

CHARACTER TABLES AND THE PROBLEM OF EXISTENCE OF FINITE PROJECTIVE PLANES

MÁTÉ MATOLCSI AND MIHÁLY WEINER

ABSTRACT. Recently, the authors of the present work (together with M.N. Kolountzakis) introduced a new version of the non-commutative Delsarte scheme and applied it to the problem of mutually unbiased bases. Here we use this method to investigate the existence of a finite projective plane of a given order d . In particular, a short new proof is obtained for the nonexistence of a projective plane of order 6. For higher orders like 10 and 12, the method is non decisive but could turn out to give important supplementary informations.

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

Keywords: *non-commutative Delsarte scheme, character table, finite projective planes*

1. INTRODUCTION

Given a group G and a “forbidden set” $A = A^{-1} \subset G$, at most how many elements a subset $B = \{b_1, \dots, b_n\} \subset G$ can have, if all “differences” $b_j^{-1}b_k$ ($j \neq k$) “avoid” A ? This is a very general type of question; many famous problems can be re-phrased in this manner.

A method that often proved to be fruitful when dealing with such problems — e.g. in the context of sphere-packing [5, 2] or in the maximum number of code-words [3] — is the Fourier-analytical approach first pioneered by Delsarte [3] in the commutative case. Later Oliveira Filho and Vallentin proved the optimization bound [8, Theorem 2], which can be viewed as a generalization of Delsarte’s method that includes the non-commutative case. Recently, together with Kolountzakis, the authors of this work presented another non-commutative Delsarte-scheme [7], which they applied to the famous quantum physically motivated question regarding the existence of complete collections of mutually unbiased bases in \mathbb{C}^d . Since there are many indications pointing to some relation between this question and that of the existence of a projective plane of order d , it seems natural to also re-phrase and investigate this latter problem in the above manner.

For any prime-power order, at least one projective plane can be constructed using finite fields. However, although there are also other constructions, so far no one has managed to present a projective plane with a non prime-power order and in fact it is widely believed that there are no such planes. In the beginning of the XX. century, Tarry [11] proved that there is no 6×6 Greco-Latin square, which is actually a stronger statement than the nonexistence of a finite projective plane of order 6. However, his proof is not so instructing, as it is based on a rather tedious hand-checking of each 6×6 Latin square. Then some 40

M. Matolcsi was supported by the ERC-AdG 321104, M. Weiner was supported by the ERC-AdG 669240 QUEST “Quantum Algebraic Structures and Models” and by OTKA Grant NKFI K 124152.

years later, Bruck and Ryser [1] proved that if a finite projective plane of order $d \equiv 1, 2 \pmod{4}$ exists, then d must be a sum of two squares. This again rules out the existence of a finite projective plane of order 6 (and of course many other orders, too), but leaves open the question for the next two non prime-powers: $d = 10$ and $d = 12$. For $d = 10$ we only know the nonexistence because of a massive computer search [6], and for $d = 12$, the question is still open.

Although the argument of Bruck and Ryser is elegant, their proof is certainly not one of those that can be digested in 5 minutes. Thus, up to now, even for the smallest non prime-power order — i.e. for $d = 6$ — there was no easily presentable, short argument for the nonexistence in question; hence we felt that there was room here for yet another proof.

Let us shortly see now how the existence of projective planes of a given order d can be investigated in a Delsarte scheme. Instead of finite projective planes, one may work with some equivalent structures like that of finite affine planes or complete sets of mutually orthogonal Latin squares. For our purpose 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” on our plane. As any further line intersects each “horizontal” and “vertical” line exactly once, we can view each such line as the graph of a bijective function $\{1, 2 \dots d\} \rightarrow \{1, 2 \dots d\}$; 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 $\sigma_1, \sigma_2, \dots, \sigma_{(d-1)d} \in S_d$. Then σ_j and σ_k stand for two (different) parallel (i.e. non-intersecting) lines if and only if $\sigma_j^{-1}\sigma_k$ has no fixed points, whereas if they are from different parallel classes, then — as they must intersect in exactly one point — $\sigma_j^{-1}\sigma_k$ must have precisely one fixed point. So one may ask: at most how large a subset $B \subset S_d$ can be so that the difference $\sigma^{-1}\tilde{\sigma}$ between any two different elements $\sigma, \tilde{\sigma} \in B$ “avoids” the forbidden set A consisting of permutations with more than one fixed points? As we have seen, if this number is less than $(d - 1)d$, then there can be no projective plane of order d .

Note that actually we have more information than just the fact that the differences must avoid the forbidden set A . If we assume that $B = \{\sigma_1, \dots, \sigma_{(d-1)d}\} \subset S_d$ comes from an affine plane of order d , then, apart from saying that the differences are not in A , we can even tell how many of the differences have one fixed point and how many of them have zero. In our proof of nonexistence, we shall also make use of such finer details.

The Delsarte scheme recently presented in [7] involves general positive (semi)definite functions on G . Now in our present case — in contrast with the cited work — the forbidden set A is invariant under conjugations. As a consequence, it suffices to consider positive semidefinite functions that are also *class-functions*; i.e. ones that take constant values inside each conjugacy class. However, using representation theory, it is a rather easy exercise to show that if G is a finite group and $h : G \rightarrow \mathbb{C}$ is a class-function, then h is positive semidefinite if and only if it is a linear combination of the irreducible characters of G with nonnegative coefficients only. For this reason — and also for self-containment — rather than recalling the mentioned recently introduced general method (involving positive semidefinite functions), here we shall give a presentation 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 , — as we shall see in the next section — our method gives a system of linear equations and inequalities regarding the number of differences (between different elements of B) falling in each conjugacy class of S_d . However, in general one can easily find some further conditions that are somehow not “recognized” by our method; e.g. that these numbers must be all even integers. So, although for $d = 6$ our linear system does have a — unique — solution, we could then easily conclude the nonexistence of a finite projective plane of order 6.

This can all be done on a small piece of paper because of two reasons. First, 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 [10]), second, because in the $d = 6$ case, S_d has only 11 conjugacy classes and hence we have a rather small linear system to solve. However, for $d = 12$ for example, 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 a linear programming problem even with hundreds of variables and equations / inequalities.

So we went ahead and tried out what happens up to $d = 12$. We found that up to $d = 6$ there is a unique solution, but uniqueness breaks down starting from $d = 7$ — even though that up to equivalence, there is a unique projective plane of order seven [9, 4]. Like for $d = 6$, we also tried for $d = 10$ and 12 to add some further conditions using *ad hoc* considerations. However, unlike in the $d = 6$ case, these were not sufficient to arrive to a contradiction. We still hope though that the information given by our method will turn out to be useful in the future even at higher orders.

2. THE METHOD APPLIED

Let G be a finite group with conjugacy classes $C_0 = \{e\}, C_1 \dots C_r$ and let γ be the function assigning to each element the cardinality of the conjugacy class it is contained in:

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

For a $B = \{b_1, \dots, b_n\} \subset G$ we shall consider the class-function θ_B counting the number of times that the difference between elements of B falls in a certain conjugacy class; that is,

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

Note that θ_B takes nonnegative values (actually: nonnegative *integer* values) only, $\theta_B(e) = |B| = n$ 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 ones, our main observation is the following.

Proposition 2.1. *For any character χ 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 χ of G and the class-function θ_B/γ is a nonnegative real. Hence θ_B/γ is a linear combination of the irreducible characters of G with nonnegative coefficients only.

Proof. It is clearly enough to prove the first affirmation; as the irreducible characters form an orthonormed bases in the space of class-functions, the value of the scalar product in question is precisely the coefficient of θ_B/γ in this basis corresponding to χ . Now let U be the representation giving χ . 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

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

showing the non-negativity of the scalar product in question. \square

Now let us consider the case when $G = S_d$ and the subset $B = \{\sigma_1, \dots, \sigma_{(d-1)d}\}$ is given by an affine plane of order d as explained in the introduction. Then of the total of $((d-1)d)^2$ differences between the elements of B , $(d-1)d$ gives the identity (i.e. a difference between an element and itself), $(d-1)d$ are differences between elements corresponding to two (different) lines of the same parallel class and $(d-2)(d-1)d^2$ are differences between elements corresponding lines of different equivalent classes. Thus, denoting by \mathcal{S}_j the collection of conjugacy classes of S_d containing permutations with $j = 0, 1, \dots, d$ fixed points, we have the linear equations

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

as well the linear inequalities given by our previous proposition and the noted fact that B takes nonnegative values only:

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

We view this linear system as a restriction on possible θ_B functions. (Note that we dropped the conjugation signs as both θ_B and χ are real-valued functions¹.)

Let us consider now in particular the case when $d = 6$. 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

¹A particular “feature” of the permutation group is that all of its characters are real-valued.

points (as θ_B is constant zero over them), the following shortened version of the character table of S_6 will be sufficient for us:

	e	S_0				S_1	
		(123)(456)	(12)(34)(56)	(1234)(56)	(123456)	(123)(45)	(12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	1	-1	1	-1	-1	1
χ_3	5	-1	-1	-1	-1	0	0
χ_4	5	-1	1	-1	1	0	0
χ_5	5	2	3	-1	0	-1	0
χ_6	5	2	-3	-1	0	1	0
χ_7	9	0	3	1	0	0	-1
χ_8	9	0	-3	1	0	0	-1
χ_9	10	1	2	0	-1	1	0
χ_{10}	10	1	-2	0	1	-1	0
χ_{11}	16	-2	0	0	0	0	1
θ_B	30	x	y	z	v	a	b
		150				720	

In the last line we put (as parameters) the values of the function θ_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 θ_B) with any other line is nonnegative.

In particular, considering that the sum of the lines corresponding to the characters χ_5, χ_7, χ_8 and χ_{10} is $(33, 3, 1, 1, 1, -1, -1)$, we have the inequality:

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

Thus, as $x + y + z + v = 150$ and $a + b = 720$, we have that $990 + 2x + 150 - 2 * 720 \geq 0$ which 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 χ_5 and χ_7 can be simplified resulting the inequalities

$$(5) \quad 5 * 30 + 2 * 150 - a \geq 0, \quad 9 * 30 - b \geq 0.$$

Hence $a \leq 450$ and $b \leq 270$. But then we have no choice: these inequalities must actually be equalities, as a and b must add up to 720. Thus the only possibility is:

$$(6) \quad x = 150, y = 0, z = 0, v = 0, a = 450, b = 270.$$

At this point we could just stop the investigation of our linear system, since in what follows we shall only use that this is how θ_B *should be*. However, we note that simple check shows that with the values given by (6), all scalar products are indeed positive and hence (6) is actually a solution.

Corollary 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 the “last” $d - 1 = 5$ parallel classes of our affine plane, with corresponding “difference-counting” function θ_B given by (6). In particular, out of the total of 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 6 lines), which contradicts to what we established earlier; namely, that precisely 15 of the elements of B should have positive parity. \square

REFERENCES

- [1] R. H. BRUCK & H. J. RYSER: *The non-existence of certain projective planes*. Can. J. Math. **1** (1949), 88–93.
- [2] H. COHN & N. ELKIES: *New upper bounds on sphere packings I*. Ann. of 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] 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.
- [5] A. KABATIANSKY & V. I. LEVENSHTAIN: *Bounds for packings on a sphere and in space*. Problems of Information Transmission **14** (1978), 1–17.
- [6] C. W. H. LAM, L. THIEL & S. SWIERCZ: *The non-existence of finite projective planes of order 10*. Can. J. Math. **XLI** (1989), 1117–1123.
- [7] M. N. KOLOUNTZAKIS, M. MATOLCSI & M. WEINER: *An application of positive definite functions to the problem of MUBs*. To appear in Proc. Amer. Math. Soc.
- [8] F. M. OLIVEIRA DE FILHO & F. VALLENTIN: *Mathematical optimization for packing problems*. SIAG/OPT Views and News **23**(2) (2015), 5–14.
- [9] 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.
- [10] R. P. STANLEY: *Enumerative combinatorics. Volume 2* Cambridge University Press, Cambridge, 1999, xii+581 pp.
- [11] G. TARRY: *Le problème des 36 officiers*. C. R. Assoc. Fran. Av. Sci. **1** (1900), 122–123, **2** (1901), 170–203.

M.M.: BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS (BME), H-1111, EGRY J. U. 1, BUDAPEST, HUNGARY (ALSO AT ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, H-1053, REALTANODA U 13-15, BUDAPEST, HUNGARY)

E-mail address: matomate@renyi.hu

M.W.: BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS (BME), H-1111, EGRY J. U. 1, BUDAPEST, HUNGARY

E-mail address: mweiner@math.bme.hu