Möbius Pairs of Simplices and Commuting Pauli Operators

Hans Havlicek* Boris Odehnal Metod Saniga*

August 25, 2009

Abstract

There exists a large class of groups of operators acting on Hilbert spaces, where commutativity of group elements can be expressed in the geometric language of symplectic polar spaces embedded in the projective spaces PG(n, p), n being odd and p a prime. Here, we present a result about commuting and non-commuting group elements based on the existence of so-called Möbius pairs of n-simplices, i. e., pairs of n-simplices which are *mutually inscribed and circumscribed* to each other. For group elements representing an n-simplex there is no element outside the centre which commutes with all of them. This allows to express the dimension n of the associated polar space in group theoretic terms. Any Möbius pair of n-simplices according to our construction corresponds to two disjoint families of group elements (operators) with the following properties: (i) Any two distinct elements of the same family do not commute. (ii) Each element of one family commutes with all but one of the elements from the other family. A three-qubit generalised Pauli group serves as a non-trivial example to illustrate the theory for $p = 2$ and $n = 5$.

Mathematics Subject Classification (2000): 51A50 – 81R05 – 20F99
PACS Numbers: 02.10.Ox, 02.40.Dr, 03.65.Ca
Key-words: Möbius Pairs of Simplices – Factor Groups – Symplectic Polarity – Generalised Pauli Groups

1 Introduction

The last two decades have witnessed a surge of interest in the exploration of the properties of certain groups relevant for physics in terms of finite geometries. The

*Fellow of the Center for Interdisciplinary Research (ZiF), University of Bielefeld, Germany.

main outcome of this initiative was a discovery of a large family of groups – Dirac and Pauli groups – where commutativity of two distinct elements admits a geometrical interpretation in terms of the corresponding points being joined by an isotropic line (symplectic polar spaces, see [11], [18], [16], [14], [17], [15], [19], [20], and [6] for a comprehensive list of references) or the corresponding unimodular vectors lying on the same free cyclic submodule (projective lines over modular rings, e. g., [7], [8]). This effort resulted in our recent paper [6], where the theory related to polar spaces was given the most general formal setting.

Finite geometries in general, and polar spaces in particular, are endowed with a number of remarkable properties which, in light of the above-mentioned relations, can be directly translated into group theoretical language. In this paper, our focus will be on one of them. Namely, we shall consider pairs of n-simplices of an n-dimensional projective space (n odd) which are mutually inscribed and circumscribed to each other. First, the existence of these so-called Möbius pairs of n-simplices will be derived over an arbitrary ground field. Then, it will be shown which group theoretical features these objects entail if restricting to finite fields of prime order p. Finally, the case of three-qubit Pauli group is worked out in detail, in view of also depicting some distinguished features of the case $p = 2$.

2 Möbius pairs of simplices

We consider the n-dimensional projective space $\mathrm{PG}(n, F)$ over any field F, where $n \geq 1$ is an odd number. Our first aim is to show an n-dimensional analogue of a classical result by Möbius [13]. Following his terminology we say that two n-simplices of $\mathrm{PG}(n, F)$ are *mutually inscribed and circumscribed* if each point of the first simplex is in a hyperplane of the second simplex, and *vice versa* for the points of the second simplex. Two such n-simplices will be called a *Möbius pair of simplices* in $\mathrm{PG}(n, F)$ or shortly a *Möbius pair*. There is a wealth of newer and older results about Möbius pairs in $\mathrm{PG}(3, F)$. See, among others, [5], [4, p. 258], [21], [22]. The possibility to find Möbius pairs of simplices in any odd dimension $n \geq 3$ is a straightforward task [2, p. 188]: Given any n-simplex in $\mathrm{PG}(n, F)$ take the image of its hyperplanes under any null polarity π as second simplex. By this approach, it remains open, though, whether or not the simplices have common vertices. For example, if one hyperplane of the first simplex is mapped under π to one of the vertices of the first simplex, then the two simplices share a common point. However, a systematic account of the n-dimensional case seems to be missing. A few results can be found in [1] and [9]. There is also the possibility to find Möbius pairs which are not linked by a null polarity. See [1, p. 137] for an example over the real numbers and [3, p. 290ff.] for an example over the field with three elements. Other examples arise from the points of the

Klein quadric representing a *double six* of lines in PG(3, F). See [10, p. 31]

We focus our attention to *non-degenerate* Möbius pairs. These are pairs of n-simplices such that each point of either simplex is incident with *one and only one* hyperplane of the other simplex. This property implies that each point of either simplex does not belong to any subspace which is spanned by less than n points of the other simplex, for then it would belong to at least two distinct hyperplanar faces. We present a construction of non-degenerate Möbius pairs which works over any field F. The problem of finding *all* Möbius pairs in PG(n, F) is not within the scope of this article.

In what follows we shall be concerned with matrices over F which are composed of the matrices

$$K := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J := \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad L := \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \tag{1}$$

and the 2×2 unit matrix I. We define a null polarity π of PG(n, F) in terms of the alternating $(n+1) \times (n+1)$ matrix[1]

$$A := \begin{pmatrix} K & -J & \dots & -J \\ J & K & \dots & -J \\ \vdots & \vdots & \ddots & \vdots \\ J & J & \dots & K \end{pmatrix}. \tag{2}$$

Thus all entries of A above the diagonal are -1, whereas those below the diagonal are 1. Using the identities $-K^2 = I$, $JK - KL = 0$, and $JL = 0$ it is easily verified that A is indeed an invertible matrix, because

$$A^{-1} = \begin{pmatrix} -K & -L & \dots & -L \\ L & -K & \dots & -L \\ \vdots & \vdots & \ddots & \vdots \\ L & L & \dots & -K \end{pmatrix}. \tag{3}$$

Let $\mathcal{P} := \{P_0, P_1, \dots, P_n\}$ be the n-simplex which is determined by the vectors $e_0, e_1, \dots, e_n$ of the standard basis of F^{n+1}, i. e.,

$$P_j = Fe_j \text{ for all } j \in \{0, 1, \dots, n\}. \tag{4}$$

The elements of F^{n+1} are understood as column vectors. We first exhibit the image of $\mathcal{P}$ under the null polarity π.

Lemma 1. *Let S be a subspace of* PG(n, F) *which is generated by $k+1 \geq 2$ distinct points of the simplex $\mathcal{P}$. Then the following assertions hold:*

[1] Note that indices range from 0 to n.

(a) $S \cap \pi(S) = \emptyset$ *if* k *is odd.*

(b) $S \cap \pi(S)$ *is a single point, which is in general position to the chosen points of* $\mathcal{P}$*, if* k *is even.*

Proof. Suppose that S is the span of the points $P_{j_0}, P_{j_1}, \ldots, P_{j_k}$, where $0 \leq j_0 < j_1 < \cdots < j_k \leq n$. A point Y is in S if, and only if, it is represented by a vector $y \in F^{n+1}$ of the form

$$y = \sum_{i=0}^{k} y_{j_i} e_{j_i} \neq 0. \tag{5}$$

The rows of A with numbers $j_0, j_1, \ldots, j_k$ comprise the coefficients of a system of linear equations in $n+1$ unknowns $x_0, x_1, \ldots, x_n$ whose solutions are the vectors of $\pi(S)$. Substituting the vector y into this system gives the homogeneous linear system (written in matrix form)

$$A_k \cdot (y_{j_0}, y_{j_1}, \ldots, y_{j_k})^{\mathrm{T}} = (0, 0, \ldots, 0)^{\mathrm{T}}, \tag{6}$$

where A_k is the principal submatrix of A which arises from the first $k+1$ rows and columns of A. Note that (6) holds, because the matrix A_k coincides with the principal submatrix of A which arises from the rows and columns with indices $j_0, j_1, \ldots, j_k$. The solutions of (6) are the vectors of $S \cap \pi(S)$. There are two cases:

k odd: Here A_k has full rank $k+1$, as follows by replacing n with k in (2) and (3). Hence the system (6) has only the zero-solution and $S \cap \pi(S) = \emptyset$, as asserted.

k even: Here A_k cannot be of full rank, as it is an alternating matrix with an odd number of rows. By the above, the submatrix A_{k-1} has rank k, so that the rank of A_k equals to k. This implies that the solutions of the linear system (6) is the span of a single non-zero vector. For example,

$$(-1, 1, -1, 1, -1, \ldots, -1)^{\mathrm{T}} \in F^{k+1} \tag{7}$$

is such a vector. It determines the point

$$P_{j_0, j_1, \ldots, j_k} := F\left(\sum_{i=0}^{k} (-1)^{i+1} e_{j_i}\right). \tag{8}$$

Since the coordinates of $P_{j_0, j_1, \ldots, j_k}$ with numbers $j_0, j_1, \ldots, j_k$ are non-zero, the points $P_{j_0}, P_{j_1}, \ldots, P_{j_k}, P_{j_0, j_1, \ldots, j_k}$ are in general position. □

The previous lemma holds trivially for $k+1 = 0$ points, since then $S = \emptyset$. It is also valid, *mutatis mutandis*, in the case $k+1 = 1$, even though here one has to take into account $S = P_{j_0}$ yields again the point $S \cap \pi(S) = P_{j_0}$. Hence the

null polarity π and the simplex $\mathcal{P}$ give rise to the following points: $P_0, P_1 \ldots, P_n$ (the points of $\mathcal{P}$), $P_{012}, P_{013}, \ldots, P_{n-2,n-1,n}$ (one point in each plane of $\mathcal{P}$), $\ldots$, $P_{0,1,\ldots,n-1}, \ldots, P_{1,2,\ldots,n}$ (one point in each hyperplane of $\mathcal{P}$). All together these are

$$\binom{n+1}{1} + \binom{n+1}{3} + \cdots + \binom{n+1}{n-1} = \sum_{i=0}^{n} \binom{n}{i} = 2^n \tag{9}$$

mutually distinct points. We introduce another notation by defining

$$P_{j_0,j_1,\ldots,j_k} =: Q_{m_0,m_1,\ldots,m_{n-k}}, \tag{10}$$

where $0 \leq m_0 < m_1 < \cdots < m_{n-k} \leq n$ are those indices which do not appear in $P_{j_0,j_1,\ldots,j_k}$. We are now in a position to state our first main result:

Theorem 1. *In* PG(n, F)*, $n \geq 3$, let the null-polarity π and the n-simplex $\mathcal{P} = \{P_0, P_1, \ldots, P_n\}$ be given according to* (2) *and* (4)*, respectively. Then the following assertions hold:*

(a) *$\mathcal{P}$ and $\mathcal{Q} := \{Q_0, Q_1, \ldots, Q_n\}$, where the points Q_m are defined by* (10)*, is a non-degenerate Möbius pair of n-simplices.*

(b) *The n-simplices $\mathcal{P}$ and $\mathcal{Q}$ are in perspective from a point if, and only if, F is a field of characteristic two.*

Proof. Ad (a): Choose any index $m \in \{0, 1, \ldots, n\}$. Then Q_m is the image under π of the hyperplane S which is spanned by $P_0, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$. The proof of Lemma 1 shows how to find a system of linear equations for Q_m. Furthermore, formula (8) provides a coordinate vector for Q_m. However, such a vector can be found directly by extracting the m-th column of the matrix A^{-1}, viz.

$$\sum_{i=0}^{m-1} (-1)^{i+m+1} e_i + \sum_{k=m+1}^{n} (-1)^{k+m} e_k =: q_m. \tag{11}$$

(The vector from (8) is $(-1)^m q_m$.) As the columns of A^{-1} form a basis of F^{n+1}, the point set $\mathcal{Q}$ is an n-simplex.

The $n+1$ hyperplanes of the simplex $\mathcal{Q}$ are the images under π of the vertices of $\mathcal{P}$. Each of these hyperplanes has a linear equation whose coefficients comprise one of the rows of the matrix A. So a point P_j is incident with the hyperplane $\pi(P_i)$ if, and only if, the (i, j)-entry of A is zero. Since each row of A has precisely one zero entry, we obtain that each point of $\mathcal{P}$ is incident with one and only one hyperplane of $\mathcal{Q}$.

In order to show that each point of $\mathcal{Q}$ is incident with precisely one hyperplane of the simplex $\mathcal{P}$, we apply a change of coordinates from the standard basis

$e_0, e_1, \ldots, e_n$ to the basis $b_i := (-1)^i q_i$, $i \in \{0, 1, \ldots, n\}$. The points Fb_i constitute the n-simplex $\mathcal{Q}$. Let B be the matrix with columns $b_0, b_1, \ldots, b_n$. With respect to the basis b_i the columns of B^{-1} describe the points of $\mathcal{P}$, and $B^{\mathrm{T}}AB = A$ is a matrix for π. The columns of B^{-1} and A^{-1} are identical up to an irrelevant change of signs in columns with odd indices. Therefore, with respect the basis b_i, the simplex $\mathcal{Q}$ plays the role of $\mathcal{P}$, and *vice versa*. So the assertion follows from the result in the preceding paragraph.

Ad (b): For each $j \in \{0, 2, \ldots, n-1\}$ the lines P_jQ_j and $P_{j+1}Q_{j+1}$ meet at that point which is given by the vector

$$-e_j + q_j = -(e_{j+1} + q_{j+1}) = (-1, 1, \ldots, -1, 1, \underbrace{-1, -1}_{j,\, j+1}, 1, -1, \ldots, 1, -1)^{\mathrm{T}}. \quad (12)$$

Comparing signs we see that $-e_0 + q_0$ and $-e_2 + q_2$ are linearly independent for $\mathrm{Char}\, K \neq 2$, whereas for $\mathrm{Char}\, K = 2$ all lines P_kQ_k, $k \in \{0, 1, \ldots, n\}$ concur at the point

$$C := F(1, 1, \ldots, 1)^{\mathrm{T}}. \quad (13)$$

□

Remark 1. Choose $k+1$ distinct vertices of $\mathcal{P}$, where $3 \leq k \leq n$ is odd. Up to a change of indices it is enough to consider the k-simplex $\{P_0, P_1, \ldots, P_k\}$ and its span, say S. The null polarity π induces a null polarity π_S in S which assigns to $X \in S$ the $(k-1)$-dimensional subspace $\pi(X) \cap S$. We get within S the settings of Theorem 1 with k rather than n points and π_S instead of π. The *nested* non-degenerate Möbius pair in S is formed by the k-simplex $\{P_0, P_1, \ldots, P_k\}$ and the k-simplex comprising the points

$$Q_{0,k+1,\ldots,n},\ Q_{1,k+1,\ldots,n},\ \ldots,\ Q_{k,k+1,\ldots,n}. \quad (14)$$

This observation illustrates the meaning of all the 2^n points which arise from $\mathcal{P}$ and the null polarity π. If we allow $k = 1$ in the previous discussion then, to within a change of indices, the *nested* degenerate Möbius pair $\{P_0, P_1\} = \{Q_{0,2,\ldots,n}, Q_{1,2,\ldots,n}\}$ is obtained.

Remark 2. The case $F = \mathrm{GF}(2)$ deserves particular mention, since we can give an interpretation for *all points* of $\mathrm{PG}(n, 2)$ in terms of our Möbius pair. Recall the following notion from the theory of binary codes: The *weight* of an element of $\mathrm{GF}(2)^{n+1}$ is the number of 1s amongst its coordinates. The 2^n points addressed in Remark 1 are given by the vectors with *odd weight*. The 2^n vectors with *even weight* are, apart from the zero vector, precisely those vectors which yield the $2^n - 1$ points of the hyperplane $\pi(C) : \sum_{i=0}^{n+1} x_i = 0$. More precisely, the vectors with even weight $w \geq 4$ are the centres of perspectivity for the nested non-degenerate

Möbius pairs of $(w-1)$-simplices, whereas the vectors with weight 2 are the points of intersection of the edges of $\mathcal{P}$ with $\pi(C)$. The latter points may be regarded as "centres of perspectivity" for the degenerate Möbius pairs formed by the two vertices of $\mathcal{P}$ on such an edge. Each point of the hyperplane $\pi(C)$ is the centre of perspectivity of precisely one nested Möbius pair.

3 Commuting and non-commuting elements

Our aim is to translate the properties of Möbius pairs into properties of commuting and non-commuting group elements. We shortly recall some results from [6]. Let $(\boldsymbol{G}, \cdot)$ be a group and p be a prime. Suppose that the centre $Z(\boldsymbol{G})$ of $\boldsymbol{G}$ contains the commutator subgroup $\boldsymbol{G}' = [\boldsymbol{G}, \boldsymbol{G}]$ and the set $\boldsymbol{G}^{(p)}$ of pth powers. Also, let $\boldsymbol{G}'$ be of order p. Then $V := \boldsymbol{G}/Z(\boldsymbol{G})$ is a commutative group which, if written additively, is a vector space over $\mathrm{GF}(p)$ in a natural way. Furthermore, given any generator g of $\boldsymbol{G}'$ we have a bijection $\psi_g : \boldsymbol{G}' \to \mathrm{GF}(p) : g^m \mapsto m$ for all $m \in \{0, 1, \ldots, p\}$. The commutator function in G assigns to each pair $(x, y) \in \boldsymbol{G} \times \boldsymbol{G}$ the element $[x, y] = xyx^{-1}y^{-1}$. It gives rise to the non-degenerate alternating bilinear form

$$[\cdot, \cdot]_g : V \times V \to \mathrm{GF}(p) : (xZ(\boldsymbol{G}), yZ(\boldsymbol{G})) \mapsto \psi_g([x, y]). \tag{15}$$

We assume now that V has finite dimension $n + 1$, and we consider the projective space $\mathrm{PG}(n, p) := \mathbb{P}(V)$. Its points are the one-dimensional subspaces of V. In our group theoretic setting a non-zero vector of V is a coset $xZ(\boldsymbol{G})$ with $x \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$. The scalar multiples of $xZ(\boldsymbol{G})$ are the cosets of the form $x^kZ(\boldsymbol{G})$, $k \in \{0, 1, \ldots, p - 1\}$, because multiplying a vector of V by $k \in \mathrm{GF}(p)$ means taking a kth power in $\boldsymbol{G}/Z(\boldsymbol{G})$. So $x, x' \in \boldsymbol{G}$ describe the same point X of $\mathrm{PG}(n, p)$ if, and only if, none of them is in the centre of $\boldsymbol{G}$, and $x' = x^kz$ for some $k \in \{1, 2, \ldots, p - 1\}$ and some $z \in Z(\boldsymbol{G})$. Under these circumstances x (and likewise x') is said to *represent* the point X. Conversely, the point X is said to *correspond* to x (and likewise x'). Note that the elements of $Z(\boldsymbol{G})$ determine the zero vector of V. So they do not represent any point of $\mathrm{PG}(n, p)$.

The non-degenerate alternating bilinear form from (15) determines a null polarity π in $\mathrm{PG}(n, p)$. We quote the following result from [6, Theorem 6]: *Two elements $x, y \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$ commute if, and only if, their corresponding points in* $\mathrm{PG}(n, p)$ *are conjugate with respect to π, i. e., one of the points is in the polar hyperplane of the other point.* This crucial property is the key for proving Lemma 2 and Theorem 2 below.

Lemma 2. *Suppose that $x_0, x_1, \ldots, x_r \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$ is a family of group elements. Then the following assertions are equivalent:*

(a) *The points corresponding to* $x_0, x_1, \ldots, x_r$ *constitute an n-simplex of the projective space* PG(n, p)*, whence* $r = n$.

(b) *There exists no element in* $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ *which commutes with all of* $x_0, x_1, \ldots, x_r$*, but for each proper subfamily of* $x_0, x_1, \ldots, x_r$ *at least one such element exists.*

Proof. The points corresponding to the family (x_i) generate PG(n, p) if, and only if, their polar hyperplanes have no point in common. This in turn is equivalent to the non-existence of an element in $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ which commutes with all elements of the family (x_i). The proof is now immediate from the following observation: An n-simplex of PG(n, p) can be characterised as being a minimal generating family of PG(n, p). □

This result shows that the dimension $n + 1$ of V can be easily determined by counting the cardinality of a family of group elements which satisfies condition (b). We close this section by translating Theorem 1:

Theorem 2. *Let* $\boldsymbol{G}$ *be a group which satisfies the assumptions stated in the first paragraph of this section. Also, let* $V = \boldsymbol{G}/Z(\boldsymbol{G})$ *be an* $(n + 1)$*-dimensional vector space over* GF(p)*. Suppose that* $x_0, x_1, \ldots, x_n \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$ *and* $y_0, y_1, \ldots, y_n \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$ *are two families of group elements which represent a non-degenerate Möbius pair of* PG(n, p) *as in Theorem* 1*. Then the following assertions hold:*

(a) *There exists no element in* $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ *which commutes with* $x_0, x_1, \ldots, x_n$.

(b) *The elements* $x_0, x_1, \ldots, x_n$ *are mutually non-commuting.*

(c) *For each* $i \in \{1, 2, \ldots, n\}$ *the element* x_i *commutes with all* y_j *such that* $j \neq i$.

Each of these three assertions remains true when changing the role of the elements $x_0, x_1, \ldots, x_n$ *and* $y_0, y_1, \ldots, y_n$.

Proof. The assertion in (a) follows from Lemma 2. Since all non-diagonal entries of the matrix A from (2) equal to 1, no two points which are represented by the elements x_i are conjugate with respect to π. Hence (b) is satisfied. Finally, (c) follows, as the polar hyperplane of the point represented by x_i contains all the points which are represented by the elements y_j with $j \neq i$. The last statement holds due to the symmetric role of the two simplices of a Möbius pair which was established in the proof of Theorem 1 (a). □

Remark 3. According to Remark 1 we may obtain nested non-degenerate Möbius pairs from appropriate subfamilies of $x_0, x_1, \ldots, x_n$. These Möbius pairs satisfy, *mutatis mutandis*, properties (b) and (c).

Example 1. We consider the complex matrices

$$\sigma_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{16}$$

The matrices $i^\alpha \sigma_\beta$ with $\alpha \in \{0, 1, 2, 3\}$ and $\beta \in \{0, x, y, z\}$ constitute the *Pauli group* $\boldsymbol{P}$ of order 16. The centre of $\boldsymbol{P}$ is $Z(\boldsymbol{P}) = \{i^\alpha \sigma_0 \mid \alpha \in \{0, 1, 2, 3\}\}$. The commutator subgroup $\boldsymbol{P}' = \{\pm\sigma_0\}$ and the set $\boldsymbol{P}^{(2)} = \{\pm\sigma_0\}$ of squares are contained in $Z(\boldsymbol{P})$. By Section 3, the factor group $\boldsymbol{P}/Z(\boldsymbol{P})$, if written additively, is a vector space over GF(2). For each $\beta \in \{0, x, y, z\}$ the coset $Z(\boldsymbol{P})\sigma_\beta$ is denoted by β. In this notation, addition can be carried out according to the relations $0 + \beta = \beta$, $\beta + \beta = 0$, and $x + y + z = 0$. The mapping

$$0 \mapsto (0, 0)^{\mathrm{T}}, \quad x \mapsto (1, 0)^{\mathrm{T}}, \quad y \mapsto (0, 1)^{\mathrm{T}}, \quad z \mapsto (1, 1)^{\mathrm{T}} \tag{17}$$

is an isomorphism of $\boldsymbol{P}/Z(\boldsymbol{P})$ onto the additive group of the vector space GF(2) $\times$ GF(2).

Let $\boldsymbol{G}$ be the group of order 256 comprising the three-fold Kronecker products $i^\alpha \sigma_\beta \otimes \sigma_\gamma \otimes \sigma_\delta$ with $\alpha \in \{0, 1, 2, 3\}$ and $\beta, \gamma, \delta \in \{0, x, y, z\}$. This group acts on the eight-dimensional Hilbert space of three qubits. In our terminology from Section 3 (with $p := 2$) we have

$$Z(\boldsymbol{G}) = \{i^\alpha \sigma_0 \otimes \sigma_0 \otimes \sigma_0 \mid \alpha \in \{0, 1, 2, 3\}\}, \quad \boldsymbol{G}' = \boldsymbol{G}^{(2)} = \{\pm\sigma_0 \otimes \sigma_0 \otimes \sigma_0\}, \tag{18}$$

and $g = -\sigma_0 \otimes \sigma_0 \otimes \sigma_0$. Hence $V = \boldsymbol{G}/Z(\boldsymbol{G})$ is a six-dimensional vector space over GF(2) endowed with an alternating bilinear form $[\cdot, \cdot]_g$. We introduce $\beta\gamma\delta$ as a shorthand for $Z(\boldsymbol{G})(\sigma_\beta \otimes \sigma_\gamma \otimes \sigma_\delta)$, where $\beta, \gamma, \delta \in \{0, x, y, z\}$. In this notation, addition in V can be carried out componentwise according to the relations stated before. An isomorphism of V onto GF(2)^6 is obtained by replacing the three symbols of an element of V according to (17). This gives the *coordinate vector* of an element of V. For example, the coordinate vectors of the six elements

$$x00, y00, 0x0, 0y0, 00x, 00y \in V \tag{19}$$

comprise the standard basis of GF(2)^6. These six elements therefore form a basis of V. The projective space PG(5, 2) = $\mathbb{P}(V)$, like any projective space over GF(2), has the particular property that each of its points is represented by one and only one non-zero vector of V. *We therefore identify* $V \setminus \{000\}$ *with* PG(5, 2).

Recall the matrices defined in (1). The matrix of the alternating bilinear form from (15) with respect to the basis (19) equals to the 6×6 matrix diag(K, K, K) over GF(2). In order to obtain a Möbius pair

$$\mathcal{P} = \{P_0, P_1, \ldots, P_5\}, \quad \mathcal{Q} = \{Q_0, Q_1, \ldots, Q_5\} \tag{20}$$

we have to use another basis of V, e. g., the one which arises in terms of coordinates from the six columns of the matrix

$$T := \begin{pmatrix} I & J & J \\ 0 & I & J \\ 0 & 0 & I \end{pmatrix}. \tag{21}$$

Indeed, $T^{\mathrm{T}} \cdot \mathrm{diag}(K, K, K) \cdot T$ gives an alternating 6×6 matrix A as in (2). We thus can translate our results from Section 2 as follows: First, we multiply T with the "old" coordinate vectors from there and, second, we express these "new" coordinate vectors as triplets in terms of $0, x, y, z$. The vertices $P_0, P_1, \ldots, P_5$ and $Q_0, Q_1, \ldots, Q_5$ can be read off, respectively, from the first and second row of the following matrix:

$$\begin{array}{cccccc} x00 & y00 & zx0 & zy0 & zzx & zzy \\ yzz & xzz & 0yz & 0xz & 00y & 00x \end{array} \tag{22}$$

We note that $\mathcal{P}$ and $\mathcal{Q}$ are in perspective from a point according to Theorem 1. This point is zzz. Since each line of PG$(5, 2)$ has only three points, the entries of the second row in (22) can be found by adding zzz to the entries from the first row. Each point of PG$(5, 2)$ corresponds to four elements of the group $\boldsymbol{G}$, whence the points of $\mathcal{P} \cup \mathcal{Q}$ correspond to 48 elements of $\boldsymbol{G}$, none of them in the centre $Z(\boldsymbol{G})$. We can rephrase the Möbius property as follows: *Let two out of these* 48 *elements of* $\boldsymbol{G}$ *represent distinct points. Then these two elements commute if, and only if, they represent points which are in distinct rows and distinct columns of the matrix* (22). The 20 points $P_{012}, P_{013}, \ldots, P_{345}$ are obtained by adding three of the points of $\mathcal{P}$. Explicitly, we get:

$$\begin{array}{cccccccccc} 0x0 & 0y0 & 0zx & 0zy & xz0 & xyx & xyy & xxx & xxy & x0z \\ yz0 & yyx & yyy & yxx & yxy & y0z & z0x & z0y & zxz & zyz \end{array} \tag{23}$$

We leave it to the reader to find the $\binom{6}{4} = 15$ nested Möbius pairs of tetrahedra which are formed by four points from $\mathcal{P}$ and the four appropriate points from (23). By Remark 2, the 32 points from (22) and (23) are precisely the points off the polar hyperplane of zzz. This means that none of the corresponding elements of $\boldsymbol{G}$ commutes with the representatives of the distinguished point zzz.

The results from [6] show that Theorem 2 can be applied to a wide class of groups, including the generalised Pauli groups acting on the space of N-qudits provided that d is a prime number.

4 Conclusion

Following the strategy set up in our recent paper [6], we have got a deeper insight into the geometrical nature of a large class of finite groups, including many asso-

ciated with finite Hilbert spaces. This was made possible by employing the notion of a Möbius pair of n-simplices in a finite odd-dimensional projective space, PG(n, p), p being a prime. Restricting to non-degenerate Möbius pairs linked by a null polarity, we have first shown their existence for any odd n, a remarkable nested structure they form, and perspectivity from a point of the simplices in any such pair if $p = 2$. Then, the commutation properties of the group elements associated with a Möbius pair have been derived. In particular, the two disjoint families of $n + 1$ group elements that correspond to a Möbius pair are such that any two distinct elements/operators from the same family do not commute and each element from one family commutes with all but one of the elements from the other family. As the theory also encompasses a number of finite generalised Pauli groups, that associated with three-qubits ($n = 5$ and $p = 2$) was taken as an illustrative example, also because of envisaged relevance of Möbius pairs to entanglement properties of a system of three fermions with six single-particle states [12]. It should, however, be stressed that above-outlined theory is based on a particular construction of Möbius pairs, and so there remains an interesting challenge to see in which way it can be generalised to incorporate arbitrary Möbius pairs.

Acknowledgements

This work was carried out in part within the "Slovak-Austrian Science and Technology Cooperation Agreement" under grants SK 07-2009 (Austrian side) and SK-AT-0001-08 (Slovak side), being also partially supported by the VEGA grant agency projects Nos. 2/0092/09 and 2/7012/27. The final version was completed within the framework of the Cooperation Group "Finite Projective Ring Geometries: An Intriguing Emerging Link Between Quantum Information Theory, Black-Hole Physics, and Chemistry of Coupling" at the Center for Interdisciplinary Research (ZiF), University of Bielefeld, Germany.

References

[1] L. Berzolari. Sull' estensione del concetto di tetraedri di Möbius agli iperspazî. *Rend. Circ. Mat. Palermo*, 22:136–140, 1906.

[2] H. Brauner. *Geometrie projektiver Räume II*. BI Wissenschaftsverlag, Mannheim, 1976.

[3] H. S. M. Coxeter. Twelve points in PG(5, 3) with 95040 self-transformations. *Proc. Roy. Soc. London, Ser. A*, 247:279–293, 1958.

[4] H. S. M. Coxeter. *Introduction to Geometry*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1989. Reprint of the 1969 edition.

[5] A. P. Guinand. Graves triads, Möbius pairs, and related matrices. *J. Geom.*, 10(1-2):9–16, 1977.

[6] H. Havlicek, B. Odehnal, and M. Saniga. Factor-group-generated polar spaces and (multi-) qudits. *SIGMA Symmetry Integrability Geom. Methods Appl.*, submitted. (arXiv:0903.5418).

[7] H. Havlicek and M. Saniga. Projective ring line of a specific qudit. *J. Phys. A*, 40(43):F943–F952, 2007. (arXiv:0708.4333).

[8] H. Havlicek and M. Saniga. Projective ring line of an arbitrary single qudit. *J. Phys. A*, 41(1):015302, 12 pp., 2008. (arXiv:0710.0941).

[9] H. Herrmann. Matrizen als projektive Figuren. *Jber. Deutsch. Math. Verein.*, 56(Abt. 1):6–20, 1952. Erratum: ibid. 104.

[10] J. W. P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Oxford University Press, Oxford, 1985.

[11] B. Huppert. *Endliche Gruppen. I*. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[12] P. Lévay and P. Vrana. Three fermions with six single-particle states can be entangled in two inequivalent ways. *Phys. Rev. A*, 78:022329, 10 pp., 2008. (arXiv:0903.0541).

[13] F. A. Möbius. Kann von zwei dreiseitigen Pyramiden eine jede in Bezug auf die andere um- und eingeschrieben zugleich heissen? *J. reine angew. Math.*, 3:273–278, 1828.

[14] M. Planat and M. Saniga. On the Pauli graphs of N-qudits. *Quantum Inf. Comput.*, 8(1-2):127–146, 2008. (arXiv:quant-ph/0701211).

[15] A. R. P. Rau. Mapping two-qubit operators onto projective geometries. *Phys. Rev. A*, 79:042323, 6 pp., 2009. (arXiv:0808.0598).

[16] M. Saniga and M. Planat. Multiple qubits as symplectic polar spaces of order two. *Adv. Stud. Theor. Phys.*, 1(1-4):1–4, 2007. (arXiv:quant-ph/0612179).

[17] A. N. Sengupta. Finite geometries with qubit operators. *Infin. Dimens. Anal. Quantum Probab. Relat. Top.*, 12(2):359–366, 2009. Preprint (arXiv:0904.2812).

[18] R. Shaw. Finite geometry, Dirac groups and the table of real Clifford algebras. In *Clifford algebras and spinor structures*, volume 321 of *Math. Appl.*, pages 59–99. Kluwer Acad. Publ., Dordrecht, 1995.

[19] K. Thas. Pauli operators of N-qubit Hilbert spaces and the Saniga-Planat conjecture. *Chaos, Solitons, Fractals*. in press.

[20] K. Thas. The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs. *Europhys. Lett. EPL*, 86:60005, 3 pp., 2009.

[21] K. Witczyński. Some remarks on the theorem of Möbius. *J. Geom.*, 51(1-2):187–189, 1994.

[22] K. Witczyński. Möbius' theorem and commutativity. *J. Geom.*, 59(1-2):182–183, 1997.

Hans Havlicek and Boris Odehnal
Institut für Diskrete Mathematik und Geometrie
Technische Universität
Wiedner Hauptstraße 8–10/104
A-1040 Wien, Austria
havlicek, boris@geometrie.tuwien.ac.at

Metod Saniga
Astronomical Institute
Slovak Academy of Sciences
SK-05960 Tatranská Lomnica
Slovak Republic
msaniga@astro.sk