addendum to James Singer's theorem on difference sets

Barbu C. Kestenband

Department of Mathematics, New York Institute of Technology, Old Westbury, NY 11568, USA

Received 9 September 2002; accepted 23 October 2003

Available online 12 April 2004

Abstract

If a Singer difference set over a field of square order q^{2n} is partitioned into $q+1$ subsets such that the numbers in each subset belong to a different residue class modulo $q+1$, then q of the subsets are equicardinal, while one subset has a different cardinality.

Let $D = \{d_1, d_2, \ldots, d_k\}$ be a set of integers modulo v such that every $a \not\equiv 0 \bmod v$ can be expressed in exactly λ ways in the form $d_i - d_j \equiv a \bmod v$. Then D is a (v, k, λ)-*difference set*.

Consider the finite field $GF(q^m)$, q a prime power. Let w be a primitive root of this field. Then $GF(q^m)$ can be regarded as an m-dimensional vector space V over the $GF(q)$ subfield. Let an $(m-1)$-dimensional subspace of V comprise, besides 0, the vectors $w^{j_r}, r = 1, 2, \ldots, (q^{m-1}-1)/(q-1)$, where w^{j_r} and $cw^{j_r}, c \in GF(q)\backslash\{0\}$, are considered identical.

Note that for m even, the elements of the $GF(q)$ subfield are $(q+1)$th powers.

We state Singer's theorem [3] as follows, where Part (b) is the object of the present article:

Theorem. (a) *The exponents j_r form a cyclic (v, k, λ)-difference set D with:*

$$v = (q^m - 1)/(q-1),\ k = (q^{m-1} - 1)/(q-1),\ \lambda = (q^{m-2} - 1)/(q-1).$$

(b) *Assume m is even and let $m = 2n, n > 1$.*

E-mail address: bkestenb@iris.nyit.edu (B.C. Kestenband).

0195-6698/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2003.10.014

Then, if the difference set $D = \{j_r : r = 1, 2, \ldots, (q^{2n-1} - 1)/(q - 1)\}$ *is partitioned into* $q + 1$ *subsets* $D_0, D_1, \ldots, D_q$ *such that for all* i, $j_r \in D_i \Leftrightarrow j_r \equiv i \bmod q + 1$, *we have:*

$$|D_i| = \begin{cases} (q^{2n-1} + q^{n+1} - q^n - 1)/(q^2 - 1) \text{ if } 2 \nmid n \\ (q^{2n-1} - q^{n+1} + q^n - 1)/(q^2 - 1) \text{ if } 2 \mid n \end{cases} \text{ for one value of } i$$

$$|D_i| = \begin{cases} (q^{2n-1} - q^n + q^{n-1} - 1)/(q^2 - 1) \text{ if } 2 \nmid n \\ (q^{2n-1} + q^n - q^{n-1} - 1)/(q^2 - 1) \text{ if } 2 \mid n \end{cases} \text{ for } q \text{ values of } i.$$

Some preliminary work is required before we can proceed to the actual proof.

In $GF(q^m)$, consider the polynomial

$$\Xi(x) = x^{q^{m-1}} + x^{q^{m-2}} + \cdots + x^q + x.$$

Note that:

Ξ is an additive function;
$\Xi(c) \in GF(q)$ for every $c \in GF(q^m)$;
$\Xi(tc) = t \cdot \Xi(c)$ for $t \in GF(q)$.

It was shown in [2, Theorem 15(iii)] that the zeros of Ξ make up an $(m-1)$-dimensional vector space over $GF(q)$, where zeros which differ by a factor $c \in GF(q)\backslash\{0\}$ are identified. As such, we shall adopt the view that Singer's theorem concerns the exponents j_r of the primitive root w in the set of nonvanishing zeros of Ξ. Specifically, the difference set D will be regarded as the set of exponents of w in the set of nonvanishing zeros of Ξ, where, again, no distinction is made between w^{j_r} and cw^{j_r}, $c \in GF(q)\backslash\{0\}$.

We shall be concerned exclusively with finite fields $GF(q^{2n})$ and w will stand for a primitive root of such a field. Nothing similar takes place in fields of nonsquare orders.

The proof of Part (b) of the theorem depends upon the parity of n, and, if n is even, upon the parity of q as well.

Proposition 1 constitutes the proof for the case in which n is odd, i.e. $m \equiv 2 \bmod 4$—see the paragraph immediately following the proof of the proposition. The proof for the case $2 \mid n$, i.e. $4 \mid m$, is the object of Proposition 6.

Proposition 1 is valid for all prime powers, but there are slight differences in the proof between the cases in which q is odd or even. We shall make the following convention regarding the proof: whenever a sentence is followed by a similar sentence enclosed in brackets, the former is valid for q odd, while the latter holds for q even. Everything else is valid regardless of the parity of q.

Proposition 1. *Consider the finite field* $GF(q^{2n})$, n *odd, and the* $q^{2n-1} - 1$ *exponents of* w *in the set of nonvanishing zeros of* $\Xi(x) = x^{q^{2n-1}} + x^{q^{2n-2}} + \cdots + x^q + x$.

(i) *If* q *is odd, there are* $(q^{2n-1} + q^{n+1} - q^n - 1)/(q + 1)$ *exponents that are congruent to* $\frac{1}{2}(q + 1)$ *modulo* $q + 1$.

Then, for each $i \in \{0, 1, \ldots, \frac{1}{2}(q - 1), \frac{1}{2}(q + 3), \ldots, q\}$, *there are* $(q^n + 1)(q^{n-1} - 1)/(q + 1)$ *exponents that are congruent to* i *modulo* $q + 1$.

(ii) *If* q *is even, there are* $(q^{2n-1} + q^{n+1} - q^n - 1)/(q + 1)$ *exponents that are multiples of* $q + 1$.

Then, for each $i \in \{1, 2, \ldots, q\}$, there are $(q^n + 1)(q^{n-1} - 1)/(q + 1)$ exponents that are congruent to i modulo $q + 1$.

Proof. We have $\Xi(x) = 0 \Leftrightarrow x^{q^n} + x = b$, where b is a zero of the polynomial $\Theta(x) = x^{q^{n-1}} + x^{q^{n-2}} + \cdots + x^q + x$.

As Ξ possesses q^{2n-1} distinct zeros [2, Theorem 15(i)], Θ cannot have fewer than q^{n-1} distinct zeros, nor can the equation $x^{q^n} + x = b$ with $\Theta(b) = 0$ have fewer than q^n distinct roots.

Thus, in order to find the zeros of Ξ, one has to solve q^{n-1} equations $x^{q^n} + x = b$ with b as above.

For $b = 0$ we have $x^{q^n} + x = 0$. The solutions of this equation are 0 and $w^{(i+\frac{1}{2})(q^n+1)}$, $i = 0, 1, \ldots, q^n - 2$ [the solutions of this equation are 0 and $w^{i(q^n+1)}$, $i = 0, 1, \ldots, q^n - 2$]. Note that n being odd, the exponents of w in the preceding sentence are congruent to $\frac{1}{2}(q+1)$ modulo $q+1$ [note that n being odd, the exponents of w in the preceding sentence are multiples of $q + 1$].

Let now a be a solution of the equation $x^{q^n} + x = b \neq 0$. Since $[w^{(q^n+1)j}]^{q^n} = w^{(q^n+1)j}$ for any j, we see that $aw^{(q^n+1)j}$ is a solution of the equation $x^{q^n} + x = bw^{(q^n+1)j}$. What this shows is that no two exponents of w in the solutions of the equation $x^{q^n} + x = b \neq 0$ can differ by a multiple of $q^n + 1$.

Hence, the q^n exponents of w in the solution set of the above equation are that many different residues modulo $q^n + 1$. So one residue is missing. The missing residue is $\frac{1}{2}(q^n + 1)$, because $w^{(i+\frac{1}{2})(q^n+1)}$ is a zero of $x^{q^n} + x$ for any integer i, as shown earlier in the proof [the missing residue is 0, i.e. $q^n + 1$, because $w^{i(q^n+1)}$ is a zero of $x^{q^n} + x$ for any i].

The set $\{0, 1, \ldots, q^n\}$ contains $(q^n + 1)/(q + 1)$ numbers congruent to each of the numbers $0, 1, \ldots, q$ modulo $q + 1$. If $\frac{1}{2}(q^n + 1)$ is removed from the set, one is evidently left with $(q^n - q)/(q + 1)$ numbers congruent to $\frac{1}{2}(q + 1)$ modulo $q + 1$ [if 0 is removed from the set, one is left with $(q^n - q)/(q + 1)$ numbers divisible by $q + 1$].

As there are altogether $q^{n-1} - 1$ nonzero b's, we end up with a total of $q^n - 1 + [(q^n - q)/(q + 1)](q^{n-1} - 1)$ exponents that are congruent to $\frac{1}{2}(q + 1)$ modulo $q + 1$ and $[(q^n + 1)/(q + 1)](q^{n-1} - 1)$ exponents congruent to each of the numbers $0, 1, \ldots, \frac{1}{2}(q-1), \frac{1}{2}(q+3), \ldots, q$, modulo $q+1$ [as there are altogether $q^{n-1} - 1$ nonzero b's, we end up with a total of $q^n - 1 + [(q^n - q)/(q + 1)](q^{n-1} - 1)$ exponents that are multiples of $q + 1$ and $[(q^n + 1)/(q + 1)](q^{n-1} - 1)$ exponents congruent to each of the numbers $1, 2, \ldots, q$, modulo $q + 1$]. □

Since w^{j_r} and cw^{j_r}, $c \in GF(q)\backslash\{0\}$, are identified in the theorem, it is necessary to divide the results of Proposition 1 by $q - 1$ in order to arrive at the corresponding numbers in the theorem.

We now turn to the more complicated situation in which n is even, i.e. $4 \mid m$.

Let T denote the set of nonvanishing zeros of Ξ: $T = \{cw^{j_r} : c \in GF(q)\backslash\{0\}, j_r \in D\}$.

Our partition of D into $q + 1$ subsets $D_0, D_1, \ldots, D_q$, induces a partition of T into $q + 1$ subsets $T_0, T_1, \ldots, T_q$, where $T_i = \{cw^{j_r} : c \in GF(q)\backslash\{0\}, j_r \in D_i\}$ for all i. We have $|T_i| = (q - 1)|D_i|$.

The automorphism $d \to d^q$ maps the subset T_i onto T_{q+1-i}, because $\ell \equiv i \bmod q+1 \Leftrightarrow q\ell \equiv q+1-i \bmod q+1$. Hence the subsets T_0 and, if q is odd, $T_{\frac{1}{2}(q+1)}$ as well, are left invariant by said automorphism. But for $i \neq 0$ or $\frac{1}{2}(q+1)$, the subsets T_i and T_{q+1-i} are interchanged.

Let now $|D_i| = n_i$, $i = 0, 1, \ldots, q$. We have

$$\sum_{i=0}^{q} n_i = (q^{2n-1}-1)/(q-1) \tag{1}$$

and also, in virtue of the preceding paragraph:

$$n_1 = n_q, \qquad n_2 = n_{q-1}, \ldots, n_{q/2} = n_{1+q/2} \qquad \text{for } q \text{ even} \tag{2}$$

$$n_1 = n_q, \qquad n_2 = n_{q-1}, \ldots, n_{\frac{1}{2}(q-1)} = n_{\frac{1}{2}(q+3)} \qquad \text{for } q \text{ odd.} \tag{3}$$

Therefore Eq. (1) becomes Eq. (4) if q is even, or (5) if q is odd:

$$n_0 + 2n_1 + 2n_2 + \cdots + 2n_{q/2} = (q^{2n-1}-1)/(q-1) \tag{4}$$

$$n_0 + 2n_1 + 2n_2 + \cdots + 2n_{\frac{1}{2}(q-1)} + n_{\frac{1}{2}(q+1)} = (q^{2n-1}-1)/(q-1). \tag{5}$$

If, and only if, two numbers in D are in the same subset D_i, the two differences they give rise to are multiples of $q+1$ (one should bear in mind that this only holds because $q+1 \mid (q^m-1)/(q-1)$ for m even). Since the set $\{1, 2, \ldots, (q^{2n}-1)/(q-1)-1\}$ includes $(q^{2n}-q^2)/(q^2-1)$ multiples of $q+1$, it follows that

$$\sum_{i=0}^{q} n_i(n_i-1) = [(q^{2n-2}-1)/(q-1)][(q^{2n}-q^2)/(q^2-1)].$$

Combining this with (1) gives

$$\sum_{i=0}^{q} n_i^2 = (q^{4n-2}+q^{2n+1}-2q^{2n}-q^{2n-1}+1)/[(q-1)(q^2-1)]. \tag{6}$$

In the case of $GF(q^{2n})$, n even, the parity of q plays a crucial role. For q even, the proof is fairly straightforward. But for odd prime powers q, our attempts at finding a more or less "direct" proof, based on elementary properties of finite fields, have not been successful. Eventually a proof was found, but it has the heuristically unsatisfactory feature that it requires an incursion into the realm of correlations of finite projective planes.

For our present purposes it is not necessary to define the concept of correlation or of absolute point of a correlation. It suffices to mention the following two facts concerning correlations:

Fact 1 (Ball's Theorem [1]). In a projective plane of order n^*s^2, where n^* is square-free, the number of absolute points of a correlation is congruent to 1 modulo n^*s.

Fact 2. For every positive integer r there exists a correlation of the Desarguesian projective plane $PG(2, q^r)$ whose absolute points are precisely those points $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ which satisfy the equation $xy^q + x^q y + z^{q+1} = 0$.

We also need a third fact, which is a particular case of Theorem 19 in [2]. We state it as follows:

Fact 3. Consider the equation $x^q = \lambda x + \theta$, $\lambda, \theta \in GF(q^r)$, $\lambda \neq 0$.

If λ is a $(q-1)$th power, let $\lambda = \omega^{q-1}$. Then the given equation has q solutions, or no solution, in $GF(q^r)$, according to whether θ/ω^q is, or is not, a zero of Ξ.

We need to obtain a few more results before we can prove the theorem for n even.

Proposition 2. *In $PG(2, q^{2n})$, q odd, n even, the number of points $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ satisfying the equation $xy^q + x^q y + z^{q+1} = 0$ is given by $(q^2+q)N + q + 1$, where N stands for the number of zeros of Ξ which are $(q+1)$th powers.*

Proof. For $z = 0$, the equation in the statement of the proposition is satisfied by the points $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} \omega \\ 1 \\ 0 \end{pmatrix}$, where $\omega + \omega^q = 0$, i.e. $\omega = aw^{\frac{1}{2}(q^{2n}-1)/(q-1)}$, a ranging through the $GF(q)$ subfield. We have thus obtained $q+1$ points on the line $z = 0$.

For $z = 1$, the equation under consideration becomes

$$(x/y)^q = -x/y - 1/y^{q+1}. \tag{7}$$

As -1 is a $(q-1)$th power in $GF(q^{2n})$, it follows from Fact 3 that Eq. (7) has q solutions for x/y, or no solution. In the notation of Fact 3, we have $\theta = -1/y^{q+1}$, while ω is given by the expression in the first paragraph of this proof.

Then $\omega^q = aw^{\frac{1}{2}q(q^{2n}-1)/(q-1)}$, $a \in GF(q)$.

By virtue of Fact 3, Eq. (7) has q solutions if $\theta/\omega^q = -1/(y^{q+1}\omega^q) = -1/(ay^{q+1}w^{\frac{1}{2}q(q^{2n}-1)/(q-1)})$ is a zero of Ξ, and no solution otherwise. Here, the exponent of w is a multiple of $q+1$, because n is even by assumption. Thus θ/ω^q is a $(q+1)$th power.

Since N is the number of $(q+1)$th powers among the zeros of Ξ, there are N acceptable values for y^{q+1}. Hence there are N equations (7) to solve and each such equation yields q values for the ratio x/y. On the other hand, each of the N values for y^{q+1} supplies $q+1$ distinct values for y, because the equation $y^{q+1} = t^{q+1}$ has $q+1$ distinct solutions:

$$y = tw^{s(q^{2n}-1)/(q+1)}, \qquad s = 0, 1, \ldots, q.$$

Therefore we end up with $Nq(q+1)$ points with $z \neq 0$. □

The purpose of the foregoing proposition is to prove the next corollary. The number to the right of the divisibility bar in the corollary will be denoted a little later by a_0 and will play an important role in the case in which q is odd.

Corollary 3. $q^{n-1} \mid n_0 - (q^{2n-1} - q^{n+1} + q^n - 1)/(q^2-1)$.

Proof. With our notation, the number N in the preceding proposition is $(q-1)n_0$. By virtue of Fact 1, we therefore have:

$$(q-1)n_0(q^2+q) + q + 1 \equiv 1 \bmod q^n.$$

This leads to $n_0 = (uq^{n-1} - 1)/(q^2 - 1)$ for some integer u and the conclusion follows readily. □

Lemma 4. *If $a \in GF(q^{2n})$, q odd, n even, is of the form $a = w^{\frac{1}{2}(q+1)(2i+1)}$, where w is a primitive root of the field and $a^{q^s} = ca$ for some odd number s and some $c \in GF(q)$, then $q \equiv 1 \bmod 4$ and a is a zero of Ξ.*

Moreover, the number of elements a as described above, in $GF(q^{2n})$, is an even multiple of $q - 1$.

Proof. The condition $a^{q^s} = ca$ is equivalent to:

$$w^{\frac{1}{2}q^s(q+1)(2i+1)} = w^{r(q^{2n}-1)/(q-1)} w^{\frac{1}{2}(q+1)(2i+1)} w^{(q^{2n}-1)t}$$

for some integers r, t. This equation entails:

$$\tfrac{1}{2}(q^s - 1)(2i + 1) = [(q^{2n} - 1)/(q^2 - 1)][r + (q - 1)t]$$

which shows that:

$$(q^{2n} - 1)/(q^2 - 1) \mid \tfrac{1}{2}(q^s - 1)(2i + 1). \tag{8}$$

Since we have assumed that n is even and s is odd, the relationship (8) cannot take place if $q \equiv 3 \bmod 4$, proving the first claim of the lemma.

Next we will demonstrate that if a is of the form in the statement of the lemma and (8) holds, then $a^{q^n-1} = -1$, where $q \equiv 1 \bmod 4$. This equation is equivalent to $a^{q^n} + a = 0$, which implies $\Xi(a) = 0$.

Using the expression for a, the equation $a^{q^n-1} = -1$ is rewritten as

$$\begin{aligned} w^{\frac{1}{2}(q+1)(2i+1)(q^n-1)} &= w^{\frac{1}{2}(q^{2n}-1)} \\ &\Rightarrow q^{2n} - 1 \mid \tfrac{1}{2}(q + 1)(2i + 1)(q^n - 1) - \tfrac{1}{2}(q^{2n} - 1) \\ &\Rightarrow q^n + 1 \mid \tfrac{1}{2}(q + 1)(2i + 1) - \tfrac{1}{2}(q^n + 1). \end{aligned}$$

Let

$$t = \frac{\frac{1}{2}(q^s - 1)(2i + 1)}{(q^{2n} - 1)/(q^2 - 1)}. \tag{9}$$

Then $\frac{1}{2}(q + 1)(2i + 1) = \frac{(q^{2n}-1)t}{(q-1)(q^s-1)}$.

Thus we have to prove that $q^n + 1 \mid \frac{(q^{2n}-1)t}{(q-1)(q^s-1)} - \frac{1}{2}(q^n + 1)$, i.e. that $\frac{(q^n-1)t}{(q-1)(q^s-1)}$ is one half of an odd number.

Let $n = 2^r(2u + 1),\ r \geq 1$. Then

$$\frac{q^{2n} - 1}{q^2 - 1} = \frac{q^4 - 1}{q^2 - 1} \cdot \frac{q^8 - 1}{q^4 - 1} \cdot \frac{q^{16} - 1}{q^8 - 1} \cdots \frac{q^{2^{r+1}} - 1}{q^{2^r} - 1} \cdot \frac{q^{2n} - 1}{q^{2^{r+1}} - 1}.$$

The last fraction is an odd integer, because $2n = 2^{r+1}(2u+1)$. We rewrite the expression (9) for t as:

$$t = \frac{\frac{1}{2}(q^s - 1)(2i + 1)}{(q^2 + 1)(q^4 + 1) \ldots (q^{2^r} + 1)[(q^{2n} - 1)/(q^{2^{r+1}} - 1)]}.$$

As $q^{2^j}+1 \equiv 2 \bmod 4$ for all j, $\frac{1}{2}(q^s-1)$ must be a multiple of 2^r. So let $q^s-1 = 2^{r+1}v$. Then the last expression for t becomes:

$$t = \frac{(2i+1)v}{\frac{1}{2}(q^2+1)\cdot\frac{1}{2}(q^4+1)\ldots\frac{1}{2}(q^{2^r}+1)[(q^{2n}-1)/(q^{2^{r+1}}-1)]}. \tag{10}$$

Since $(q^u+1, q^s-1) = 2$ for any integer u (this is a consequence of [2, Lemma 8]), it follows that $(\frac{1}{2}(q^{2^j}+1), v) = 1$ for $j = 1, 2, \ldots, r$.

Further, let $(v, (q^{2n}-1)/(q^{2^{r+1}}-1)) = h$, where h is odd. It then follows that $2i+1$ is a (necessarily odd) multiple of the odd number:

$$\tfrac{1}{2}(q^2+1)\cdot\tfrac{1}{2}(q^4+1)\cdot\tfrac{1}{2}(q^8+1)\cdots\tfrac{1}{2}(q^{2^r}+1)\{(q^{2n}-1)/[h(q^{2^{r+1}}-1)]\}.$$

But this last number reduces to $(q^{2n}-1)/[2^r h(q^2-1)]$. As a consequence, Eq. (10) shows that t is an odd multiple of v/h, so that we can write $t = (2j+1)(q^s-1)/(2^{r+1}h)$. Then:

$$\frac{(q^n-1)t}{(q-1)(q^s-1)} = \frac{(q^n-1)(2j+1)(q^s-1)}{2^{r+1}h(q-1)(q^s-1)} = \frac{2j+1}{2^{r+1}h}\cdot\frac{q^n-1}{q-1}$$
$$= \frac{1}{2}\left[\frac{2j+1}{h}\cdot\frac{1}{2}(q+1)\cdot\frac{1}{2}(q^2+1)\cdot\frac{1}{2}(q^4+1)\cdots\frac{1}{2}(q^{2^{r-1}}+1)\cdot\frac{q^n-1}{q^{2^r}-1}\right].$$

All the factors in the square brackets are odd and thus $(q^n-1)t/[(q-1)(q^s-1)]$ is one half of an odd number indeed, completing the proof of the first paragraph of the lemma.

Concerning the second paragraph:

It has been shown above that $2i+1$ must be of the form $(2k+1)(q^{2n}-1)/[2^r h(q^2-1)]$. Therefore:

$$a = w^{\frac{1}{2}(q+1)(2i+1)} = w^{(2k+1)(q^{2n}-1)/[2^{r+1}h(q-1)]}.$$

In order to find the range of k, observe that the exponent of w must be less than $q^{2n}-1$, whence it follows that $k < 2^r h(q-1) - \frac{1}{2}$, i.e. $k = 0, 1, 2, \ldots, 2^r h(q-1) - 1$. Hence k takes on $2^r h(q-1)$ values. This last number is an even multiple of $q-1$, because $r \geq 1$. This completes the proof. □

Corollary 5. *In $GF(q^{2n})$, the number n_0 is odd.*

Proof. The fact that n_0 is odd plays a role in the proof of the theorem only if q is odd and n is even. For the sake of completeness, however, we have stated the corollary in its full generality.

For q even, Eq. (4), which is valid regardless of the parity of n, shows that n_0 must be an odd number.

We omit the proof for the case in which q and n are odd. So let q be odd and n be even.

We will demonstrate that the number $n_{\frac{1}{2}(q+1)}$ is even, which entails, by virtue of (5), that n_0 is odd.

We will say that two members of $T_{\frac{1}{2}(q+1)}$ are equivalent if their ratio is in the $GF(q)$ subfield. This equivalence relation partitions $T_{\frac{1}{2}(q+1)}$ into $n_{\frac{1}{2}(q+1)}$ equivalence classes of cardinality $q-1$. It has been observed earlier that the set $T_{\frac{1}{2}(q+1)}$ is invariant under the

group of automorphisms generated by the automorphism $d \to d^q$. The effect of this group on the equivalence classes just defined is to permute them in cycles of various lengths. If s is the smallest integer for which $a^{q^s}/a \in GF(q)$, then the equivalence class containing a belongs to a cycle of length s, where s, of course, can be even or odd.

By virtue of Lemma 4, every element $a = w^{\frac{1}{2}(q+1)(2i+1)}$ satisfying $a^{q^s}/a \in GF(q)$ for some odd s is a zero of Ξ and thus it is a member of $T_{\frac{1}{2}(q+1)}$. Consequently, in the case in which s is odd, there must be an even number of cycles of length s, because said lemma has shown that the *total* number of elements a as described in the preceding sentence is an even multiple of $q-1$.

Then, as $n_{\frac{1}{2}(q+1)}$ represents the sum of the lengths of all the cycles, it must be an even number, as claimed. □

We are now prepared to prove the next proposition, which completes the proof of the theorem.

Proposition 6. *Consider the finite field $GF(q^{2n})$, n even, and the $q^{2n-1}-1$ exponents of w in the set of nonvanishing zeros of $\Xi(x) = x^{q^{2n-1}} + x^{q^{2n-2}} + \cdots + x^q + x$. Among these exponents, there are $(q^{2n-1} - q^{n+1} + q^n - 1)/(q+1)$ that are multiples of $q+1$.*

Then, for each $i \in \{1, 2, \ldots, q\}$, there are $(q^{2n-1} + q^n - q^{n-1} - 1)/(q+1)$ exponents that are congruent to i modulo $q+1$.

Proof. Let:

$$A = (q^{2n-1} - q^{n+1} + q^n - 1)/(q^2-1),\ B = (q^{2n-1} + q^n - q^{n-1} - 1)/(q^2-1).$$

Since $|T_i| = (q-1)|D_i| = (q-1)n_i$, the following statements are equivalent to the claims of the present proposition: $n_0 = A$, $n_1 = n_2 = \cdots = n_q = B$.

We shall let:

$$n_0 = a_0 + A, \qquad n_i = a_i + B, \qquad i = 1, 2, \ldots, q. \tag{11}$$

Thus our goal is to show that $a_0 = a_1 = \cdots = a_q = 0$.

With this notation, Eqs. (4) and (5) become:

$$a_0 + 2a_1 + 2a_2 + \cdots + 2a_{\frac{1}{2}q} + A + qB = (q^{2n-1} - 1)/(q-1)$$

$$a_0 + 2a_1 + 2a_2 + \cdots + 2a_{\frac{1}{2}(q-1)} + a_{\frac{1}{2}(q+1)} + A + qB = (q^{2n-1} - 1)/(q-1)$$

But $A + qB = (q^{2n-1} - 1)/(q-1)$. Hence:

$$a_0 + 2a_1 + 2a_2 + \cdots + 2a_{\frac{1}{2}q} = 0 \qquad \text{for } q \text{ even} \tag{12}$$

$$a_0 + 2a_1 + 2a_2 + \cdots + 2a_{\frac{1}{2}(q-1)} + a_{\frac{1}{2}(q+1)} = 0 \qquad \text{for } q \text{ odd.} \tag{13}$$

Case I. q is a power of two.

Then, because of (2), the left side of (6) is $n_0^2 + 2n_1^2 + 2n_2^2 + \cdots + 2n_{\frac{1}{2}q}^2$, while its right side is $A^2 + qB^2$ (easy check).

Substitute here the expressions for n_i:

$$(a_0 + A)^2 + 2(a_1 + B)^2 + 2(a_2 + B)^2 + \cdots + 2(a_{\frac{1}{2}q} + B)^2 = A^2 + qB^2.$$

But (12) reduces this equation to: $a_0^2 + 2a_1^2 + 2a_2^2 + \cdots + 2a_{\frac{1}{2}q}^2 + 2(A-B)a_0 = 0$.

Furthermore, $A - B = -q^{n-1}$, hence:

$$a_0^2 + 2a_1^2 + 2a_2^2 + \cdots + 2a_{\frac{1}{2}q}^2 - 2a_0 q^{n-1} = 0. \tag{14}$$

For each i modulo $q+1$, the set $\{1, 2, \ldots, (q^{2n}-1)/(q-1)\}$ contains $(q^{2n}-1)/(q^2-1)$ numbers congruent to i modulo $q+1$. Therefore the difference set D yields Q differences congruent to i modulo $q+1$, where $Q = \lambda(q^{2n}-1)/(q^2-1) = [(q^{2n-2}-1)/(q-1)][(q^{2n}-1)/(q^2-1)]$.

For a fixed i, these differences are produced by pairs $\{j_r, j_{r'}\}$, where $j_r \in D_u$, $j_{r'} \in D_{u+i}$, $u = 0, 1, \ldots, q$. But $j_r - j_{r'} \equiv i \bmod q+1 \Leftrightarrow j_{r'} - j_r \equiv q+1-i \bmod q+1$. This leads to the following $\frac{1}{2}q$ equations, each of which contains one term that has been boxed:

$$\begin{aligned}
&n_0n_1 + n_1n_2 + \cdots + \boxed{n_{\frac{1}{2}q}n_{\frac{1}{2}q+1}} + \cdots + n_qn_0 = Q\\
&n_0n_2 + n_1n_3 + \cdots + n_{q-1}n_0 + \boxed{n_qn_1} = Q\\
&n_0n_3 + n_1n_4 + \cdots + \boxed{n_{\frac{1}{2}q-1}n_{\frac{1}{2}q+2}} + \cdots + n_{q-1}n_1 + n_qn_2 = Q\\
&n_0n_4 + n_1n_5 + \cdots + \boxed{n_{q-1}n_2} + n_qn_3 = Q\\
&\vdots\\
&n_0n_{\frac{1}{2}q} + n_1n_{\frac{1}{2}q+1} + \cdots + \boxed{n_{\frac{3}{4}q+1}n_{\frac{1}{4}q}} + \cdots + n_{q-1}n_{\frac{1}{2}q-2} + n_qn_{\frac{1}{2}q-1} = Q.
\end{aligned}$$

Each left side comprises $q+1$ terms. In the terms that have been boxed, and in none other, the two factors are equal, by (2). The $\frac{1}{2}q$ boxed terms are all different, obviously. By virtue of (2) again, the remaining q terms on each left side can be grouped into $\frac{1}{2}q$ pairs, such that the two terms in each pair are equal. As a consequence, we have for each $i \in \{1, 2, \ldots, \frac{1}{2}q\}$:

$$2n_0n_i + 2n_{j_{i1}}n_{k_{i1}} + \cdots + 2n_{j_{i,\frac{1}{2}q-1}}n_{k_{i,\frac{1}{2}q-1}} + n_{\ell_i}^2 = Q \tag{15}$$

where, for each i, the set of subscripts $\{i, j_{i1}, k_{i1}, \ldots, j_{i,\frac{1}{2}q-1}, k_{i,\frac{1}{2}q-1}, \ell_i\}$ consists of two copies of the set $\{1, 2, \ldots, \frac{1}{2}q\}$. Also, the $\frac{1}{2}q$ subscripts ℓ_i are all different.

Substitute into Eq. (15), the expressions (11) for $n_0, n_1, \ldots, n_{\frac{1}{2}q}$:

$$\begin{aligned}
&2(a_0+A)(a_i+B) + 2(a_{j_{i1}}+B)(a_{k_{i1}}+B)\\
&\quad + \cdots + 2(a_{j_{i,\frac{1}{2}q-1}}+B)(a_{k_{i,\frac{1}{2}q-1}}+B) + (a_{\ell_i}+B)^2 = Q.
\end{aligned}$$

This equation is transformed into:

$$\begin{aligned}
&2a_0a_i + 2a_{j_{i1}}a_{k_{i1}} + \cdots + 2(a_{j_{i,\frac{1}{2}q-1}}a_{k_{i,\frac{1}{2}q-1}} + a_{\ell_i}^2 + 2Aa_i\\
&\quad + 2B(a_0 + a_{j_{i1}} + a_{k_{i1}} + \cdots + a_{j_{i,\frac{1}{2}q-1}} + a_{k_{i,\frac{1}{2}q-1}} + a_{\ell_i})\\
&\quad + 2AB + (q-1)B^2 = Q.
\end{aligned}$$

It is an easy verification that $2AB + (q-1)B^2 = Q$. Also, $A = B - q^{n-1}$. Thus the last equation becomes:

$$2a_0a_i + 2a_{j_{i1}}a_{k_{i1}} + \cdots + 2a_{j_{i,\frac{1}{2}q-1}}a_{k_{i,\frac{1}{2}q-1}} + a_{\ell_i}^2 + 2B(a_0 + a_i + a_{j_{i1}} + a_{k_{i1}} + \cdots + a_{j_{i,\frac{1}{2}q-1}} + a_{k_{i,\frac{1}{2}q-1}} + a_{\ell_i}) - 2q^{n-1}a_i = 0.$$

Here, the coefficient of $2B$ is simply $a_0 + 2a_1 + \cdots + 2a_{\frac{1}{2}q}$, i.e. 0 (see (12)). Therefore, for each $i \in \{1, 2, \ldots, \frac{1}{2}q\}$ we have the equation:

$$2a_0a_i + 2a_{j_{i1}}a_{k_{i1}} + \cdots + 2a_{j_{i,\frac{1}{2}q-1}}a_{k_{i,\frac{1}{2}q-1}} + a_{\ell_i}^2 - 2q^{n-1}a_i = 0. \tag{16}$$

It has been observed earlier that the subscripts ℓ_i are all different, so that the set $\{\ell_i : i = 1, 2, \ldots, \frac{1}{2}q\}$ is actually the set $\{1, 2, \ldots, \frac{1}{2}q\}$.

As our goal is to prove that $a_0 = a_1 = \cdots = a_{\frac{1}{2}q} = 0$, we shall assume that some of the a_i's do not vanish and a contradiction will be arrived at.

Since all the a_i's must be integers, Eqs. (16) shows that $2 \mid a_1, a_2, \ldots, a_{\frac{1}{2}q}$. But $2 \mid a_0$ as well, by (12). It follows that all the terms with coefficient 2 in (16) are divisible by 2^3 (provided so is the last term). Hence $2^3 \mid a_i^2$, so that $2^2 \mid a_i$ for all i. Thus all the terms with coefficient 2 in (16) are multiples of 2^5 (provided so is the last term). Thus $2^5 \mid a_i^2$, whence $2^3 \mid a_i$. This inductive process can be continued as long as $2^r \leq q^{n-1}$, so that one obtains successively: $2^4 \mid a_i, \ldots, q^{n-1} \mid a_i$, for all i. But then every term with coefficient 2 in (16) is a multiple of $2q^{2n-2}$, hence $2q^{2n-2} \mid a_i^2 \Rightarrow 2q^{n-1} \mid a_i$ for all $i \neq 0$. This entails, by virtue of (12), that $4q^{n-1} \mid a_0$. But this can only take place if $a_0 = 0$, because Eq. (14) shows that $0 \leq a_0 \leq 2q^{n-1}$.

Therefore $a_0 = 0$. Now Eq. (14) shows that $a_1 = a_2 = \cdots = a_{\frac{1}{2}q} = 0$ and from Eqs. (2) we infer that $a_{\frac{1}{2}q+1} = \cdots = a_{q-1} = a_q = 0$ as well, concluding the proof of Case I.

*

Trusting that the attentive reader has noticed why for odd prime powers one cannot use the same approach as in Case I, and also that he/she will see in due course why the argument for odd prime powers fails for even prime powers, we now proceed to Case II.

*

Case II. q is an odd prime power.

Note that A, as defined at the beginning of the present proof, is an odd number. Then, because of (3), the left side of Eq. (6) is $n_0^2 + 2n_1^2 + 2n_2^2 + \cdots + 2n_{\frac{1}{2}(q-1)}^2 + n_{\frac{1}{2}(q+1)}^2$ and its right side is $A^2 + qB^2$, as in Case I. Proceeding as in that case, one arrives at the equation:

$$a_0^2 + 2a_1^2 + \cdots + 2a_{\frac{1}{2}(q-1)}^2 + a_{\frac{1}{2}(q+1)}^2 - 2a_0q^{n-1} = 0. \tag{17}$$

This equation shows that $0 \leq a_0 \leq 2q^{n-1}$. But Corollary 3 has shown that $q^{n-1} \mid a_0$ (see (11)), so that the only possibilities are $a_0 = 0$ or q^{n-1} or $2q^{n-1}$. The last number must

be ruled out, because $a_0 = 2q^{n-1} \Rightarrow a_1 = a_2 = \cdots = a_{\frac{1}{2}(q-1)} = a_{\frac{1}{2}(q+1)} = 0$, by virtue of (17). This, in turn, implies $a_0 = 0$, by (13).

The value $a_0 = q^{n-1}$ cannot be accepted, either, for the following reason: $n_0 = a_0 + A$, where A is odd and so is n_0 (by Corollary 5), so a_0 cannot be an odd number.

Therefore $a_0 = 0$, so that $a_1 = a_2 = \cdots = a_{\frac{1}{2}(q-1)} = a_{\frac{1}{2}(q+1)} = 0$, by (17). From Eqs. (3) we now infer that $a_{\frac{1}{2}(q+3)} = \cdots = a_{q-1} = 0$, too. □

References

[1] R.W. Ball, Dualities of finite projective planes, Duke Math. J. 15 (1948) 929–940.

[2] B.C. Kestenband, The correlations of finite Desarguesian planes, Part I: Generalities, J. Geom. 77 (2003) 61–101.

[3] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938) 377–385.