Europ. J. Combinatorics (2002) **23**, 201–206
doi:10.1006/eujc.2001.0523
Available online at http://www.idealibrary.com on IDEAL®

Proof of a Conjecture of De Caen and Van Dam

GARY L. EBERT, SEBASTIAN EGNER, HENK D. L. HOLLMANN† AND QING XIANG

We present a proof for a conjecture of De Caen and Van Dam (2001, Europ. J. Combinatorics, **22,** 297–301) concerning the existence of a four-class association scheme on the set of all unordered pairs of points of the projective line PG$(1, q^2)$, where $q = 2^m$.

1. INTRODUCTION

In this paper we present a proof for a conjecture in [3] on the existence of a certain four-class association scheme. In order to explain the conjecture, we briefly review some of the results from [3], in which further background and proofs can be found.

Let $\mathbf{F}_q$ denote the Galois field of order q, q a prime power. The group PGL$(2, q)$ of Möbius transformations is sharply three-transitive on the projective line PG$(1, q)$; moreover, the natural induced action on unordered pairs of points from PG$(1, q)$ is generously transitive, hence affords a (symmetric) association scheme FT$(q + 1)$. The relations of this scheme, a fission scheme of the triangular (Johnson) scheme T$(q+1)$ = J$(q+1, 2)$, can be described as follows. The *cross-ratio*

$$\rho(a, b; c, d) = (a - c)(b - d)/(a - d)(b - c) \tag{1}$$

is a complete invariant for ordered quadruples (a, b, c, d) of distinct points of PG$(1, q)$, that is, a quadruple can be mapped to another quadruple if and only if they have the same cross-ratio. As a consequence, the scheme FT$(q + 1)$ has relations R_0 (the diagonal relation), R_1 (the line graph of the complete graph on $\binom{q+1}{2}$ vertices), and a relation $R_{\{s,s^{-1}\}}$ for each pair $\{s, s^{-1}\}$ from $\mathbf{F}_q \setminus \{0, 1\}$, where $(\{a, b\}, \{c, d\}) \in R_{\{s,s^{-1}\}}$ if $\rho(a, b; c, d) \in \{s, s^{-1}\}$.

In [3], De Caen and Van Dam conjectured that fusion of certain relations in FT$(q^2 + 1)$, $q = 2^m$, produces a four-class scheme. To make this precise, let us define subsets $\mathbf{B}_0^*$ and $\mathbf{B}_1^*$ of $\mathbf{F}_{q^2}$ by

$$\mathbf{B}_0^* := \mathbf{F}_q \setminus \{0, 1\}, \qquad \mathbf{B}_1^* := \{x \in \mathbf{F}_{q^2} | x \neq 1, x^q = x^{-1}\}. \tag{2}$$

Now let $S_0 = R_0$, $S_1 = R_1$, let S_2 and S_3 be the union of all relations $R_{\{s,s^{-1}\}}$ with $s \in \mathbf{B}_0^*$ and $s \in \mathbf{B}_1^*$, respectively, and let S_4 be the union of all remaining relations $R_{\{s,s^{-1}\}}$. De Caen and Van Dam [3] conjectured the following.

THEOREM 1. *The relations S_i, $i = 0, \ldots, 4$, form a four-class association scheme.*

They noted that in order to prove this, it is sufficient to prove that for all i, j in $\{0, 1\}$ the numbers

$$\pi_{i,j}(r) := \frac{1}{2} \sum_{s \in \mathbf{B}_i^*, t \in \mathbf{B}_j^*} |\{x \in \mathbf{F}_{q^2} \mid x^2 + (r + s + t + rst)x + rs + rt + st = 0\}| \tag{3}$$

are constant for $r \in \mathbf{B}_0^*$, $r \in \mathbf{B}_1^*$, and $r \in \mathbf{F}_{q^2} \setminus (\{0, 1\} \cup \mathbf{B}_0^* \cup \mathbf{B}_1^*)$, respectively. Note that these (supposedly) constant values would be the intersection numbers of the fusion scheme $\mathcal{S}(q^2 + 1)$ in Theorem 1 involving the relations S_2, S_3, and S_4, as can be easily seen from [3].

†To whom correspondence should be addressed. *E-mail*: henk.d.l.hollmann@philips.com

0195–6698/02/020201 + 06 $35.00/0

Our proof consists of a direct evaluation of (3). Although by the time of submitting this paper we knew of at least three other proofs [2, 4, 5], we still feel that this proof is of interest since it is completely elementary, based only on some well-chosen substitutions.

2. Preliminaries

In the remainder of this paper, q will denote a fixed power of two. We write $t_q(x)$ to denote the image of $x \in \mathbf{F}_{q^2}$ under the map $x \mapsto x + x^2 + \cdots + x^{q/2}$. Note that if $x \in \mathbf{F}_q$, then $t_q(x)$ is just the trace from $\mathbf{F}_q$ to $\mathbf{F}_2$ of x. Also, we write $\mathrm{Tr}_{q^2}(x)$ to denote the trace of $x \in \mathbf{F}_{q^2}$ from $\mathbf{F}_{q^2}$ to $\mathbf{F}_2$. For $e \in \mathbf{F}_q$ we define

$$\mathbf{G}_e := \{x \in \mathbf{F}_{q^2} \mid x^q = x + e\}$$

and

$$\mathbf{T}_e := \{x \in \mathbf{F}_{q^2} \mid t_q(x) = e\}.$$

Note that $\mathbf{G}_0 = \mathbf{F}_q$, $\mathbf{F}_{q^2} = \mathbf{G}_0 \cup \mathbf{G}_1 \cup (\cup_{e \neq 0,1} \mathbf{G}_e)$, and $\mathbf{F}_q = \mathbf{T}_0 \cup \mathbf{T}_1$. Define the map $\tau : \mathbf{F}_{q^2} \cup \{\infty\} \to \mathbf{F}_{q^2} \cup \{\infty\}$ via

$$\tau(x) = x/(x+1).$$

We will denote the image $\tau(\mathbf{G}_e)$ of $\mathbf{G}_e$ under the map τ by $\mathbf{B}_e$. Finally, for any subset S of $\mathbf{F}_{q^2} \cup \{\infty\}$, we define $S^* := S \setminus \{0, \infty\}$ and $\tilde{S} := S \setminus \{0, 1\}$. It is not difficult to see that the definitions for $\mathbf{B}_0^*$ and $\mathbf{B}_1^*$ given earlier coincide with the definition of $\mathbf{B}_e^*$ for $e = 0, 1$ given here (see also Lemma 1).

We will be interested in the number of solutions $x \in \mathbf{F}_{q^2}$ of the equation

$$x^2 + (rst + r + s + t)x + rs + rt + st = 0, \tag{4}$$

where $s, t \in \mathbf{B}_0^* \cup \mathbf{B}_1^*$. It turns out that this equation can be transformed by some well-chosen substitutions into an 'equivalent' equation (that is, an equation having the same number of solutions) that is easy to deal with. Our approach is based on the following easily verified observation.

Lemma 1. *The map $\tau : x \mapsto x/(x+1)$ is 1-1 on $\mathbf{F}_{q^2} \cup \{\infty\}$, with $\tau(0) = 0$, $\tau(1) = \infty$, and $\tau(\infty) = 1$. Moreover, we have that*

(i) τ maps $\mathbf{G}_0 = \mathbf{F}_q$ to $\mathbf{B}_0 = (\mathbf{F}_q \cup \{\infty\}) \setminus \{1\}$, $\mathbf{G}_1$ to $\mathbf{B}_1 = \{x \in \mathbf{F}_{q^2} \mid x \neq 1, x^q = x^{-1}\}$, and $\mathbf{G}_e$ to $\mathbf{B}_e$, $e \neq 0, 1$.

Also, for all $e \in \mathbf{F}_q$, we have the following.

(ii) The set $\mathbf{T}_e$ (resp. $\mathbf{T}_e^*$) is the image of $\mathbf{G}_e$ (resp. $\tilde{\mathbf{G}}_e$) under the map $x \mapsto x^2 + x$, hence $\mathbf{T}_e \subseteq \mathbf{G}_{e^2+e}$.

(iii) The set $\mathbf{T}_e$ (resp. $\mathbf{T}_e^*$) is the image of $\mathbf{B}_e$ (resp. $\mathbf{B}_e^*$) under the map $x \mapsto 1/(x + x^{-1})$.

Now we proceed to evaluate $\pi_{i,j}(r)$ defined in (3). Note that since $\mathbf{F}_{q^2} = \cup_{e \in \mathbf{F}_q} \mathbf{G}_e$, we have

$$\mathbf{F}_{q^2} \setminus \{0, 1\} = \mathbf{B}_0^* \cup \mathbf{B}_1^* \cup \bigcup_{k \in \mathbf{F}_q \setminus \{0,1\}} \mathbf{B}_k^*.$$

So we may view the element r in the definition of $\pi_{i,j}(r)$ running through $\mathbf{B}_k^*$, $k \in \mathbf{F}_q$. When $r \in \mathbf{B}_k^*$, to emphasize the dependence of $\pi_{i,j}(r)$ on k, we write $\pi_{i,j}(r)$ as $\pi_{i,j}^k(r)$.

We now transform (4) into an equivalent equation which is easier to handle. Suppose that $s \in \mathbf{B}_i^*$, $t \in \mathbf{B}_j^*$, and $r \in \mathbf{B}_k^*$, where $i, j \in \{0, 1\}$ and $k \in \mathbf{F}_q$. Let $\alpha \in \tilde{\mathbf{G}}_i$, $\beta \in \tilde{\mathbf{G}}_j$, and $\gamma \in \tilde{\mathbf{G}}_k$ be such that

$$s = \alpha/(1+\alpha), \qquad t = \beta/(1+\beta), \qquad r = \gamma/(1+\gamma), \tag{5}$$

and define

$$a = \alpha^2 + \alpha, \qquad b = \beta^2 + \beta, \qquad c = \gamma^2 + \gamma. \tag{6}$$

Remark that by Lemma 1 this is possible, and $a \in \mathbf{T}_i^*$, $b \in \mathbf{T}_j^*$, and $c \in \mathbf{T}_k^*$; hence $a, b \in \mathbf{F}_q$ and $c \in \mathbf{G}_{k^2+k}$. Moreover, if s, t, and r run through $\mathbf{B}_i^*$, $\mathbf{B}_j^*$, and $\mathbf{B}_k^*$, then α, β, and γ run through $\tilde{\mathbf{G}}_i$, $\tilde{\mathbf{G}}_j$, and $\tilde{\mathbf{G}}_k$, respectively; moreover, a, b, and c run through $\mathbf{T}_i^*$, $\mathbf{T}_j^*$, and $\mathbf{T}_k^*$, and attain each element in these sets exactly twice.

Using (5), we find that

$$rst + r + s + t = (\alpha + \beta + \gamma)/\pi \tag{7}$$

and

$$rs + rt + st = (\alpha\beta\gamma + \alpha\beta + \alpha\gamma + \beta\gamma)/\pi, \tag{8}$$

where

$$\pi = (1+\alpha)(1+\beta)(1+\gamma) \neq 0. \tag{9}$$

So, if we multiply (4) by π^2, we obtain the equivalent equation

$$y^2 + (\alpha + \beta + \gamma)y = \pi(\alpha\beta\gamma + \alpha\beta + \alpha\gamma + \beta\gamma) \tag{10}$$

over $\mathbf{F}_{q^2}$. Next, we eliminate β from the right-hand side of (10). To this end, write

$$y = z + (\alpha + \gamma + \alpha\gamma)\beta + \alpha + \gamma. \tag{11}$$

After a tedious but routine computation, we obtain the equivalent equation

$$z^2 + (\alpha + \beta + \gamma)z = (1+\alpha)(1+\gamma)\alpha\gamma = (\alpha^2 + \alpha)c \tag{12}$$

over $\mathbf{F}_{q^2}$. From the above, we conclude that

$$\begin{aligned} \pi_{i,j}^k(r) &= \frac{1}{2} \sum_{\alpha \in \tilde{\mathbf{G}}_i} \sum_{\beta \in \tilde{\mathbf{G}}_j} |\{z \in \mathbf{F}_{q^2} \mid z^2 + (\alpha + \beta + \gamma)z = (\alpha^2 + \alpha)c\}| \\ &= -\theta(i, j, k) + \tilde{\pi}_{i,j}^k(r), \end{aligned} \tag{13}$$

where

$$\tilde{\pi}_{i,j}^k(r) = \frac{1}{2} \sum_{\alpha \in \mathbf{G}_i} \sum_{\beta \in \mathbf{G}_j} |\{z \in \mathbf{F}_{q^2} \mid z^2 + (\alpha + \beta + \gamma)z = (\alpha^2 + \alpha)c\}| \tag{14}$$

and $\theta(i, j, k)$ denotes the contribution to the sum (14) from α or β in $\{0, 1\}$.

First, we evaluate $\theta(i, j, k)$. To this end, note that for $\alpha \in \{0, 1\}$, Eqn (12) over $\mathbf{F}_{q^2}$ has exactly one solution if $\alpha + \beta + \gamma = 0$ and exactly two solutions otherwise. Moreover, due to symmetry the same statement holds for $\beta \in \{0, 1\}$. Using these observations, we find that

$$\begin{aligned} \theta(i, j, k) &= \frac{1}{2}\delta_{i,0} \sum_{\alpha \in \{0,1\}} \sum_{\beta \in \tilde{\mathbf{G}}_j} (2 - \delta_{\alpha+\beta+\gamma,0}) + \frac{1}{2}\delta_{j,0} \sum_{\alpha \in \mathbf{G}_i} \sum_{\beta \in \{0,1\}} (2 - \delta_{\alpha+\beta+\gamma,0}) \\ &= \delta_{i,0}(2|\tilde{\mathbf{G}}_j| - \delta_{j,k}) + \delta_{j,0}(2|\mathbf{G}_i| - \delta_{i,k}) \\ &= 2q(\delta_{i,0} + \delta_{j,0}) - 4\delta_{i,0}\delta_{j,0} - \delta_{i,0}\delta_{j,k} - \delta_{j,0}\delta_{i,k}, \end{aligned} \tag{15}$$

where $\delta_{u,v}$ is the Kronecker Delta function, i.e., $\delta_{u,v} = 1$ if $u = v$, and $\delta_{u,v} = 0$ if $u \neq v$.

Next, we evaluate $\tilde{\pi}^k_{i,j}(r)$. Define

$$H := \{x^2 + x \mid x \in \mathbf{F}_{q^2}\} = \{y \in \mathbf{F}_{q^2} \mid \mathrm{Tr}_{q^2}(y) = 0\}, \tag{16}$$

and write $e = i + j + k$. We have that

$$\begin{aligned}\tilde{\pi}^k_{i,j}(r) &= \frac{1}{2}\sum_{\alpha\in\mathbf{G}_i}\sum_{\beta\in\mathbf{G}_j} |\{z \in \mathbf{F}_{q^2} \mid z^2 + (\alpha+\beta+\gamma)z = (\alpha^2+\alpha)c\}| \\ &= \sum_{\sigma\in\mathbf{G}_e} |\{z \in \mathbf{F}_{q^2} \mid z^2 + \sigma z \in c\mathbf{T}_i\}| \\ &= \frac{q}{2}\delta_{e,0} + 2\sum_{\sigma\in\mathbf{G}^*_e} |H \cap (c/\sigma^2)\mathbf{T}_i|. \end{aligned} \tag{17}$$

We will use the following observation.

LEMMA 2. *Let $\lambda \in \mathbf{F}^*_{q^2}$ and $i \in \{0, 1\}$. Then*

$$|H \cap \lambda\mathbf{T}_i| = \begin{cases} q/2, & \text{if } \lambda \in \mathbf{G}_0; \\ \frac{q}{2}\delta_{i,0}, & \text{if } \lambda \in \mathbf{G}_1; \\ q/4, & \text{otherwise.} \end{cases} \tag{18}$$

PROOF. Let $a \in \mathbf{T}_i$. We have that $\lambda a \in H$ if and only if $\mathrm{Tr}_{q^2}(\lambda a) = \mathrm{Tr}_q((\lambda + \lambda^q)a) = 0$, that is, if and only if $\lambda \in \mathbf{G}_0 = \mathbf{F}_q$ or $(\lambda + \lambda^q)a \in \mathbf{T}_0$. So if $\lambda \in \mathbf{G}_0$ and $\lambda \neq 0$, then $|H \cap \lambda\mathbf{T}_i| = |\mathbf{T}_i| = q/2$, and if $\lambda \notin \mathbf{G}_0$, then $|H \cap \lambda\mathbf{T}_i| = |\mathbf{T}_0 \cap \mu\mathbf{T}_i|$, where $\mu = \lambda + \lambda^q$.

Now both $\mathbf{T}_0$ and $\mu\mathbf{T}_0$ are $\mathbf{F}_2$-linear subspaces of $\mathbf{F}_q$, of dimension $m - 1$ if $q = 2^m$, and $\mathbf{T}_1 = \mathbf{F}_q \setminus \mathbf{T}_0$. So either $\mathbf{T}_0$ and $\mu\mathbf{T}_0$ are equal, or $|\mathbf{T}_0 \cap \mu\mathbf{T}_i| = q/4$. It is well-known that $\mathbf{T}_0 = \mu\mathbf{T}_0$ only if $\mu = 1$ (indeed, note that $\mathbf{T}_0$ is the Singer difference set in $\mathbf{F}_q$), so the result follows. □

In order to use Lemma 2 to evaluate (17), we need to determine when $c/\sigma^2 \in \mathbf{G}_0$ and when $c/\sigma^2 \in \mathbf{G}_1$. To this end, let $\lambda = c/\sigma^2$, where $c \in \mathbf{T}^*_k \subseteq \mathbf{G}_{k^2+k} = \mathbf{G}_{e^2+e}$, $\sigma \in \mathbf{G}^*_e$, and put

$$\mu = \mu(\sigma) = \lambda + \lambda^q = e(ce + \sigma^2(e+1))/(\sigma^4 + e^2\sigma^2). \tag{19}$$

We determine when $\mu = 0$ and when $\mu = 1$. Solving these equations for σ produces the following result.

LEMMA 3. *Let $i, j \in \{0, 1\}$, $k \in \mathbf{F}_q$, $e = i + j + k$, and suppose that $c = \gamma^2 + \gamma$ with $\gamma \in \tilde{\mathbf{G}}_k$. Let μ be defined as above.*

(i) We have that $\mu = 0$ if and only if $e = 0$ or $e \neq 0, 1$, $\sigma = (ec/(e+1))^{1/2} \in \mathbf{G}_e$;

(ii) we have that $\mu = 1$ if and only if $e \neq 0$ and $\sigma^2 \in \{e\gamma, e(\gamma+1)\}$; these solutions σ are in $\mathbf{G}_e$ if and only if $k = e$, that is, $i = j$.

A straightforward application of the above results now shows that

$$\tilde{\pi}^k_{i,j}(r) = \begin{cases} q(2q-1)/2, & \text{if } e = 0; \\ 2q\delta_{i,0} + q(q-2)/2, & \text{if } e = 1 \text{ and } i = j; \\ q^2/2, & \text{if } e = 1 \text{ and } i \neq j; \\ 2q\delta_{i,0} + q(q-1)/2, & \text{if } e \neq 0, 1 \text{ and } i = j; \\ q(q+1)/2, & \text{if } e \neq 0, 1 \text{ and } i \neq j. \end{cases} \tag{20}$$

Combining (13), (15), and (20), we see that for $i, j \in \{0, 1\}$, the number $\pi_{i,j}^k(r)$ does not depend on the choice of $r \in \mathbf{B}_k^*$ and in fact only depends on whether $k = 0$, $k = 1$, or $k \in \mathbf{F}_q \setminus \{0, 1\}$. So indeed $\mathcal{S}(q^2 + 1)$ defined in Section 1 is a four- class scheme, and the intersection numbers are as follows.

For the cases where $e = i + j + k = 0$, we obtain that

$$p_{22}^2 = (2q^2-9q+12)/2, \qquad p_{33}^2 = q(2q-1)/2, \qquad p_{23}^3 = p_{32}^3 = (q-2)(2q-1)/2. \quad (21)$$

Here, for example, $p_{22}^2 = \pi_{0,0}^0(r) = |\{z \mid (x, z) \in S_2 \text{ and } (z, y) \in S_2\}|$ for any pair $(x, y) \in S_2$.

For the cases where $e = i + j + k = 1$, we obtain that

$$p_{22}^3 = (q-2)(q-4)/2, \qquad p_{23}^2 = p_{32}^2 = q(q-4)/2, \qquad p_{33}^3 = q(q-2)/2. \quad (22)$$

Finally, for the cases where $e = i + j + k \neq 0, 1$, we obtain that

$$p_{22}^4 = (q^2 - 5q + 8)/2, \qquad p_{23}^4 = p_{32}^4 = q(q-3)/2, \qquad p_{33}^4 = q(q-1)/2. \quad (23)$$

The existence of these intersection numbers together with the existence of the valencies is sufficient to conclude that all other intersection numbers also exist and enables us to compute them. It is then an easy exercise to compute the P-matrix of the four-class scheme and to verify that this P-matrix is indeed as given in [3].

We remark that there is an even more direct way to obtain (21). Indeed, let

$$f = f(r, s, t) = (rs + rt + st)/(rst + r + s + t)^2. \quad (24)$$

We claim that $\mathrm{Tr}_{q^2}(f) = 0$ if $i + j + k = 0$ and $rst + r + s + t \neq 0$. This is obvious if $r, s, t \in \mathbf{B}_0^*$ (since then $f \in \mathbf{F}_q$). Otherwise, due to the symmetry of f we may assume without loss of generality that $r \in \mathbf{B}_0^*$, $s, t \in \mathbf{B}_1^*$. Then $r^q = r$, $s^q = s^{-1}$, $t^q = t^{-1}$, and a routine computation shows that $f^q + f = g^2 + g$, where

$$g = (s + t)/(rst + r + s + t). \quad (25)$$

A second routine computation shows that $g^q = g$, so $g \in \mathbf{F}_q$; hence $\mathrm{Tr}_{q^2}(f) = \mathrm{Tr}_q(f^q + f) = \mathrm{Tr}_q(g^2 + g) = 0$ as claimed.

Now note that if $rst + r + s + t \neq 0$, then the number of solutions to (4) over $\mathbf{F}_{q^2}$ equals $1 + (-1)^{\mathrm{Tr}_{q^2}(f)} = 2$ by our claim and so the numbers $\pi_{i,j}(r)$ (and hence the numbers in (21)) can easily be computed directly from their definition (3). Further details are left to the reader.

3. Conclusions

We have shown that fusion of relations as proposed in [3] indeed produces a four-class association scheme, whose P-matrix is the one given there. This P-matrix reveals that further fusion of the relations S_1, S_2 and S_3 produces a strongly regular graph. We remark that in contrast to the suggestion in [3], this graph is isomorphic to the Brouwer-Wilbrink graph. This is shown both in [2] and in [4]; moreover, in [4] it is shown that a similar fusion process in a related scheme produces first a three-class scheme, then a renewed fusion produces a strongly regular graph isomorphic to the Metz graph (for these two srgs, see e.g. [1]).

Acknowledgement

We wish to thank Edwin van Dam for pointing out an omission in an earlier version of our proof.

REFERENCES

1. A. E. Brouwer and J. H. van Lint, Strongly regular graphs and partial geometries, in: *Enumeration and Design*, Part 7, D. M. Jackson and S. A. Vanstone (eds), Academic Press, Toronto, 1984, pp. 85–122.
2. G. Ebert, S. Egner, H. D. L. Hollmann and Q. Xiang, On a four-class association scheme, *J. Comb. Theory, Ser. A*, **96** (2001), 180–191.
3. D. de Caen and E. R. van Dam, Fissioned triangular schemes via the cross-ratio, *Europ. J. Combinatorics*, **22** (2001), 297–301.
4. H. D. L. Hollmann, Association schemes from the action of PSL$(2, 2^m)$ fixing an oval in PG$(2, 2^m)$ and their fusion schemes, preprint.
5. H. Tanaka, A four-class subscheme of the association scheme coming from the action of PGL$(2, 4^f)$, preprint.

Received 6 November 2000 and accepted 15 May 2001

GARY L. EBERT
Department of Mathematical Sciences,
University of Delaware,
Newark,
DE 19716, U.S.A.
E-mail: ebert@math.udel.edu

SEBASTIAN EGNER AND HENK D. L. HOLLMANN
Philips Research Laboratories,
Prof. Holstlaan 4,
5656 AA Eindhoven,
The Netherlands
E-mail: sebastian.egner@natlab.research.philips.com

AND

QING XIANG
Department of Mathematical Sciences,
University of Delaware,
Newark,
DE 19716, U.S.A.
E-mail: xiang@math.udel.edu