JP Journal of Geometry and Topology

Published Online: February 2015
Available online at http://www.pphmj.com/journals/jpgt.htm
Volume 16, Number 2, 2014, Pages 127-152

THE CORRELATIONS OF FINITE DESARGUESIAN PLANES OF EVEN SQUARE ORDER DEFINED BY UPPER TRIANGULAR MATRICES WITH FOUR NONZERO ENTRIES

Barbu C. Kestenband

Department of Mathematics
New York Institute of Technology
Old Westbury, NY 11568, U. S. A.
e-mail: bkestenb@nyit.edu

Abstract

The present article continues the classification of the correlations of $PG(2, q^{2n})$, q an even prime number.

As in the case in which q is odd, some matrices with four nonvanishing entries are equivalent to diagonal matrices. When this equivalence does not take place, a correlation defined by an upper triangular matrix with four nonzero entries, with companion automorphism (q^m), where $(m, 2n) = 1$, can have the following numbers of absolute points:

$$q^{2n} - q^{n+1} + 1 \text{ or } q^{2n} + q^n + 1 \text{ or } q^{2n} + 1 \text{ for } n \text{ odd},$$

$$q^{2n} + q^{n+1} + 1 \text{ or } q^{2n} - q^n + 1 \text{ or } q^{2n} + 1 \text{ for } n \text{ even}.$$

We also discuss the equivalence classes into which these correlations fall, as well as the configurations of their sets of absolute points.

Received: October 9, 2014; Accepted: November 14, 2014
2010 Mathematics Subject Classification: 51E15.
Keywords and phrases: companion automorphism, absolute set of a correlation, q^m-equivalence, residue class, full secant, short secant.

1. Introduction and Algebraic Preliminaries

The present article is the ninth, and penultimate, in a series devoted to the classification of correlations of finite Desarguesian planes.

Our plane now is $PG(2, q^{2n})$, where q is a power of two, and the companion automorphism is always (q^m), where $(m, 2n) = 1$, so m is invariably an odd number.

We assume familiarity on the part of the reader with basic definitions and results in previous papers in this series; we will refer to them whenever necessary.

Furthermore, many of the lemmas, propositions and theorems in the present article differ only slightly (and in some cases not at all), both in statement and in proof, from their counterparts in [4]. In these situations, we shall state the result in full, with the obvious understanding that q is a power of two, but if the proofs differ only in minor details, then we will omit them. Whenever this happens, next to each result we include in parentheses its original source and its number there.

The following symbols and abbreviations will be used, all in agreement with the notation, we used in previous papers devoted to the classification of correlations:

F: $GF(q^{2n})$, q an even prime power,

F': the $GF(q)$ subfield of F,

Q: the subset of F comprising the nonvanishing $(q+1)$th powers,

ZQ: the subset of F comprising the nonvanishing $(q-1)$th powers,

TQ: the subset of F comprising the nonvanishing (q^2-1)th powers,

w: a primitive root of F,

$*$: a matrix entry that may or may not be zero,

$*'$: a matrix entry that cannot be zero,

$$\Xi(x) = x^{q^{2n-1}} + x^{q^{2n-2}} + \cdots + x^q + x \text{ over } F,$$

$$\Phi_{\pi,\mu}(x) = x^{q^m+1} + \pi x + \mu \text{ over } F,\ (m,\ 2n) = 1.$$

Whenever a $\pm$ or a $\mp$ is used, it will be understood that the top sign pertains to n odd, and the bottom sign, to n even. The one exception to this rule occurs in the proof of Proposition 26, where the $\pm$ and $\mp$ are used in a slightly different way, as explained there.

Lemma 1. *In the field* F, $t \in Q \Leftrightarrow t^2 \in Q$.

Proof. Let $t = w^k$. Then $t^2 \in Q \Rightarrow 2k = (q+1)i + (q^{2n}-1)j$ for some integers i, j. This implies $q+1 \mid 2k$, whence $q+1 \mid k$, because q is even by assumption. □

We need to discuss the zeros of the trinomials $\Phi_{\pi,\mu}$. As always, they can have $q+1$, two, one, or no zeros, and, for a fixed μ, the number of values of π for which $\Phi_{\pi,\mu}$ possesses each of the four possible numbers of zeros depends solely upon whether $\mu \in Q$ or $\mu \notin Q$. Hence we introduce, as in the past, the following symbol, where μ is fixed and $i \in \{q+1,\ 2,\ 1,\ 0\}$:

${}_\mu\Omega_i$: the set of elements $\pi \in F$ for which $\Phi_{\pi,\mu}$ possesses i zeros.

Before we can calculate the numbers $|{}_\mu\Omega_i|$, we need two lemmas.

Let $q > 2$. For every $\ell \in \{1,\ 2,\ ...,\ q-2\}$, let $\ell \cdot ZQ$ denote the set obtained upon multiplying the members of ZQ by w^ℓ.

Lemma 2. *Let* $q > 2$ *and* $\ell \in \{1, 2, ..., q-2\}$ *be fixed. Then, as* ψ *ranges through* $\ell \cdot ZQ$, *so does the expression* $\psi(\psi+1)^{q^m-1}$.

Proof. By definition, $ZQ = \{w^{(q-1)i} : i = 1, 2, ..., (q^{2n}-1)/(q-1)\}$. We will show that ZQ can also be represented as $ZQ = \{w^{(q^m-1)i} : i = 1, 2, ..., (q^{2n}-1)/(q-1)\}$. If $w^{(q^m-1)i} = w^{(q^m-1)j}$, then $q^{2n}-1 | (i-j)(q^m-1)$. But $(m, 2n) = 1$ by assumption, which implies $(q^{2n}-1, q^m-1) = q-1$, by [1, Lemma 12], and thus, $(q^{2n}-1)/(q-1) | i-j$. As $1 \le i, j \le (q^{2n}-1)/(q-1)$, we have $|i-j| < (q^{2n}-1)/(q-1)$, hence $i = j$.

Let now $\psi = w^{\ell} w^{(q^m-1)i} \in \ell \cdot ZQ$. Then

$$\psi(\psi+1)^{q^m-1} = w^{\ell} w^{(q^m-1)i} [w^{\ell} w^{(q^m-1)i} + 1]^{q^m-1}$$

$$= w^{\ell} (w^{\ell+q^m i} + w^i)^{q^m-1} \in \ell \cdot ZQ.$$

In order to demonstrate that $\psi(\psi+1)^{q^m-1}$ ranges through $\ell \cdot ZQ$, we have to show that

$$(w^{\ell+q^m j} + w^j)^{q^m-1} = (w^{\ell+q^m i} + w^i)^{q^m-1} \Rightarrow i = j.$$

The last equation implies

$$w^{\ell+q^m j} + w^j = r(w^{\ell+q^m i} + w^i),\ r \in F'. \tag{1}$$

Let $w^{j-i} = r + u$, so that $w^j = rw^i + uw^i$ and $w^{q^m j} = rw^{q^m i} + u^{q^m} w^{q^m i}$. Substitute these expressions into (1): $w^{\ell}(rw^{q^m i} + u^{q^m} w^{q^m i}) + rw^i + uw^i = r(w^{\ell+q^m i} + w^j)$, whence $u^{q^m} w^{\ell+q^m i} = uw^i$. This equation shows that $u \neq 0 \Rightarrow w^{\ell} \in ZQ$. But we know that $w^{\ell} \notin ZQ$ (because $0 < \ell < q-1$), so $u = 0$ and $w^{j-i} = r \in F'$.

Now the same argument as above leads to the conclusion that $i = j$. □

For any fixed integer t, let tQ be the set obtained upon multiplying the members of Q by w^t. There are $q+1$ distinct sets tQ, corresponding to $t = 0, 1, ..., q$.

For each $\ell \in \{1, 2, ..., q-2\}$, we partition the set $\ell \cdot ZQ$ into $q+1$ equicardinal subsets $V_0, V_1, ..., V_q$, as follows: $V_k = \{w^{\ell+k(q-1)+j(q^2-1)} : j = 0, 1, ..., (q^{2n}-q^2)/(q^2-1)\}$.

The ratio of any two members of $\ell \cdot ZQ$ is an element of Q if and only if they belong to the same V_k subset, obviously.

We have, thus, proved the following lemma:

Lemma 3. *For every* $\ell \in \{1, 2, ..., q-2\}$ *and every* $t \in \{0, 1, ..., q\}$, *we have* $|\ell \cdot ZQ \cap tQ| = (q^{2n}-1)/(q^2-1)$.

Theorem 4. *Consider the field F. Then*:

A. *For a fixed* $\mu = \phi^{q^m+1} \in Q$,

(a) $|{}_\mu\Omega_{q+1}| = (q^{2n-1} \pm q^{n+1} \mp q^n - 1)/(q^2-1)$. *This count includes* $\pi = 0$. *For a fixed* $\pi \in {}_\mu\Omega_{q+1}$, *the ratio of any two zeros of* $\Phi_{\pi,\mu}$ *is a* $(q-1)th$ *power. If a is a zero of* $\Phi_{\pi,\mu}$ *for some* $\pi \in {}_\mu\Omega_{q+1}$, *then* $a/\phi \in ZQ$. *If* $a = \phi\varepsilon^{q^m-1}$ *is a zero, then* $\Xi(1/\varepsilon^{q^m+1}) = 0$. *Conversely, if* $1/\varepsilon^{q^m+1}$ *is a zero of* Ξ, *then* $\phi\varepsilon^{q^m-1}$ *is a zero of a trinomial* $\Phi_{\pi,\mu}$ *which has* $q+1$ *zeros*.

(b) $|{}_\mu\Omega_2| = \frac{1}{2}(q-2)(q^{2n}-1)/(q-1)$. *If a, b are the two zeros of* $\Phi_{\pi,\mu}$ *for some* $\pi \in {}_\mu\Omega_2$, *then* a/ϕ, b/ϕ, $a/b \notin ZQ$.

(c) $|{}_\mu\Omega_1| = q^{2n-1} \mp q^n$.

If a is the unique zero of $\Phi_{\pi,\mu}$ *for some* $\pi \in {}_{\mu}\Omega_1$, *then* $a/\phi \in ZQ$.

(d) $|{}_{\mu}\Omega_0| = \frac{1}{2}q(q^n \pm 1)^2/(q+1)$.

B. *For a fixed* $\mu \notin Q$,

(e) $|{}_{\mu}\Omega_{q+1}| = (q^{2n-1} \mp q^n \pm q^{n-1} - 1)/(q^2 - 1)$. *For a fixed* $\pi \in {}_{\mu}\Omega_{q+1}$, *the ratio of any two zeros of* $\Phi_{\pi,\mu}$ *is a* $(q-1)$*th power. If a is a zero of* $\Phi_{\pi,\mu}$ *for some* $\pi \in {}_{\mu}\Omega_{q+1}$, *then* $a^2/\mu \in ZQ$. *If a is a zero and* $a^2/\mu = \delta^{q^m-1}$, *then* $\Xi(1/a\delta) = 0$. *Conversely, if* $1/a\delta$ *is a zero of* Ξ, *where* $a^2 = \mu\delta^{q^m-1}$, *then a is a zero of a trinomial* $\Phi_{\pi,\mu}$ *which has* $q+1$ *zeros*.

(f) $|{}_{\mu}\Omega_2| = \frac{1}{2}(q-2)(q^{2n}-1)/(q-1)$. *If a, b are the two zeros of* $\Phi_{\pi,\mu}$ *for some* $\pi \in {}_{\mu}\Omega_2$, *then* a^2/μ, b^2/μ, $a/b \notin ZQ$.

(g) $|{}_{\mu}\Omega_1| = q^{2n-1} \pm q^{n-1}$. *If a is the unique zero of* $\Phi_{\pi,\mu}$ *for some* $\pi \in {}_{\mu}\Omega_1$, *then* $a^2/\mu \in ZQ$.

(h) $|{}_{\mu}\Omega_0| = \frac{1}{2}(q^{2n+1} \mp 2q^n + q)/(q+1)$. *This count includes* $\pi = 0$.

Proof. Let *a*, *b* be two distinct zeros of $\Phi_{\pi,\mu}$. Then

$$\pi = (\mu + a^{q^m+1})/a = (\mu + b^{q^m+1})/b. \tag{2}$$

If we let $\psi = b/a$, then equation (2) yields

$$a^{q^m+1} = \frac{\mu}{\psi(\psi+1)^{q^m-1}}. \tag{3}$$

Hence a necessary condition for the existence of (at least) two zeros is that

$$\frac{\mu}{\psi(\psi+1)^{q^m-1}} \in Q. \tag{4}$$

Conversely, assume that this condition is met and let a be any of the $q+1$ solutions of equation (3). Then

$$\pi = \frac{\mu + a^{q^m+1}}{a} = \frac{\mu}{a} + \frac{\mu}{a\psi(\psi+1)^{q^m-1}} = \frac{\mu}{a}\left[1 + \frac{\psi+1}{\psi(\psi+1)^{q^m}}\right] = \frac{\mu(\psi^{q^m+1}+1)}{a\psi(\psi+1)^{q^m}}$$

and it is a straightforward verification that

$$\begin{aligned} b^{q^m+1} + \pi b + \mu &= \psi^{q^m+1}a^{q^m+1} + \pi\psi a + \mu \\ &= \frac{\psi^{q^m+1}\mu}{\psi(\psi+1)^{q^m-1}} + \frac{\mu(\psi^{q^m+1}+1)}{a\psi(\psi+1)^{q^m}} \cdot a\psi + \mu = 0. \end{aligned}$$

Therefore, equation (4) is a necessary and sufficient condition for the existence of at least two zeros, a and $a\psi$.

If there is a third zero $(\psi+\ell)a$, $\ell \neq 0$, $\psi+1$, then we have $[(\psi+\ell)a]^{q^m+1} + \pi(\psi+\ell)a + \mu = 0$. Since $a\psi$ is a zero of $\Phi_{\pi,\mu}$, this equation reduces to

$$(\psi^{q^m}a^{q^m+1} + \pi a)\ell + \psi a^{q^m+1}\ell^{q^m} + \ell^{q^m+1}a^{q^m+1} = 0. \tag{5}$$

As $\pi a = \mu + a^{q^m+1}$ (by (2)) and a^{q^m+1} is given by equation (3), the coefficient of ℓ in (5) reduces to μ/ψ. Thus, since $\ell \neq 0$, we rewrite equation (5) as

$$\frac{1}{\ell^{q^m}} = \frac{\psi}{(\psi+1)^{q^m-1}} \cdot \frac{1}{\ell} + \frac{1}{(\psi+1)^{q^m-1}}. \tag{6}$$

This equation has the unwanted solution $\ell = \psi + 1$. If $\psi \notin ZQ$, then this is the only solution, by [1, Theorem 19(ii)]. If $\psi \in ZQ$, let $\psi = \xi^{q^m - 1}$ (by [2, Result 10], $\psi \in ZQ$ entails that ψ is a $(q^m - 1)$th power). Then equation (6) is of the form required by [1, Theorem 19]: $x^{q^m} = \lambda x + \theta$, where $x = 1/\ell$, $\lambda = [\xi/(\psi + 1)]^{q^m - 1}$, $\theta = 1/(\psi + 1)^{q^m - 1}$. In the notation of that theorem, $\omega = \xi/(\psi + 1)$, whence

$$\frac{\theta}{\omega^{q^m}} = \frac{(\psi + 1)^{q^m}}{(\psi + 1)^{q^m - 1}\xi^{q^m}} = \frac{\psi + 1}{\xi^{q^m}} = \frac{\xi^{q^m - 1} + 1}{\xi^{q^m}} = \frac{1}{\xi} + \frac{1}{\xi^{q^m}}.$$

Since $\Xi(1/\xi) = \Xi(1/\xi^{q^m})$, we infer that $\Xi(\theta/\omega^{q^m}) = 0$, and, in virtue of the above mentioned theorem, equation (6) will possess q roots (one of which is $\ell = \psi + 1$). Hence we have obtained $q - 1$ values $\ell \neq 0, \psi + 1$.

We conclude that $\Phi_{\pi,\mu}$ has $q + 1$ zeros if and only if $\psi \in ZQ$.

For $\psi = \alpha^{q^m - 1} \in ZQ$, we have

$$\psi(\psi + 1)^{q^m - 1} = (\alpha\psi + \alpha)^{q^m - 1} = (\alpha^{q^m} + \alpha)^{q^m - 1}.$$

As α ranges through $F\backslash\{0\}$, ψ takes on $(q^{2n} - 1)/(q - 1)$ distinct values, and they give rise to the same number of values for $\psi(\psi + 1)^{q^m - 1}$. But the latter are not distinct, as we shall now prove.

By [1, Lemma 13], the equation $\alpha^{q^m} + \alpha = 0$ has q solutions; they are the members of F' and we do not consider them.

If $\alpha^{q^m} + \alpha = t \neq 0$, then $\Xi(t) = 0$, in virtue of [1, Theorem 19(i)] (with $\lambda = \omega = 1$ and $\theta = t$). Then, according to the same theorem, the equation $\alpha^{q^m} + \alpha = t$ possesses q solutions, therefore, as a ranges through $F\backslash\{0\}$,

$t = \alpha^{q^m} + \alpha$ takes on $\frac{1}{q}(q^{2n} - q) = q^{2n-1} - 1$ distinct nonvanishing values, each repeated q times.

But $[\alpha w^{(q^{2n}-1)/(q-1)}]^{q^m} + \alpha w^{(q^{2n}-1)/(q-1)} = (\alpha^{q^m} + \alpha) w^{(q^{2n}-1)/(q-1)}$, which shows that if we let S stand for the set of distinct values of t (so $|S| = q^{2n-1} - 1$), the number of distinct exponents of w, reduced modulo $(q^{2n} - 1)/(q - 1)$, in the elements of S, is $(q^{2n-1} - 1)/(q - 1)$. Denote this $(q^{2n-1} - 1)/(q - 1)$-set by D.

The foregoing argument also implies that as α ranges through $F\backslash\{0\}$, the expression $\psi(\psi+1)^{q^m-1} = (\alpha^{q^m} + \alpha)^{q^m-1}$ takes on $(q^{2n-1} - 1)/(q - 1)$ values, each repeated q times.

The set D has been defined as the set of exponents of w in the set of nonzero solutions of the equation $\Xi(t) = 0$, reduced modulo $(q^{2n} - 1)/(q - 1)$. But Ξ is an additive function, whence it follows that D is a Singer difference set with parameters

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

The following facts are immediate consequences of the Theorem in [3] (with $r = 1$):

The set D comprises $(q^{2n-1} \pm q^{n+1} \mp q^n - 1)/(q^2 - 1)$ numbers divisible by $q + 1$. Then, for each $i = 1, 2, ..., q$, the set D contains $(q^{2n-1} \mp q^n \pm q^{n-1} - 1)/(q^2 - 1)$ numbers congruent to i modulo $q + 1$.

Since q is even and m is odd, we have $(q + 1, q^m - 1) = 1$, by Result 6 in [2]. Therefore, upon multiplying each element of D by $q^m - 1$, the numbers in the preceding paragraph do not change. As $\psi(\psi+1)^{q^m-1} = (\alpha^{q^m} + \alpha)^{q^m-1}$

$= t^{q^{m-1}}$, we see that those numbers also apply to the $(q^{2n-1}-1)/(q-1)$ distinct exponents of w in the set $\{\psi(\psi+1)^{q^m-1}\}$, as α ranges through $F\backslash\{0\}$, i.e., as ψ ranges through $ZQ\backslash\{1\}$.

In conclusion, as ψ ranges through $ZQ\backslash\{1\}$, among the exponents of w in the set $\{\psi(\psi+1)^{q^m-1}\}$ there are $(q^{2n} \pm q^{n+2} \mp q^{n+1} - q)/(q^2-1)$ numbers divisible by $q+1$. Then, for each $i = 1, 2, ..., q$, there are

$$(q^{2n} \mp q^{n+1} \pm q^n - q)/(q^2-1)$$

numbers congruent to i modulo $q+1$.

Let $\mu \in Q$ be fixed. Then equation (3) requires that $\psi(\psi+1)^{q^m-1} \in Q$ as well. Each ψ meeting this requirement produces $q+1$ a's and the same number of b's. We have, thus, obtained $(q^{2n} \pm q^{n+2} \mp q^{n+1} - q)/(q-1)$ pairs (a, b). Each pair leads to a unique π, by (2). But, for each of these π's, $\Phi_{\pi,\mu}$ must have $q+1$ zeros, which produce $q(q+1)$ different ratios ψ. Consequently, each π is arrived at $q(q+1)$ times, so that the numbers of distinct π's (including $\pi = 0$) are those given in the statement of this theorem (Part A(a)).

The same reasoning produces the numbers in Part B(e).

Let now a be a zero of $\Phi_{\pi,\mu}$ for some $\pi \in {}_{\mu}\Omega_{q+1}$, $\mu = \phi^{q^m+1}$. Then equation (3) becomes $(a/\phi)^2(a/\phi)^{q^m-1} = 1/\psi(\psi+1)^{q^m+1}$. As $\psi \in ZQ$, we have $(a/\phi)^2 \in ZQ$, too. By Lemma 1, this implies $a/\phi \in ZQ$ as well, as the present theorem claims (Part A(a)).

Let now $a = \phi\varepsilon^{q^m-1}$ be a zero. Then, upon using equation (3) with $\psi = \xi^{q^m-1}$ and $\mu = \phi^{q^m+1}$, we have

$$a^{q^m+1} = \phi^{q^m+1}\varepsilon^{q^{2m}-1} = \frac{\phi^{q^m+1}}{\xi^{q^m-1}(\xi^{q^m-1}+1)^{q^m-1}} = \frac{\phi^{q^m+1}}{(\xi^{q^m}+\xi)^{q^m-1}},$$

whence $1/\varepsilon^{q^m+1} = c(\xi^{q^m}+\xi)$ for some $c \in F'$. As $\Xi(ca) = c \cdot \Xi(a)$ for any $a \in F$ and any $c \in F'$, and $\Xi(\xi^{q^m}) = \Xi(\xi)$, we see that $\Xi(1/\varepsilon^{q^m+1}) = 0$, as claimed in Part A(a).

To conclude the proof of Part A(a), assume that $1/\varepsilon^{q^m+1}$ is a zero of Ξ for some ε. Then, by virtue of [1, Theorem 19(i)], the equation $\xi^{q^m} = \xi + 1/\varepsilon^{q^m+1}$ possesses solutions. Thus, $\varepsilon^{q^m+1} = 1/(\xi^{q^m}+\xi)$ for some ξ.

Let $a = \phi\varepsilon^{q^m-1}$, so that

$$a^{q^m+1} = \mu\varepsilon^{q^{2m}-1} = \mu/(\xi^{q^m}+\xi)^{q^m-1} = \mu/\psi(\psi+1)^{q^m-1},$$

where $\psi = \xi^{q^m-1}$.

Hence equation (3) holds, with $\psi \in ZQ$, which entails that a is a zero of a trinomial $\Phi_{\pi,\mu}$ which has $q+1$ zeros, the desired conclusion.

We pass now to Part A(b).

Let $\mu \neq 0$ be fixed. There is a unique $t \in \{0, 1, ..., q\}$ such that $\mu \in tQ$. Our trinomial will possess two zeros if and only if there exists a $\psi \notin ZQ$ (i.e., $\psi \in \ell \cdot ZQ$ for some ℓ) such that (4) holds (i.e., such that $\psi(\psi+1)^{q^m-1} \in tQ$). By Lemma 2, as ψ ranges through $\overline{ZQ}\backslash\{0\}$ (i.e., through all the sets $\ell \cdot ZQ$), so does $\psi(\psi+1)^{q^m-1}$. Since each of the $q-2$ sets $\ell \cdot ZQ$ includes $(q^{2n}-1)/(q^2-1)$ members of tQ - see Lemma 3 - we infer that there are $(q-2)(q^{2n}-1)/(q^2-1)$ ψ's that need to be considered.

Each such ψ gives $q+1$ triples (a, b, π). But ψ and $1/\psi$ produce the same pair (a, b) - and hence the same π - because $\mu/(1/\psi)(1/\psi+1)^{q^m-1} = \mu\psi^{q^m+1}/\psi(\psi+1)^{q^m-1} = (\psi a)^{q^m+1} = b^{q^m+1}$.

Therefore,

$$|{}_\mu\Omega_2| = \frac{1}{2}(q-2)(q^{2n}-1)(q+1)/(q^2-1) = \frac{1}{2}(q-2)(q^{2n}-1)/(q-1)$$

for every $\mu \neq 0$. This is the number that appears in Parts A(b), B(f).

Observe now the following:

If $\mu = \phi^{q^m+1}$ and $a/\phi \in ZQ$, where a is a zero of $\Phi_{\pi,\mu}$, and there is one more zero, then equation (3) shows that $\psi \in ZQ$, whence it follows that $\pi \in {}_\mu\Omega_{q+1}$. Therefore, if a is a zero of $\Phi_{\pi,\mu}$ with $\mu = \phi^{q^m+1}$, then $a/\phi \notin ZQ$, as Part A(b) claims.

Moreover, the converse is also true, i.e., if a is a zero of $\Phi_{\pi,\mu}$ with $\mu = \phi^{q^m+1}$ and $a/\phi \notin ZQ$, then $\pi \in {}_\mu\Omega_2$:

Let a be a zero of some $\Phi_{\pi,\mu}$, where $\mu = \phi^{q^m+1}$ and $a/\phi \notin ZQ$. Then $(a/\phi)^2 \notin ZQ$, either (in virtue of Lemma 1). This, in turn, shows that $(a/\phi)^{q^m+1} \notin ZQ$. As a consequence, the equation

$$\frac{1}{\ell^{q^m}} = \left(\frac{a}{\phi}\right)^{q^m+1} \cdot \frac{1}{\ell} + \frac{a^{q^m+1}}{\mu} \tag{7}$$

in the unknown ℓ has a unique solution and that solution is clearly not $\ell = 1$.

Equation (7) is equivalent to $\mu\ell = a^{q^m+1}(\ell^{q^m} + \ell^{q^m+1})$. It follows that

$(1+\ell)a$ is another zero of $\Phi_{\pi,\mu}$, because

$$[(1+\ell)a]^{q^m+1} + \pi(1+\ell)a + \mu$$

$$= a^{q^m+1}(1+\ell+\ell^{q^m}+\ell^{q^m+1}) + \pi a + \pi\ell a + \mu$$

$$= a^{q^m+1}(1+\ell) + \mu\ell + \pi a + \pi\ell a + \mu = (1+\ell)(a^{q^m+1} + \pi a + \mu) = 0.$$

Conversely, if $(1+\ell)a$ is another zero, then equation (7) must hold true. As said equation has a unique solution ℓ, we infer that a and $(1+\ell)a$ are the only zeros of $\Phi_{\pi,\mu}$, and thus, $\pi \in {}_\mu\Omega_2$, as claimed. This concludes the proof of Part A(b).

Next, we obviously have

$$|{}_\mu\Omega_1| = q^{2n} - 1 - (q+1)|{}_\mu\Omega_{q+1}| - 2|{}_\mu\Omega_2|, \tag{8}$$

$$|{}_\mu\Omega_0| = q^{2n} - |{}_\mu\Omega_{q+1}| - |{}_\mu\Omega_2| - |{}_\mu\Omega_1|. \tag{9}$$

These equations produce the numbers in Parts A(c), A(d).

The proof of Part A is now complete.

Let $\mu \notin Q$.

If a and $b = \psi a$ are two zeros of $\Phi_{\pi,\mu}$, then equation (3) must hold. This equation shows that $a^{q^m+1}/\mu \in ZQ \Rightarrow \psi \in ZQ$ as well, in which case equation (6) yields q values for ℓ, i.e., $\pi \in {}_\mu\Omega_{q+1}$. Hence, if $a^{q^m+1}/\mu \in ZQ$ (or, equivalently, $a^2/\mu \in ZQ$) for some zero a, then $\pi \in {}_\mu\Omega_1$ or ${}_\mu\Omega_{q+1}$, whence we deduce that $\pi \in {}_\mu\Omega_2 \Rightarrow a^2/\mu,\ b^2/\mu \notin ZQ$.

We shall now prove the converse: $a^{q^m+1}/\mu \notin ZQ$ and $\Phi_{\pi,\mu}(a) = 0$ imply $\pi \in {}_\mu\Omega_2$. Consider the equation $1/\ell^{q^m} = (a^{q^m+1}/\mu)(1/\ell) + a^{q^m+1}/\mu$,

which is the analogue of equation (7). Exactly as there, this equation yields a unique solution for ℓ (which is again not $\ell = 1$) and thus, $(1 + \ell)a$ is another zero, proving that $\pi \in {}_{\mu}\Omega_2$.

Next we demonstrate the last paragraph of Part B(e).

Let $a^2/\mu = \delta^{q^m - 1}$, whence $a^{q^m + 1} = \mu(a\delta)^{q^m - 1}$. Upon comparing this equation with equation (3), where $\psi = \xi^{q^m - 1}$, we obtain

$$(a\delta)^{q^m - 1} = \frac{1}{\xi^{q^m - 1}(\xi^{q^m - 1} + 1)^{q^m - 1}} = \frac{1}{(\xi^{q^m} + \xi)^{q^m - 1}},$$

so that $1/a\delta = c(\xi^{q^m} + \xi)$ for some $c \in F'$. This shows that $\Xi(1/a\delta) = 0$.

Conversely, assume that $1/a\delta$, where $a^2 = \mu\delta^{q^m - 1}$, is a zero of Ξ. Then, in virtue of [1, Theorem 19(i)], the equation $\xi^{q^m} = \xi + 1/a\delta$ has solutions for ξ, so that $a\delta = 1/(\xi^{q^m} + \xi)$ for some ξ.

Hence $(a\delta)^{q^m - 1} = 1/(\xi^{q^m} + \xi)^{q^m - 1}$, or

$$a^{q^m - 1}a^2/\mu = 1/\xi^{q^m - 1}(\xi^{q^m - 1} + 1)^{q^m - 1},$$

which is equation (3) with $\psi = \xi^{q^m - 1} \in ZQ$. As $\psi \in ZQ$, we conclude that a is a zero of a trinomial $\Phi_{\pi, \mu}$ with $q + 1$ zeros.

One now uses equations (8), (9) to arrive at the numbers in Parts B(g), B(h). □

As in [4], we devote the next four sections (one for each possible number of zeros) to the classification of correlations defined by upper triangular matrices of the form

$$A = \begin{pmatrix} r & \rho & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The absolute points of the correlation (A) satisfy the equation $rx^{q^m+1} + \rho xy^{q^m} + sy^{q^m+1} + z^{q^m+1} = 0$. As such, the number of zeros of the trinomial $rx^{q^m+1} + \rho x + s$ (which is clearly analogous to $\Phi_{\pi,\mu}$) represents the number of absolute points of (A) on the line $z = 0$.

2. Correlations with $q+1$ Absolute Points on the Line $z = 0$

Proposition 5. *If the correlation* (A) *possesses* $q+1$ *absolute points on the line* $z = 0$, *then* $A \sim diag(1, 1, t)$ *for some* $t \neq 0$.

Proof. We have seen in Theorem 4 Parts A(a) and B(e) that whenever the trinomial $\Phi_{\pi,\mu}$ has $q+1$ zeros, the ratio of any two of them is in ZQ, and the same obviously holds true for our trinomial $rx^{q^m+1} + \rho x + s$.

Then Lemma 6 in [4] - which is valid for q odd or even - states that if the ratio of two zeros is a member of ZQ, then $A \sim diag(1, 1, t)$ for some $t \neq 0$.

□

3. Correlations with One Absolute Point on the Line $z = 0$

The character of an absolute point of the correlation (A) is given by Definition 8 in [4].

Result 6 (Proposition 9 [4])**.** Assume that the absolute point $(a \;\; b \;\; 1)^T$ of (A) has character σ relative to (A). Then

$$C^T A C^{(q^m)} = \begin{pmatrix} 1 & \sigma & 0 \\ 0 & rs & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{10}$$

where $C = \begin{pmatrix} a & sb^{q^m} & 0 \\ b & ra^{q^m} + \rho b^{q^m} & 0 \\ 0 & 0 & J \end{pmatrix}$ and $J = w^{(q^{2n}-1)/(q+1)}$.

Conversely, if there exists a matrix $C = \begin{pmatrix} a & c & 0 \\ b & d & 0 \\ 0 & 0 & J \end{pmatrix}$ with $ad + bc = 1$ and such that equation (10) holds, then $(a \;\; b \;\; 1)^T$ is an absolute point of (A) and has character σ relative to (A). Moreover, $c = sb^{q^m}$ and $d = ra^{q^m} + \rho b^{q^m}$.

Result 7 (Lemma 11 [4])**.** Consider the field F and the exponents of w in the set of solutions of the equation $\Xi(x) = a$, where a is any nonzero element of F'.

Among these exponents, there are $(q^{2n-1} \mp q^n)/(q+1)$ which are multiples of $q+1$, and, for each $i \in \{1, 2, ..., q\}$, $(q^{2n-1} \pm q^{n-1})/(q+1)$ exponents which are congruent to i modulo $q+1$.

Exactly, as in [4], from Theorem 4, we infer that if a correlation (A) has a unique absolute point $(a \;\; 1 \;\; 0)^T$ on the line $z = 0$, then $ra^2/s \in ZQ$.

Result 8 (Theorem 12 [4])**.** If the trinomial $rx^{q^m+1} + \rho x + s$ has a unique zero a in F, let $ra^2/s = \delta^{q^m-1}$. Then the correlation (A) possesses the following number of absolute points:

$$q^{2n} \mp q^{n+1} + 1 \text{ if } ra\delta \in Q,$$

$$q^{2n} \pm q^n + 1 \text{ if } ra\delta \notin Q.$$

Result 9 (Theorem 13 [4])**.** Let $A = \begin{pmatrix} r & \rho & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $A' = \begin{pmatrix} r' & \rho' & 0 \\ 0 & s' & 0 \\ 0 & 0 & 1 \end{pmatrix}$ be such that the correlations $(A), (A')$ have a unique absolute point on the line $z = 0 : (a \ 1 \ 0)^T, (a' \ 1 \ 0)^T$, respectively. Then $A \sim A'$ if and only if $(r'a'\rho')^{\alpha}/ra\delta \in Q$ for some automorphism α of the field, where $\delta^{q^m-1} = ra^2/s$, $\delta'^{q^m-1} = r'a'^2/s'$.

The preceding two results imply, as in the case in which q was odd, the next corollary.

Corollary 10. *All the correlations with* $q^{2n} - q^{n+1} + 1$ *or* $q^{2n} + q^{n+1} + 1$ *absolute points are* q^m*-equivalent.*

In [4], where q was odd, Theorem 13 was the "last word" regarding the q^m-equivalence of correlations (A) with one absolute point on the line $z = 0$. If q is even, Lemma 1 (which has no analogue for q odd) enables us to give a simpler criterion for the q^m-equivalence of these correlations:

Theorem 11. *Let* A, A' *be as in Result* 9. *Then* $A \sim A'$ *if and only if* $(r's')^{\alpha}/rs \in Q$ *for some automorphism* α *of* F.

Proof. We shall demonstrate that $(r'a'\delta')^{\alpha}/ra\delta \in Q \Leftrightarrow (r's')^{\alpha}/rs \in Q$.

We have seen (see the paragraph preceding Result 8) that $r'a'^2/s' \in ZQ$. Thus, we can write

$$a'^2 = \frac{s'\delta'^{q^m-1}}{r'} \Leftrightarrow r'^2a'^2\delta'^2 = r's'\delta'^{q^m+1} \Leftrightarrow (r'a'\delta')^{2\alpha}/(r's')^{\alpha} = \delta'^{(q^m+1)\alpha}$$

and likewise $(ra\delta)^2/rs = \delta^{q^m+1}$. Thus,

$$\frac{(r's')^{\alpha}}{rs} = \frac{(r'a'\delta')^{2\alpha}}{(ra\delta)^2} \cdot \left(\frac{\delta}{\delta'^{\alpha}}\right)^{q^m+1}. \tag{11}$$

Hence $(r'a'\delta')^{\alpha}/ra\delta \in Q \Rightarrow (r's')^{\alpha}/rs \in Q.$

Conversely, equation (11) shows that $(r's')^{\alpha}/r \in Q \Rightarrow (r'a'\delta')^{2\alpha}/(ra\delta)^2 \in Q,$ and the conclusion follows from Lemma 1. □

Result 12 (Theorem 16 [4])**.** Let a be the unique zero of the trinomial $rx^{q^m+1} + \rho x + s, \quad (m, 2n) = 1,$ and consider the correlation (A). Then, regardless of the cardinality of the absolute set:

(i) All the secants through the absolute point $(a \;\; 1 \;\; 0)^T$ are full.

(ii) Each of the other absolute points is incident with $(q^{2n+1} - 2q^{2n} + q)/(q-1)$ short secants.

4. Correlations with Two Absolute Points on the Line $z = 0$

As in [4], and for exactly the same reasons, from now on we will use, instead of A, the matrix

$$M = \begin{pmatrix} 1 & \rho & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Result 13 (Theorem 17 [4])**.** For $\rho \in {}_s\Omega_2,$ the correlation (M) possesses $q^{2n} + 1$ absolute points.

Result 14 (Theorem 18 [4])**.** Let $\rho \in {}_s\Omega_2, \;\; \rho' \in {}_{s'}\Omega_2,$ and consider the matrices

$$M = \begin{pmatrix} 1 & \rho & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M' = \begin{pmatrix} 1 & \rho' & 0 \\ 0 & s' & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let the two absolute points on the line $z = 0$ be $(a\ \ 1\ \ 0)^T$, $(b\ \ 1\ \ 0)^T$ for the correlation (M), and $(a'\ \ 1\ \ 0)^T$, $(b'\ \ 1\ \ 0)^T$ for (M').

Then $M \sim M'$ if and only if there exists an automorphism α of F such that either $h/h'^{\alpha} \in TQ$ or $hh'^{\alpha} \in TQ$, where $h = s/b\sqrt[q^m]{b}$ or $s/a\sqrt[q^m]{a}$, $h' = s'/b'\sqrt[q^m]{b'}$ or $s'/a'\sqrt[q^m]{a'}$.

Result 15 (Theorem 19 [4])**.** If the correlation (M) has two absolute points on the line $z = 0$, then:

(i) All the secants through those two points are short.

(ii) Each of the other absolute points is incident with $q^{2n} - q^{2n-1} - \cdots - q^2 - q$ short secants, $(q^{2n-1} - 1)/(q - 1)$ full secants, and q^{2n-1} tangents.

5. Correlations without Absolute Points on the Line $z = 0$

Result 16 (Lemma 20 [4])**.** Let $\rho, s \in F, \rho s \neq 0$. If there exist two distinct elements $t, u \in F$ such that the product $\begin{pmatrix} t & 1 \\ u & 1 \end{pmatrix}\begin{pmatrix} 1 & \rho \\ 0 & s \end{pmatrix}\begin{pmatrix} t^{q^m} & u^{q^m} \\ 1 & 1 \end{pmatrix}$ is a diagonal matrix, then the ratio $\vartheta = u/t$ satisfies the equation

$$\vartheta^2 + \frac{w^{i(q^m+1)}}{s}\vartheta + 1 = 0. \tag{12}$$

Result 17 (Lemma 21 [4])**.** Let i and $s \neq 0$ be fixed in such a way that equation (12) possesses solutions, and let ϑ denote one of them. Then let t be a root of the equation

$$t^{q^m+1} = \frac{w^{i(q^m+1)}}{(\vartheta + 1)^{q^m+1}}. \tag{13}$$

Further, let $u = \vartheta t$ and calculate ρ from one of the equations

$$\rho = t^{q^m} + \frac{s}{u} = u^{q^m} + \frac{s}{t}. \tag{14}$$

Let $\varepsilon = w^{(q^{2n}-1)/(q+1)}$.

Then there are $2(q+1)$ distinct ordered pairs (t_j, u_j), (u_j, t_j), $j = 0, 1, ..., q$, giving rise to $2(q+1)$ triples (t_j, u_j, ρ_j), (u_j, t_j, ρ_j), where $t_j = t\varepsilon^j$, $u_j = u\varepsilon^j$, $\rho_j = \rho\varepsilon^{-j}$ such that

$$\begin{pmatrix} t_j & 1 \\ u_j & 1 \end{pmatrix}\begin{pmatrix} 1 & \rho_j \\ 0 & s \end{pmatrix}\begin{pmatrix} t_j^{q^m} & u_j^{q^m} \\ 1 & 1 \end{pmatrix} = diag(t(t+u)^{q^m}, u(t+u)^{q^m})$$

and

$$\begin{pmatrix} u_j & 1 \\ t_j & 1 \end{pmatrix}\begin{pmatrix} 1 & \rho_j \\ 0 & s \end{pmatrix}\begin{pmatrix} u_j^{q^m} & t_j^{q^m} \\ 1 & 1 \end{pmatrix} = diag(u(t+u)^{q^m}, t(t+u)^{q^m}).$$

The same collection of $2(q+1)$ triples is arrived at regardless of which one of the solutions of (12) and (13) and which one of equations (14) are used.

Moreover, if the two solutions of (12) are not members of F', then $\rho \neq 0$. If they are, then $s \in Q$ and $\rho = 0$.

Result 18 (Lemma 22 [4])**.** Let $s \in Q$ be fixed. Then there are $\frac{1}{2}(q-2)$ integers i modulo $(q^{2n}-1)/(q+1)$ for which the solutions of equation (12) entail, via equations (13), (14), that $\rho = 0$.

Result 19 (Lemma 23 [4])**.** Let $B = \begin{pmatrix} 1 & \rho \\ 0 & s \end{pmatrix}$, $\rho \in {}_s\Omega_{q+1} \backslash \{0\}$. Then there exist at most $q^2 - q$ matrices of the form $E = \begin{pmatrix} t & u \\ 1 & 1 \end{pmatrix}$, $t \neq u$ such that $E^T B E^{(q^m)}$ is a diagonal matrix.

Result 20 (Lemma 24 [4])**.** The correlation (*I*) possesses $q^3 - q$ absolute points with character zero.

Result 21 (Corollary 25 [4])**.** The collineation $(I)^2$ leaves invariant $q^3 + 1$ absolute points of the correlation (*I*).

Result 22 (Lemma 26 [4])**.** If $s \notin Q$, then the correlation $(diag(1, s, 1))$ has $q+1$ absolute points with character zero, namely $(w^{i(q^{2n}-1)/(q+1)}, 0, 1)^T$, $i = 0, 1, ..., q$.

Result 23 (Lemma 27 [4])**.** If $s \notin Q$ and the correlation (*M*) has absolute points with character zero, then it has $q+1$ such absolute points, which are collinear, and $\rho \in {}_s\Omega_0$.

If $s \in Q$ and the correlation (*M*) has absolute points with character zero, then it has $q^3 - q$ such points, and $\rho \in {}_s\Omega_{q+1}$.

Result 24 (Lemma 28 [4])**.** (i) If $\rho \in {}_s\Omega_0 \backslash \{0\}$ and the absolute set of the correlation (*M*) comprises points with character zero, then there exists a unique unordered pair (t, u) such that $E^T M E^{(q^m)} = diag(*', *', 1)$, where $E = \begin{pmatrix} t & u & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(ii) If $\rho \in {}_s\Omega_0 \backslash \{0\}$ and the absolute set of (*M*) has no points with character zero, then there exists at most one pair (t, u) as described above.

We leave to the reader the simple proof of the next lemma.

Lemma 25. *Let* $a, b \in F\backslash\{0, 1\}$. *If* $e = a + a^{-1}$, $f = b + b^{-1}$, $g^{-1} = e^{-1} + f^{-1}$, *then* $g = c + c^{-1}$, *where* $c = (ab+1)/(a+b)$ *or* $(a+b)/(ab+1)$.

Let now $a \neq 1$. Then $a + a^{-1} \neq 0$. Therefore, for each

$$i \in \left\{1, 2, ..., \frac{1}{2}(q^{2n} - 2)\right\},$$

we can write $w^i + w^{-i} = w^{\ell_i}$. These sums (i.e., the exponents ℓ_i) are all distinct, because $a + a^{-1} = b + b^{-1} \Rightarrow a = b$ or b^{-1}. But, for any $i, j \in \left\{1, 2, ..., \frac{1}{2}(q^{2n} - 2)\right\}, i \neq j,$ we have $0 < i + j \leq q^{2n} - 2,$ so that $w^j \neq w^{-i}$.

Let $q = 2^u,$ so that F is $GF(2^{2nu})$ and we have $\frac{1}{2}(q^{2n} - 2) = 2^{2nu} - 1$ different ℓ_i's. Our field F is generated by a polynomial $f(x)$ of degree $2n$, primitive irreducible over F'. Then the polynomial $f_1\left(\frac{1}{x}\right) = \frac{1}{x^{2n}} f(x)$ is also of degree $2n$, in the variable $1/x,$ primitive irreducible over $F',$ and, as such, it generates a field $F_1 \sim F$ in which w^{-1} is a primitive root.

It follows from Lemma 25 that the elements $w^{-\ell_i}$ make up a subspace of the vector space F_1. Consequently, the numbers ℓ_i form a (v, k, λ)-Singer difference set with parameters $v = q^{2n} - 1 = 2^{2nu} - 1,$ $k = 2^{2nu-1} - 1,$ $\lambda = 2^{2nu-2} - 1.$

Proposition 26. $\rho \in {}_s\Omega_0 \Rightarrow M \sim diag(*', *', *')$.

Proof. The number of equations (12) with roots in F is the number of integers i modulo $(q^{2n} - 1)/(q + 1)$ for which

$$\vartheta + \vartheta^{-1} = \frac{w^{i(q^m + 1)}}{s}. \tag{15}$$

Case I. $s \in Q$.

In this case, equation (15) requires that $\vartheta + \vartheta^{-1} \in Q$. In order to

determine the number of possible *i*'s, we need to appeal to some results in [3]. It was shown there that one can adopt the view that Singer's theorem concerns the exponents of the primitive root w of $GF(q^{2n})$ in the set of nonvanishing zeros of Ξ. It was also shown in that paper (Propositions 1(ii), 7) that among those exponents there are $\dfrac{q^{2n-1} \pm q^{n+r} \mp q^{n+r-1} - 1}{q^r + 1}$ which are multiples of $q^r + 1,$ where r is any divisor of n; the top sign applies for n/r odd, and the bottom sign, for n/r even.

As our field is $GF(2^{2nu}),$ we replace q, n and r in the above expression with 2, nu and u, respectively. We, thus, arrive at the number

$$\frac{2^{2nu-1} \pm 2^{nu+u} \mp 2^{nu+u-1} - 1}{2^u + 1}$$

$$= \frac{2^{2nu-1} \pm 2^{nu+u-1} - 1}{2^u + 1} = \frac{2^{2nu} \pm 2^{nu+u} - 2}{2(2^u + 1)} = \frac{q^{2n} \pm q^{n+1} - 2}{2(q+1)}.$$

We let N stand for the number of *i*'s (i.e., the number of equations (12)) that correspond to nonzero values of ρ. In virtue of Result 18, we have

$$N = \frac{q^{2n} \pm q^{n+1} - 2}{2(q+1)} - \frac{q-2}{2} = \frac{q^{2n} \pm q^{n+1} - q^2 + q}{2(q+1)}. \qquad (16)$$

Since one equation (12) gives rise to $q+1$ values of ρ, the number of ρ's is $\frac{1}{2}(q^{2n} \pm q^{n+1} - q^2 + q).$ But they are not necessarily distinct, because two or more equations (12) can lead to the same $(q+1)$-set of values of ρ.

Let N_0, N_{q+1} stand for the number of equations (12) that correspond to elements $\rho \in {}_s\Omega_0,$ $\rho \in {}_s\Omega_{q+1} \backslash \{0\},$ respectively. Then $N_0 + N_{q+1} = N,$ because $\rho \in {}_s\Omega_1 \bigcup {}_s\Omega_2 \Rightarrow M \not\sim diag(*', *', *')$. Reasoning as in the proof of Proposition 30 in [4], one arrives at the following inequalities, which

are similar to (49), (50) in said article: $(q+1)N_0 \le |{}_s\Omega_0|$, $(q+1)N_{q+1} \le \frac{1}{2}(q^2-q)(|{}_s\Omega_{q+1}|-1)$. Denote the right hand sides of these inequalities by U, V, respectively. Upon substituting the numbers $|{}_s\Omega_0|$ and $|{}_s\Omega_{q+1}|$, as given by Theorem 4 Parts (a), (d), it turns out that $U+V=(q+1)N$ (see (16)).

Therefore, we have: $(q+1)N_0 \le U$, $(q+1)N_{q+1} \le V$, $(q+1)N_0 + (q+1)N_{q+1} = (q+1)N = U+V$. It follows that $(q+1)N_0 = U = |{}_s\Omega_0|$, which demonstrates our claim that *every* matrix M with $s \in Q$ and $\rho \in {}_s\Omega_0$ is q^m-equivalent to a diagonal matrix.

Case II. $s \notin Q$.

In this case, equation (15) requires that $\vartheta + \vartheta^{-1} \notin Q$.

It was shown in [3] (Propositions 1(ii), 7 again) that in $GF(q^{2n})$, among the exponents of w in the set of nonvanishing zeros of Ξ, there are $\frac{q^{2n-1} \mp q^n \pm q^{n-1} - 1}{q^r + 1}$ which are congruent to i modulo $q^r + 1$, where i is any element of the set $\{1, 2, ..., q^r\}$ and r is any divisor of n; the sign rule is the same as in Case I.

Proceeding as in Case I, i.e., using 2, nu, u instead of q, n, r in the fraction in the preceding paragraph, said fraction becomes

$$\frac{2^{2nu-1} \mp 2^{nu} \pm 2^{nu-1} - 1}{2^u + 1}$$

$$= \frac{2^{2nu-1} \mp 2^{nu-1} - 1}{2^u + 1} = \frac{2^{2nu} \mp 2^{nu} - 2}{2(2^u + 1)} = \frac{q^{2n} \mp q^n - 2}{2(q+1)}.$$

It follows now from Result 17 that the total number of nonzero ρ's is $\frac{1}{2}(q^{2n} \mp q^n - 2)$. The same argument as in Case I leads to $(q+1)N_0 \leq (|{}_s\Omega_0| - 1)$ (because $s \notin Q \Rightarrow 0 \in {}_s\Omega_0$) and

$$(q+1)N_{q+1} \leq \frac{1}{2}(q^2 - q)|{}_s\Omega_{q+1}|.$$

Using the same notation as in Case I, we have $U + V = |{}_s\Omega_0| - 1 + \frac{1}{2}(q^2 - q)|{}_s\Omega_{q+1}|$, into which we substitute the numbers $|{}_s\Omega_0|$ and $|{}_s\Omega_{q+1}|$, as given by Theorem 4 Parts B(h), B(e), to arrive, as in Case I, at $U + V = (q+1)N$.

We infer, as in that case, that *every* matrix M with $s \notin Q$ and $\rho \in {}_s\Omega_0$ is q^m-equivalent to a diagonal matrix. □

6. Synopsis of the Results

In $GF(q^{2n})$, q even, the classification of correlations (A) defined by matrices

$$A = \begin{pmatrix} r & \rho & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with companion automorphism (q^m), $(m, 2n) = 1$, depends upon the number of zeros of the trinomial $rx^{q^m+1} + \rho x + s$. This trinomial can have $q+1$ or two, or one, or no zeros (Theorem 4). If said trinomial possesses $q+1$ zeros, or no zeros, then A is q^m-equivalent to a diagonal matrix (Propositions 5, 26). These correlations have been classified in [2].

If the trinomial under consideration has one zero, then the number of absolute points of the correlation (A) is (Result 8):

$$q^{2n} - q^{n+1} + 1 \text{ or } q^{2n} + q^n + 1 \text{ if } n \text{ is odd,}$$

$$q^{2n} + q^{n+1} + 1 \text{ or } q^{2n} - q^n + 1 \text{ if } n \text{ is even.}$$

These correlations fall into several equivalence classes (Theorem 11). The configuration of their absolute sets is given by Result 12.

If the above trinomial has two zeros, then the corresponding correlation has $q^{2n} + 1$ absolute points (Result 13).

There are several equivalence classes in this case, too (Result 14).

The configuration of the absolute sets is given by Result 15.

References

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

[2] Barbu C. Kestenband, The correlations of finite Desarguesian planes of square order defined by diagonal matrices, Linear Algebra Appl. 423 (2007), 366-385.

[3] Barbu C. Kestenband, The generalized addendum to James Singer's theorem on difference sets, Oriental J. Math. (2010), 223-235.

[4] Barbu C. Kestenband, The correlations of finite Desarguesian planes of odd square order defined by upper triangular matrices with four nonzero entries, JP J. Geometry and Topology 10(2) (2010), 113-170.