Received: 30 October 2017 | Revised: 31 May 2018 | Accepted: 2 June 2018
DOI: 10.1002/jcd.21611

WILEY

RESEARCH ARTICLE

# Character tables and the problem of existence of finite projective planes

Máté Matolcsi[1,2] | Mihály Weiner[1]

[1]Department of Analysis, Budapest University of Technology and Economics (BME), H-1111, Egry J. u. 1, Budapest, Hungary

[2]Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, H-1053, Realtanoda u 13-15, Budapest, Hungary

**Correspondence**
Máté Matolcsi, Budapest University of Technology and Economics (BME), H-1111, Egry J. u. 1, Budapest, Hungary.
Email: matomate@renyi.hu

**Funding information**
Országos Tudományos Kutatási Alapprogramok, Grant/Award Numbers: K109789, K124152; FP7 Ideas: European Research Council, Grant/Award Numbers: ERC-AdG 321104, ERC-AdG 669240

Contract grant sponsor: ERC-AdG 321104; contract grant sponsor: NKFIH-OTKA; contract grant number: K109789 (to M.M.). Contract grant sponsor: ERC-AdG 669240; contract grant sponsor: NKFIH-OTKA; contract grant number: K124152 (to M.W.).

**Abstract**
We use the connection between positive definite functions and the character table of the symmetric group $S_6$ to give a short new proof of the nonexistence of a finite projective plane of order 6. For higher orders, like 10 and 12, the method seems to be inconclusive as of now, but could be a basis of further research.

**KEYWORDS**
character table, delsarte LP-bound, finite projective planes

**MSC 2010:**
Primary 05B10, Secondary 20C15, 05B25

## 1 | INTRODUCTION

In a recent paper [8] the authors (jointly with M. N. Kolountzakis) introduced a version of the Delsarte LP-bound on noncommutative groups and applied it to the problem of mutually unbiased bases. Here, we build on these ideas and investigate the existence of finite projective planes of a given order $d$. The method yields an elegant new proof of nonexistence for order 6, and could be a basis of future research for higher orders.

We begin by shortly describing the general background of what we call the Delsarte LP method on a group. Given a finite group $G$ and a symmetric set $A = A^{-1} \subset G$ (sometimes referred to as the "forbidden set"), what is the maximal cardinality of a subset $B = \{b_1, \dots, b_n\} \subset G$, such that all "differences"$b_j^{-1} b_k$ $(j \neq k)$ fall into $A^c$, the complement of $A$? This is a very general type of question and many famous problems can be rephrased in this manner. In many applications $G$ is not finite, e.g. $G = \mathbb{R}^n$ but we will only consider finite groups in this note.

The Delsarte LP-bound has often proved fruitful when dealing with such problems, e.g. in the context of sphere-packing [2,16] or in the maximum number of code-words in error correcting codes [3]. It is based on the observation that the function $1_B * 1_{B^{-1}}$ is positive definite on the group $G$. A Fourier-analytic formulation of the method over *commutative groups* was described in [9], and the authors used it to give computer-aided proofs for some existence and uniqueness results about finite projective planes of small orders [10]. A recent version over *noncommutative groups* was given by the authors (jointly with M. N. Kolountzakis) in [8, Theorem 2.3], based on previous work of F. M. Oliveira de Filho and F. Vallentin [11, Theorem 2]. We will build on these ideas here, but will not directly use any of the mentioned results to keep this short note self-contained.

For primepower orders, projective planes can be constructed using finite fields. Some other constructions—not based on finite fields—are also known. However, it is widely believed that finite projective planes do not exist if the order is not a primepower. In the beginning of the XX. century, Tarry [15] proved that there exists no $6 \times 6$ Greco-Latin square, which is a stronger statement than the nonexistence of a finite projective plane of order 6. However, his proof is based on a rather tedious checking of each $6 \times 6$ Latin square. Some 40 years later, Bruck and Ryser [1] proved the celebrated result that if a finite projective plane of order $d \equiv 1, 2 \bmod(4)$ exists, then $d$ must be a sum of two squares. This result rules out an infinite family of nonprimepower orders (including 6, again), but leaves the problem open for orders such as $d = 10$ or $d = 12$. Other proofs for the case $d = 6$ were later given by Stinson [14] and Dougherty [4]. As of today, for $d = 10$ we only know the nonexistence of a finite projective plane due to a massive computer search [7], and the question is still open for $d = 12$. In this paper, we present a short new proof of nonexistence for $d = 6$, which may shed new light on the problem.

In order to use Delsarte's LP method we reformulate the existence of a projective plane of order $d$ in terms of the existence of a certain family of permutations in the symmetric group $S_d$. This reformulation is well-known but we include it here for completeness.

Instead of finite projective planes, we may work with some equivalent structures like that of finite affine planes or complete sets of mutually orthogonal Latin squares. For our purposes, we shall depart from a finite affine plane of order $d$. We fix and enumerate the lines of two of its parallel equivalence classes so that we have a "coordinate system" in our plane. We will call these parallel classes "horizontal" and "vertical." As any further line $\ell$ intersects each horizontal and vertical line exactly once, we can view $\ell$ as the graph of a bijective function $\{1, 2 \ldots, d\} \to \{1, 2 \ldots, d\}$; that is, an element of the permutation group $S_d$. In this way, the remaining $(d-1)d$ lines of the affine plane are encoded in $(d-1)d$ permutations $\sigma_1, \sigma_2, \ldots, \sigma_{(d-1)d} \in S_d$. Note that two distinct lines $\ell_j, \ell_k$ are parallel if and only if $\sigma_j^{-1}\sigma_k$ has no fixed points, whereas they intersect each other if and only if $\sigma_j^{-1}\sigma_k$ has precisely one fixed point.

Therefore, the question arises: what is the maximal cardinality of a subset

$B = \{\sigma_1, \ldots, \sigma_M\} \subset S_d$ such that all the "differences" $\sigma_j^{-1}\sigma_k$ between any two distinct elements $\sigma_j, \sigma_k \in B$ has zero or one fixed point. In other words, using the terminology above, the forbidden set $A$ consists of permutations with more than one fixed points. As we have seen, if the maximal number $M$ is strictly less than $(d-1)d$ then there can be no projective plane of order $d$. Note also, that we actually have more information about the permutations $\sigma_j$ than just the fact that the differences must avoid the forbidden set $A$. If we assume that $B = \{\sigma_1, \ldots, \sigma_{(d-1)d}\} \subset S_d$ comes from an affine plane of order $d$, then we can tell exactly how many of the differences have one fixed point and how many of them have none. We will make use of this fact.

The version of the Delsarte LP-bound presented in [8] involves general positive definite functions on $G$. In our present case, however, the forbidden set $A$ is invariant under conjugations. As a consequence, it suffices to consider positive definite functions that are also *class-functions*; i.e. ones that take constant values on each conjugacy class. For this reason, rather than recalling the general result from [8], we shall give a self-contained presentation here directly formulated in terms of class-functions and characters.

Assuming that $B = \{\sigma_1, \dots, \sigma_{(d-1)d}\} \subset S_d$ comes from an affine plane of order $d$, our method gives a system of linear equations and inequalities regarding the number of differences $\sigma_i^{-1}\sigma_j$ falling in each conjugacy class of $S_d$. For $d = 6$ this linear system has a unique solution. However, some easy combinatorial arguments show that this unique solution *cannot* correspond to a finite projective plane, thus proving the nonexistence result.

This can all be checked by hand because the character table of $S_d$ is well known (described by the the so-called *Murnaghan-Nakayama rule*; see e.g. in the book [13]), and because $S_6$ has only 11 conjugacy classes, and hence we have a rather small linear system to solve. For $d = 12$, $S_d$ has already 77 conjugacy classes and a similar computation by hand would be extremely cumbersome. Nevertheless, using a computer it easy to solve the arising linear programming problem, and we went ahead and tried out what happens up to $d = 12$. We found that for $d \leq 6$ there is a unique solution, but uniqueness breaks down starting from $d = 7$ — even though up to equivalence, there is a unique projective plane of order seven [5,10,12]. The space of solutions is always a convex body, and for $d = 12$ our task would be to use some combinatorial arguments to conclude that no points within this convex body can correspond to a finite projective plane. As of today, we cannot conclude non-existence by this method for any $d > 6$. Nevertheless, we still hope that the information given by our linear system of equations will turn out to be useful for higher orders in the future.

## 2 | CHARACTER TABLES AND A NONEXISTENCE RESULT FOR $d = 6$

Let $G$ be a finite group with conjugacy classes $C_0 = \{e\}, C_1 \dots, C_r$ and let $\gamma$ be the function assigning to each element the cardinality of the conjugacy class it is contained in: $\gamma(g) = |C_k|$ for all $g \in C_k$.. Sometimes we use the following shorthand notation for this:

$$\gamma|_{C_k} = |C_k| \ \ (k = 0, \dots, r).$$

For $B = \{b_1, \dots, b_n\} \subset G$ we shall consider the class-function $\theta_B$ counting the number of times the difference between elements of $B$ falls in a certain conjugacy class; that is, $\theta_B(g) = |\{(j,m)|b_j^{-1}b_m \in C_k\}|$ for all $g \in C_k$. In shorthand notation

$$\theta_B|_{C_k} = |\{(j,m)|b_j^{-1}b_m \in C_k\}| \ \ (k = 0, \dots, r).$$

Note that $\theta_B$ takes nonnegative values (actually: nonnegative *integer* values), $\theta_B(e) = |B| = n$ and as there are $n^2$ differences altogether, we also have that $\sum_{g\in G} \frac{\theta_B(g)}{\gamma(g)} = |B|^2 = n^2$. Apart from these obvious properties, our main observation is the following.

**Proposition 2.1.** *For any character $\chi$ of $G$, the value of the scalar product*

$$\langle \chi, (\theta_B/\gamma)\rangle \equiv \frac{1}{|G|}\sum_{g\in G} \overline{\chi(g)}\frac{\theta_B(g)}{\gamma(g)}$$

*between $\chi$ and the class-function $\theta_B/\gamma$ is a nonnegative real. Hence $\theta_B/\gamma$ is a linear combination of the irreducible characters of G with nonnegative coefficients.*

*Proof.* It is clearly enough to prove the first statement; as the irreducible characters form an orthonormal bases in the space of class-functions, the value of the scalar product in question is precisely the coefficient of $\theta_B/\gamma$ in this basis corresponding to $\chi$. Now let $U$ be the representation giving $\chi$. As $G$ is finite, we may safely assume that $U$ is actually a unitary representation. Then setting $X = \sum_{j=1}^{n} U(b_j)$, we have

$$\begin{aligned} |G|\,\overline{\langle \chi, (\theta_B/\gamma)\rangle} &= \sum_{g\in G} \chi(g)\frac{\theta_B(g)}{\gamma(g)} = \sum_{k=0}^{r} \left(\chi\,\theta_B\right)|_{C_k} = \sum_{k=0}^{r} \chi|_{C_k}\,|\{(j,m)|b_j^{-1}b_m \in C_k\}| \\ &= \sum_{j,m=1}^{n} \chi(b_j^{-1}b_m) = \sum_{j,m=1}^{n} \mathrm{Tr}(U(b_j^{-1}b_m)) \\ &= \sum_{j,m=1}^{n} \mathrm{Tr}(U(b_j)^* U(b_m)) = \mathrm{Tr}\left(X^*X\right) \geq 0, \end{aligned} \tag{1}$$

showing the nonnegativity of the scalar product in question. □

Now let us consider the case when $G = S_d$ and the subset $B = \{\sigma_1, \ldots, \sigma_{(d-1)d}\}$ is given by an affine plane of order $d$ as explained in the introduction. Out of the total of $((d-1)d)^2$ differences between the elements of $B$, $(d-1)d$ give the identity (as a difference between an element and itself), $(d-1)^2 d$ have no fixed points (corresponding to distinct parallel lines) and $(d-2)(d-1)d^2$ have one fixed point (corresponding to distinct nonparallel lines). Thus, denoting by $\mathcal{S}_j$ the collection of conjugacy classes of $S_d$ containing permutations with $j = 0, 1, \ldots, d$ fixed points, we have the linear equations

$$\begin{cases} \forall C \notin (\{e\}\cup \mathcal{S}_0 \cup \mathcal{S}_1): & \theta_B|_C = 0, \\ & \theta_B(e) = (d-1)d, \\ & \sum_{C\in\mathcal{S}_0} \theta_B|_C = (d-1)^2 d, \\ & \sum_{C\in\mathcal{S}_1} \theta_B|_C = (d-2)(d-1)d^2. \end{cases} \tag{2}$$

We also have the linear inequalities given by our previous proposition and the noted fact that $B$ takes nonnegative values only:

$$\begin{cases} & \forall C: \quad \theta_B|_C \geq 0, \\ \forall\chi \text{ irr. char.}: & \sum_C (\chi\theta_B)|_C \geq 0. \end{cases} \tag{3}$$

We view this linear system as a restriction on possible functions $\theta_B$. Note that we dropped the conjugation signs as both $\theta_B$ and $\chi$ are real-valued functions: a particular feature of the permutation group is that all of its characters are real-valued.

In particular, let us now consider the case $d = 6$. $S_6$ has 11 conjugacy classes, of which 2 are in $\mathcal{S}_1$ and 4 in $\mathcal{S}_0$. Since we do not need permutations with 2, 3, or 4 fixed points (as $\theta_B$ is constant zero over them), the following shortened version of the character table of $S_6$ will be sufficient for us:

| | e | (123)(456) | (12)(34)(56) | (1234)(56) | (123456) | (123)(45) | (12345) |
|---|---|---|---|---|---|---|---|
| | | $\mathcal{S}_0$ | | | | $\mathcal{S}_1$ | |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | -1 | 1 | -1 | -1 | 1 |
| $\chi_3$ | 5 | -1 | -1 | -1 | -1 | 0 | 0 |
| $\chi_4$ | 5 | -1 | 1 | -1 | 1 | 0 | 0 |
| $\chi_5$ | 5 | 2 | 3 | -1 | 0 | -1 | 0 |
| $\chi_6$ | 5 | 2 | -3 | -1 | 0 | 1 | 0 |
| $\chi_7$ | 9 | 0 | 3 | 1 | 0 | 0 | -1 |
| $\chi_8$ | 9 | 0 | -3 | 1 | 0 | 0 | -1 |
| $\chi_9$ | 10 | 1 | 2 | 0 | -1 | 1 | 0 |
| $\chi_{10}$ | 10 | 1 | -2 | 0 | 1 | -1 | 0 |
| $\chi_{11}$ | 16 | -2 | 0 | 0 | 0 | 0 | 1 |
| $\theta_B$ | 30 | $x$ | $y$ | $z$ | $v$ | $a$ | $b$ |
| | | 150 | | | | 720 | |

In the last line we put (as parameters) the values of the function $\theta_B$, already indicating the system (2) of equalities; namely, that $\theta_B(e) = 5 * 6 = 30$, $x + y + z + v = 5^2 * 6 = 150$ and $a + b = 4 * 5 * 6^2 = 720$. What remains is to make use of the inequalities (3), which tell us that all parameters $x, y, z, v, a, b$ as well as the scalar product of the last line of the table (corresponding to $\theta_B$) with any other line is nonnegative.

In particular, considering that the sum of the lines corresponding to the characters $\chi_5, \chi_7, \chi_8$ and $\chi_{10}$ is $(33, 3, 1, 1, 1, -2, -2)$, we have the inequality:

$$33 * 30 + 3x + y + z + v - 2a - 2b = 990 + 2x + (x + y + z + v) - 2(a + b) \geq 0. \tag{4}$$

Thus, as $x + y + z + v = 150$ and $a + b = 720$, we have that $990 + 2x + 150 - 2 * 720 \geq 0$ that results in $x \geq 150$. On the other hand, $x$ is *at most* 150, as $x + y + z + v = 150$. Hence we must have $x = 150$ and $y = z = v = 0$. Then the scalar product with the lines corresponding to $\chi_5$ and $\chi_7$ can be simplified resulting in the inequalities

$$5 * 30 + 2 * 150 - a \geq 0, \quad 9 * 30 - b \geq 0. \tag{5}$$

Hence $a \leq 450$ and $b \leq 270$. But $a + b = 720$, and hence $a = 450, b = 270$ follows. Therefore, the unique solution is:

$$x = 150, y = 0, z = 0, v = 0, a = 450, b = 270. \tag{6}$$

It is easy to check that these values indeed give a solution that satisfy all nonnegativity constraints. The main point is that the arguments above show that this solution is *unique*. We now use some combinatorial arguments to show that this solution cannot correspond to a finite projective plane of order 6.

**Proposition 2.2.** *There exists no finite projective plane of order 6.*

*Proof.* Assume that there exists a projective—and hence also an affine —plane of order $d = 6$. Then, as explained there should exist a collection of $5 * 6 = 30$ permutations $B = \{\sigma_1, \dots, \sigma_{30}\} \subset S_6$ describing the lines of $d - 1 = 5$ parallel classes of our affine plane, with corresponding "difference-counting" function $\theta_B$ given by (6). In particular, out of the total 900 differences, 450 should be of negative parity. This is only possible, if half of our permutations (i.e. 15 out of the 30) are of positive, and half are of negative parity (forming $30 * 15 = 450$ ordered pairs with opposing signs); in any other case there would be fewer differences of negative parity. However, as $y = v = 0$, all differences with zero fixed points are of positive parity and hence the permutations corresponding to the lines of a single parallel class should have the same sign. Thus, the number of elements in $B$ with positive parity should be divisible by 6 (as each parallel class contains six lines), which contradicts to what we established earlier; namely, that precisely 15 of the elements of $B$ should have positive parity. □

In conclusion, we remark that the proof relies heavily on the fact that the solution (6) is *unique*. We could then exclude this unique solution by some further combinatorial arguments. However, for $d > 6$ the solution space of our linear system (2), (3) is a convex body (not just a single point), and as of now we are unable to exclude all points of this body to prove nonexistence results for e.g. $d = 10$ or 12.

## ACKNOWLEDGMENTS

The authors are grateful for the referees for their valuable suggestions that have helped to improve the presentation of the paper.

## ORCID

*Máté Matolcsi* http://orcid.org/0000-0003-4889-697X

## REFERENCES

[1] R. H. Bruck and H. J. Ryser, *The non-existence of certain projective planes*, Can. J. Math. **1** (1949), 88–93.

[2] H. Cohn and N. Elkies, *New upper bounds on sphere packings I*, Ann. Math. **157** (2003), no. 2, 689–714.

[3] P. Delsarte, *Bounds for unrestricted codes, by linear programming*, Philips Res. Rep. **27** (1972), 272–289.

[4] S. T. Dougherty, *A coding theoretic solution to the 36 officer problem*, Designs, Codes Cryptogr. **4** (1994), 123–128.

[5] M. Hall (Jr.), *Uniqueness of the projective plane with 57 points*, Proc. Amer. Math. Soc. **4** (1953), 912–916; Correction to "Uniqueness of the projective plane with 57 points," Proc. Amer. Math. Soc. **5** (1954), 994–997.

[6] A. Kabatiansky and V. I. Levenshtein, *Bounds for packings on a sphere and in space*, Problems Inform. Trans. **14** (1978), 1–17.

[7] C. W. H. Lam, L. Thiel and S. Swiercz, *The non-existence of finite projective planes of order 10*, Can. J. Math. **XLI** (1989), 1117–1123.

[8] M. N. Kolountzakis, M. Matolcsi and M. Weiner, *An application of positive definite functions to the problem of MUBs*, Proc. Amer. Math. Soc. **146** (2018), 1143–1150.

[9] M. Matolcsi and I. Z. Ruzsa, *Difference sets and positive exponential sums I, General properties*, J. Fourier Anal. Appl. **20** (2014), 17–41.

[10] M. Matolcsi and M. Weiner, *Finite projective planes and the Delsarte LP-bound*, Anal. Math. **44** (2018), 89–98.

[11] F. M. Oliveira de Filho and F. Vallentin, *Mathematical optimization for packing problems*, SIAG/OPT Views News **23** (2015), 5–14.

[12] W. A. Pierce, *The impossibility of Fano's configuration in a projective plane with eight points per line*, Proc. Amer. Math. Soc. **4** (1953), 908–912.

[13] R. P. Stanley, Enumerative combinatorics. Volume 2, Cambridge University Press, Cambridge, 1999, xii+581 pp.

[14] D. R. Stinson, *A short proof of the nonexistence of a pair of orthogonal Latin squares of order six*, J. Combin. Theory Ser. A **36** (1984), 373–376.

[15] G. Tarry, *Le problème des 36 officiers*, C. R. Assoc. Fran. Av. Sci. **1** (1900), 122–123, **2** (1901), 170–203.

[16] M. Viazovska, *The sphere packing problem in dimension 8*, Annal. Math. **185** (2017), 991–1015.

**How to cite this article:** Matolcsi M, Weiner M. Character tables and the problem of existence of finite projective planes. *J Combin Des*. 2018;26:540–546. https://doi.org/10.1002/jcd.21611