Symmetry, Integrability and Geometry: Methods and Applications SIGMA 5 (2009), 096, 15 pages

Factor-Group-Generated Polar Spaces and (Multi-)Qudits

Hans HAVLICEK †§, *Boris ODEHNAL* † and *Metod SANIGA* ‡§

† *Institut für Diskrete Mathematik und Geometrie, Technische Universität Wien, Wiedner Hauptstraße 8–10/104, A-1040 Wien, Austria*
E-mail: *havlicek@geometrie.tuwien.ac.at, boris@geometrie.tuwien.ac.at*
URL: http://www.geometrie.tuwien.ac.at/havlicek/
URL: http://www.geometrie.tuwien.ac.at/odehnal/

‡ *Astronomical Institute, Slovak Academy of Sciences, SK-05960 Tatranská Lomnica, Slovak Republic*
E-mail: *msaniga@astro.sk*
URL: http://www.astro.sk/~msaniga/

§ *Center for Interdisciplineary Research (ZiF), University of Bielefeld, D-33615 Bielefeld, Germany*

Received August 19, 2009, in final form October 02, 2009; Published online October 13, 2009
doi:10.3842/SIGMA.2009.096

Abstract. Recently, a number of interesting relations have been discovered between generalised Pauli/Dirac groups and certain finite geometries. Here, we succeeded in finding a general unifying framework for all these relations. We introduce gradually necessary and sufficient conditions to be met in order to carry out the following programme: Given a group $\boldsymbol{G}$, we first construct vector spaces over $\mathrm{GF}(p)$, p a prime, by factorising $\boldsymbol{G}$ over appropriate normal subgroups. Then, by expressing $\mathrm{GF}(p)$ in terms of the commutator subgroup of $\boldsymbol{G}$, we construct alternating bilinear forms, which reflect whether or not two elements of $\boldsymbol{G}$ commute. Restricting to $p = 2$, we search for "refinements" in terms of quadratic forms, which capture the fact whether or not the order of an element of $\boldsymbol{G}$ is ≤ 2. Such factor-group-generated vector spaces admit a natural reinterpretation in the language of symplectic and orthogonal polar spaces, where each point becomes a "condensation" of several distinct elements of $\boldsymbol{G}$. Finally, several well-known physical examples (single- and two-qubit Pauli groups, both the real and complex case) are worked out in detail to illustrate the fine traits of the formalism.

Key words: groups; symplectic and orthogonal polar spaces; geometry of generalised Pauli groups

2000 Mathematics Subject Classification: 20C35; 51A50; 81R05

1 Introduction

The purpose of this paper is to establish the most general formal setting for reformulating, whenever possible, basic properties of groups in terms of vector spaces, alternating bilinear forms, quadratic forms and associated projective and polar spaces. As far as we know, the first outline of such an analysis can be tracked back in the textbook of Huppert [1], when addressing the so-called *extra-special groups*; however, the assumptions made there were rather specific and no finite geometry was explicitly mentioned. Another treatment of the issue, with important physical applications, was given by Shaw and his collaborators [2, 3, 4, 5, 6, 7]. These papers deal with the *Dirac groups* and their relationship to projective spaces over $\mathrm{GF}(2)$. They include also a detailed dictionary from group theory to finite geometry and *vice versa* (see also [8]). Being unaware of these developments, Planat and Saniga and others set up a similar programme [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] (see also [23]), and discovered various kinds of finite geometry behind the generalised Pauli groups of specific finite-level quantum systems, their results being put into a more general context by Koen Thas [24] ($p = 2$) and [25] ($p > 2$); these works, however, focussed uniquely on symplectic case (alternating bilinear forms), leaving the importance of quadratic forms simply unnoticed. In what follows we shall not only fill this gap, but develop the theory to such an extent that the links between the above-mentioned approaches become clearly visible and, at the same time, differences between some closely related finite groups (e.g., between the real and complex two-qubit Pauli groups) will be revealed and properly understood.

2 Preliminaries

We first collect some notions which will be used throughout the paper:

Let $(\boldsymbol{G}, \cdot)$ be a group with neutral element e. Given a set $\boldsymbol{M} \subseteq \boldsymbol{G}$ we denote by $\langle \boldsymbol{M} \rangle$ the subgroup of $\boldsymbol{G}$ generated by $\boldsymbol{M}$. Also, we let

$$\boldsymbol{M}^{(m)} := \{x^m \mid x \in \boldsymbol{M}\} \quad \text{for all} \quad m \in \mathbb{Z}.$$

The commutator of $a, b \in \boldsymbol{G}$ is written as $[a, b] := aba^{-1}b^{-1}$. The commutator group (derived group) $[\boldsymbol{G}, \boldsymbol{G}] =: \boldsymbol{G}'$ is the subgroup of $\boldsymbol{G}$ which is generated by all commutators. The centre of $\boldsymbol{G}$ is written as $Z(\boldsymbol{G})$.

Furthermore, let p be a fixed prime. We denote the Galois field with p elements by $\mathrm{GF}(p) = \mathbb{Z}/(\mathbb{Z}p)$. We shall always use $0, 1, \ldots, p-1 \in \mathbb{Z}$ as representatives for the elements of $\mathrm{GF}(p)$. Vector spaces over $\mathrm{GF}(p)$ have a series of rather simple, but nevertheless noteworthy properties which are not shared by vector spaces over arbitrary fields. If $(V, +)$ is vector space over $\mathrm{GF}(p)$ then

$$mv = \underbrace{v + v + \cdots + v}_{m} \quad \text{for all} \quad m \in \mathrm{GF}(p), \ v \in V. \tag{1}$$

So the additive group $(V, +)$ or, more precisely, V as a $\mathbb{Z}$-module, determines the structure as a vector space over $\mathrm{GF}(p)$ in a *unique* way. In particular, we have

$$\underbrace{v + v + \cdots + v}_{p} = o \quad \text{for all} \quad v \in V, \tag{2}$$

where o denotes the zero element of V. Consequently, any subgroup of V is also a (vector) subspace. Furthermore, any additive mapping of vector spaces over $\mathrm{GF}(p)$ is also linear; see, among others, [26] and [27]. Conversely, a commutative group $(V, +)$ satisfying (2) can be turned into a vector space over $\mathrm{GF}(p)$ by defining the product of $m \in \mathrm{GF}(p)$ and $v \in V$ by (1).

3 Vector spaces over GF (p)

We aim at constructing vector spaces over $\mathrm{GF}(p)$ by factorising $\boldsymbol{G}$ modulo appropriate normal subgroups.

Let $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$, i.e., $\boldsymbol{N}$ is a normal subgroup of $\boldsymbol{G}$. The factor group $\boldsymbol{G}/\boldsymbol{N}$ is commutative if, and only if, the commutator group satisfies $\boldsymbol{G}' \leq \boldsymbol{N}$. Furthermore, $\boldsymbol{G}/\boldsymbol{N}$ is isomorphic to the additive group of a vector space over $\mathrm{GF}(p)$ if, and only if, it satisfies the following condition:

Condition 1. $\boldsymbol{N}$ is a normal subgroup of $\boldsymbol{G}$ which contains the commutator subgroup $\boldsymbol{G}'$ and the set $\boldsymbol{G}^{(p)}$ of pth powers.

Remark 1. Let $\boldsymbol{N} \leq \boldsymbol{G}$ be a *subgroup* of $\boldsymbol{G}$ satisfying $\boldsymbol{G}' \leq \boldsymbol{N}$. We recall that $\boldsymbol{N}$ is a *normal subgroup* of $\boldsymbol{G}$ in this case, since for all $a \in \boldsymbol{N}$ and all $x \in \boldsymbol{G}$ we have $xax^{-1} = [x, a]a \in \boldsymbol{N}$. This means that Condition 1 can be relaxed by omitting the word "normal".

Remark 2. The complex product $\boldsymbol{G}'\boldsymbol{G}^{(p)} = \{xy \mid x \in \boldsymbol{G}',\, y \in \boldsymbol{G}^{(p)}\}$ is easily seen to be a subgroup of $\boldsymbol{G}$. Thus, by Remark 1, we have

$$\boldsymbol{G}'\boldsymbol{G}^{(p)} = \langle \boldsymbol{G}' \cup \boldsymbol{G}^{(p)} \rangle \trianglelefteq \boldsymbol{G}. \tag{3}$$

Remark 3. The case $p = 2$ deserves particular mention. Here Condition 1 can be further relaxed by deleting the condition $\boldsymbol{G}' \leq \boldsymbol{N}$, because $\boldsymbol{G}^{(2)} \subseteq \boldsymbol{N}$ implies that all elements of $\boldsymbol{G}/\boldsymbol{N}$ have order one or two, which in turn guarantees the commutativity of $\boldsymbol{G}/\boldsymbol{N}$.[1]

We assume until further notice that Condition 1 holds. Then we let

$$(V, +) := (\boldsymbol{G}/\boldsymbol{N}, \cdot),$$

i.e., the composition in V will be written additively, and we consider V as a vector space over $\mathrm{GF}(p)$ in accordance with (1).

It is an easy exercise to express notions from the vector space V (like linear dependence, dimension, etc.) in terms of the factor group $\boldsymbol{G}/\boldsymbol{N}$. For example, a linear combination $\sum_{i=1}^{k} m_i v_i$ with $m_i \in \mathrm{GF}(p)$, $v_i = x_i\boldsymbol{N}$ and $x_i \in \boldsymbol{G}$ translates into $x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}\boldsymbol{N}$. The factors in this product may be rearranged in any order. The set of all subspaces of V is precisely the set

$$\{\boldsymbol{S}/\boldsymbol{N} \mid \boldsymbol{N} \leq \boldsymbol{S} \leq \boldsymbol{G}\}. \tag{4}$$

The factor spaces of V have the form $V/(\boldsymbol{S}/\boldsymbol{N})$, with $\boldsymbol{S}$ as above. There exists the canonical isomorphism (of vector spaces)

$$\boldsymbol{G}/\boldsymbol{S} \to (\boldsymbol{G}/\boldsymbol{N})/(\boldsymbol{S}/\boldsymbol{N}) : \ x\boldsymbol{S} \mapsto (x\boldsymbol{N})(\boldsymbol{S}/\boldsymbol{N})$$

by the homomorphism theorem. Therefore, up to the canonical identification

$$\boldsymbol{G}/\boldsymbol{S} \equiv (\boldsymbol{G}/\boldsymbol{N})/(\boldsymbol{S}/\boldsymbol{N}) = V/(\boldsymbol{S}/\boldsymbol{N}), \tag{5}$$

the set of all factor spaces of V is precisely the set

$$\{\boldsymbol{G}/\boldsymbol{S} \mid \boldsymbol{N} \leq \boldsymbol{S} \leq \boldsymbol{G}\}.$$

The identification (5) will frequently be used in what follows. If V is finite then $\#V = p^d$, where d is the dimension of V. Hence in this case the dimension of V can be found by a simple counting argument.

We close this section with a complete description of all vector spaces arising from our previous construction.

Theorem 1. *Let $\boldsymbol{G}$ be any group. Then the following assertions hold:*

(a) *The subgroup $\boldsymbol{N}_0 := \boldsymbol{G}'\boldsymbol{G}^{(p)}$ is normal in $\boldsymbol{G}$ and meets the requirements of Condition* 1*. Hence it yields the vector space $V_0 := \boldsymbol{G}/\boldsymbol{N}_0$ over* $\mathrm{GF}(p)$*.*

(b) *The set of vector spaces $\boldsymbol{G}/\boldsymbol{N}$, where $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ is subject to Condition* 1*, is precisely the set of all factor spaces of V_0, up to the canonical identification $\boldsymbol{G}/\boldsymbol{N} \equiv V_0/(\boldsymbol{N}/\boldsymbol{N}_0)$ from* (5)*.*

[1] A group of prime exponent $p > 2$ need not be commutative. For example, the set of upper triangular 3×3 matrices over $\mathrm{GF}(p)$ with 1s along the diagonal is a non-commutative group of exponent p under matrix multiplication for $p > 2$.

Proof. Ad (a): This is clear by Remarks 1 and 2.

Ad (b): A subgroup $\boldsymbol{N} \leq \boldsymbol{G}$ satisfies Condition 1 if, and only if, $\boldsymbol{N}_0 \leq \boldsymbol{N}$. Under these circumstances the canonical identification from (5) can be applied to $\boldsymbol{G}/\boldsymbol{N}$. This establishes the result. ∎

The previous result can be rephrased as follows: Our construction yields (to within isomorphism) precisely the homomorphic images of the vector space V_0.

Of course, in Theorem 1 the trivial case $\boldsymbol{N}_0 = \boldsymbol{G}$ may occur so that V_0 turns out to be the zero vector space over $\mathrm{GF}(p)$. Take, for example, $\boldsymbol{G}$ as a cyclic group of prime order $\neq p$. At the other extreme, if $\boldsymbol{G}$ is a commutative group of index p then $\boldsymbol{N}_0 = \{e\}$.

4 The underlying field

For our construction of an alternating bilinear form in Section 5, we shall need an interpretation of the Galois field $\mathrm{GF}(p)$ *within the group $\boldsymbol{G}$ in terms of the commutator group $\boldsymbol{G}'$*. The (multiplicative) group $\boldsymbol{G}'$ is isomorphic to the additive group of the Galois field $\mathrm{GF}(p)$ precisely when the following is satisfied:

Condition 2. The commutator group $\boldsymbol{G}'$ has order p.

This is due to the fact that any two groups of order p are cyclic and hence isomorphic. Condition 2 is very restrictive, in sharp contrast to Condition 1.

Remark 4. Condition 2 implies that $\boldsymbol{G}$ is a *non-commutative group*, since $\boldsymbol{G}'$ has to have more than one element.

Let us assume until the end of this section that Condition 2 holds. For each generator g of $\boldsymbol{G}'$ (viz. each element $g \in \boldsymbol{G}' \setminus \{e\}$) the mapping

$$\psi_g : \ (\boldsymbol{G}', \cdot) \to \big(\mathrm{GF}(p), +\big) : \ g^m \mapsto m \quad \text{with} \ \ m \in \{0, 1, \ldots, p-1\} \tag{6}$$

is an isomorphism of groups. Given a generator $\tilde{g} \in \boldsymbol{G}'$ there exists an element $k \in \{1, \ldots, p-1\}$ such that $g = \tilde{g}^k$, whence

$$(\psi_{\tilde{g}} \circ \psi_g^{-1})(m) = km \quad \text{for all} \ \ m \in \mathrm{GF}(p).$$

Therefore, loosely speaking, $\boldsymbol{G}'$ could be identified with $\mathrm{GF}(p)$ *up to a non-zero scalar $k \in \mathrm{GF}(p)$*. In fact, Condition 2 just guarantees that $\boldsymbol{G}'$ is a one-dimensional vector space over $\mathrm{GF}(p)$, but it does not provide a unique way to identify $\boldsymbol{G}'$ with $\mathrm{GF}(p)$ unless $p = 2$. Examples of groups satisfying Condition 2 will be exhibited in Section 9.

Remark 5. If Conditions 1 and 2 are satisfied then, taking into account $\psi_g^{-1}(m) = g^m$ and $v = x\boldsymbol{N}$ for some $m \in \mathrm{GF}(p)$ and some $x \in \boldsymbol{G}$, it would be *incorrect* to calculate the product mv in terms of the factor group $\boldsymbol{G}/\boldsymbol{N}$ as $(g^m\boldsymbol{N})(x\boldsymbol{N}) = g^m x\boldsymbol{N}$. For example, $m = 0$ and $v \neq o$ (zero vector) yield $0 \cdot v = o$, but $g^0 x\boldsymbol{N} = x\boldsymbol{N} = v \neq o$. Observe that this applies even in the case $p = 2$, where there is just one possibility for choosing an isomorphism ψ_g.

5 An alternating bilinear form

Given a group $\boldsymbol{G}$ and a normal subgroup $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ satisfying Condition 1, we want to turn the commutator mapping $[\cdot, \cdot] : \boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G}'$ into a function which is well defined on $V \times V$. This amounts to requiring that for all $x, y \in \boldsymbol{G}$ their commutator $[x, y]$ does not change if x is replaced by any element from the coset $x\boldsymbol{N}$ and likewise for y. For any $a \in \boldsymbol{N}$ we have $[x, y] = [xa, y]$ if, and only if,

$$xyx^{-1}y^{-1} = xaya^{-1}x^{-1}y^{-1}$$

or, equivalently, $ay = ya$. Since here $y \in \boldsymbol{G}$ is arbitrary, this holds precisely when $a \in Z(\boldsymbol{G})$. We are thus led to the following:

Condition 3. The normal subgroup $\boldsymbol{N}$ is contained in the centre of $\boldsymbol{G}$.

By virtue of this condition, we have indeed $[x, y] = [xa, yb]$ for all $x, y \in \boldsymbol{G}$ and all $a, b \in \boldsymbol{N}$. However, there does not seem to be an obvious meaning of the commutator group $\boldsymbol{G}'$ for our vector space V. Hence we assume until further notice that Conditions 1, 2, and 3 hold. Therefore

$$\boldsymbol{G}'\boldsymbol{G}^{(p)} \trianglelefteq \boldsymbol{N} \trianglelefteq Z(\boldsymbol{G}) \triangleleft \boldsymbol{G} \tag{7}$$

is satisfied. Also, we choose an isomorphism ψ_g according to (6). This allows us to define a mapping

$$[\cdot,\cdot]_g : \ V \times V \to \mathrm{GF}(p) : \ (v, w) = (x\boldsymbol{N}, y\boldsymbol{N}) \mapsto \psi_g([x, y]), \tag{8}$$

where $x, y \in \boldsymbol{G}$. We collect now several basic properties of this mapping.

Theorem 2. *Suppose that the group $\boldsymbol{G}$ and the normal subgroup $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ satisfy Conditions 1, 2, and 3. Also, let g be a generator of the commutator group $\boldsymbol{G}'$. Then the following assertions hold:*

(a) *The mapping $[\cdot,\cdot]_g$ given by (8) is an alternating bilinear form on the vector space $V = \boldsymbol{G}/\boldsymbol{N}$.*

(b) *Two elements $x, y \in \boldsymbol{G}$ commute if, and only if, the corresponding vectors $v = x\boldsymbol{N}, w = y\boldsymbol{N} \in V$ are orthogonal with respect to $[\cdot,\cdot]_g$, i.e., $[v, w]_g = 0$.*

(c) *The bilinear form $[\cdot,\cdot]_g$ is non-zero and has the radical $V^{\perp} = Z(\boldsymbol{G})/\boldsymbol{N}$. Consequently, this form is non-degenerate if, and only if, $\boldsymbol{N}$ coincides with the centre of $\boldsymbol{G}$.*

Proof. Ad (a): Given $x, y \in \boldsymbol{G}$ we let $v := x\boldsymbol{N}$ and $w := y\boldsymbol{N}$. Then

$$[v, v]_g = \psi_g([x, x]) = \psi_g(e) = 0$$

and

$$[w, v]_g = \psi_g([y, x]) = \psi_g\big([x, y]^{-1}\big) = -[w, v]_g. \tag{9}$$

Also, we obtain

$$\begin{aligned}
[v_1 + v_2, w]_g &= \psi_g\big((x_1x_2)y(x_1x_2)^{-1}y^{-1}\big) = \psi_g\big(x_1x_2yx_2^{-1}x_1^{-1}y^{-1}\big) \\
&= \psi_g\big(x_1 \underbrace{\big(x_2yx_2^{-1}y^{-1}\big)}_{\in \boldsymbol{G}'} x_1^{-1}x_1yx_1^{-1}y^{-1}\big) = \psi_g\big(\big(x_2yx_2^{-1}y^{-1}\big)\big(x_1yx_1^{-1}y^{-1}\big)\big) \\
&= \psi_g\big([x_2, y] \cdot [x_1, y]\big) = [v_1, w]_g + [v_2, w]_g.
\end{aligned} \tag{10}$$

Here we used that $\boldsymbol{G}'$ is fixed elementwise under the inner automorphism given by x_1 due to (7). The last equality follows, because Condition 2 forces $\boldsymbol{G}'$ to be commutative. From (9) and (10), the function $[\cdot,\cdot]_g$ is biadditive and therefore also bilinear. Hence the assertion follows.

Ad (b): This is immediate from the definition of $[\cdot,\cdot]_g$.

Ad (c): We noted already in Remark 4 that $\boldsymbol{G}$ is a non-commutative group. Consequently, the bilinear form $[\cdot,\cdot]_g$ is non-zero. Its radical is

$$V^{\perp} = \{v \in V \mid v \perp w \text{ for all } w \in V\}.$$

We read off from (b) that $V^{\perp} = Z(\boldsymbol{G})/\boldsymbol{N}$ and the rest is clear. ∎

Observe that the bilinear form $[\cdot,\cdot]_g$ has to be degenerate when $\dim V$ is an odd integer. See Examples 1 and 2 in Section 9.

The previous result (b) about commuting elements does not depend on the choice of the isomorphism ψ_g. Replacing g by any generator $\tilde{g}$ of the commutator group $\boldsymbol{G}'$ changes the bilinear form $[\cdot,\cdot]_g$ by a non-zero factor $k \in \mathrm{GF}(p)$, that is $[\cdot,\cdot]_{\tilde{g}} = k[\cdot,\cdot]_g$. But the orthogonality relations with respect to these two forms are identical. We could even rule out the isomorphism ψ_g by considering the mapping $V \times V \to \boldsymbol{G}' : (x\boldsymbol{N}, y\boldsymbol{N}) \mapsto [x,y]$. The proof of Theorem 2 shows that this is a non-zero alternating bilinear mapping of vector spaces over $\mathrm{GF}(p)$. The interpretation of our results in terms of projective geometry will also eliminate the explicit choice of an isomorphism ψ_g. See Section 7.

We end with a complete description of all vector spaces and all alternating bilinear forms arising from our construction from the above; cf. Theorem 1.

Theorem 3. *Let $\boldsymbol{G}$ be a group such that Condition 2 holds. Furthermore, let at least one of the normal subgroups of $\boldsymbol{G}$ satisfy Conditions 1 and 3. Choose $g \in \boldsymbol{G}' \setminus \{e\}$. Then the following assertions hold:*

(a) *The subgroup $\boldsymbol{N}_0 = \boldsymbol{G}'\boldsymbol{G}^{(p)}$ is normal in $\boldsymbol{G}$ and meets the requirements of Conditions 1 and 3. It yields the vector space $V_0 = \boldsymbol{G}/\boldsymbol{N}_0$ over $\mathrm{GF}(p)$, the alternating bilinear form $[\cdot,\cdot]_{g,0}$ on V_0, and the radical $V_0^\perp$.*

(b) *The set of vector spaces $\boldsymbol{G}/\boldsymbol{N}$, where $\boldsymbol{N}$ is subject to Conditions 1 and 3, is precisely the set of factor spaces V_0/S, where S is any subspace of $V_0^\perp$, up to the canonical identification from (5).*

(c) *In terms of the identification from (5) the alternating bilinear form $[\cdot,\cdot]_g$ on any vector space $\boldsymbol{G}/\boldsymbol{N} \equiv V_0/S$ as in (b) is inherited from the bilinear form $[\cdot,\cdot]_{g,0}$ on V_0.*

Proof. Ad (a): By the hypotheses of the theorem, $\boldsymbol{N}_0 \le Z(\boldsymbol{G})$ holds, whence (a) is fulfilled.

Ad (b): A subgroup $\boldsymbol{N} \le \boldsymbol{G}$ satisfies Conditions 1 and 3 if, and only if, $\boldsymbol{N}_0 \le \boldsymbol{N} \le Z(\boldsymbol{G})$ which in turn is equivalent to

$$\boldsymbol{N}_0 \le \boldsymbol{N} \qquad \text{and} \qquad S = \boldsymbol{N}/\boldsymbol{N}_0 \le Z(\boldsymbol{G})/\boldsymbol{N}_0 = V_0^\perp.$$

Ad (c): The bilinear form $[\cdot,\cdot]_{g,0}$ induces a well-defined bilinear form on V_0/S for any subspace $S \le V_0^\perp$ via $(v+S, w+S) \mapsto [v,w]_{g,0}$. This induced form coincides with $[\cdot,\cdot]_g$ by its definition. ■

6 A quadratic form

We let $p := 2$ throughout this section. We exhibit a group $\boldsymbol{G}$ and a normal subgroup $\boldsymbol{N}$ satisfying Conditions 1 and 2, but we do not yet assume Condition 3 to be fulfilled. So $\boldsymbol{G}' = \{e, g\}$, say, and $g = g^{-1} \ne e$. Hence the vector space $V = \boldsymbol{G}/\boldsymbol{N}$ and the (only) isomorphism $\psi_g : (\boldsymbol{G}', \cdot) \to \big(\mathrm{GF}(2), +\big)$ are at our disposal. In the sequel the group

$$\boldsymbol{K} := \{x \in Z(\boldsymbol{G}) \mid x^2 = e\} \le Z(\boldsymbol{G}) \tag{11}$$

will play an important role.

Our first aim is merely to define a mapping $\boldsymbol{G} \to \mathrm{GF}(2)$ by the assignment $x \mapsto \psi_g(x^2)$. This is possible if, and only if, the following holds:

Condition 4. $\boldsymbol{G}$ is a group such that all its squares belong to its commutator group, i.e., $\boldsymbol{G}^{(2)} \subseteq \boldsymbol{G}'$.

Remark 6. We note that Conditions 2 and 4 imply

$$\boldsymbol{G}^{(2)} = \boldsymbol{G}',$$

since otherwise $\boldsymbol{G}^{(2)} = \{e\}$ would force $\boldsymbol{G}$ to be commutative, a contradiction to Remark 4.

We continue by demanding that also Condition 4 is satisfied. Our second aim is to find necessary and sufficient conditions for the mapping[2]

$$Q:\ V \to \mathrm{GF}(2) : v = x\boldsymbol{N} \mapsto \psi_g(x^2) \tag{12}$$

to be well-defined. This is the case if, and only if,

$$x^2 = xaxa \quad \text{for all} \quad x \in \boldsymbol{G} \quad \text{and all} \quad a \in \boldsymbol{N}. \tag{13}$$

Let us consider first of all the particular case $x = e$ which yields the necessary condition $a^2 = e$ for all $a \in \boldsymbol{N}$. As $\boldsymbol{N} = \{e\}$ is impossible due to $e \neq g \in \boldsymbol{N}$, we continue by assuming the following to be true:

Condition 5. The normal subgroup $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ has exponent 2.

Now, returning to the general case, we can use Condition 5 to rewrite (13) in the form

$$x^2 = x^2(x^{-1}a^{-1}xa) \quad \text{for all} \quad x \in \boldsymbol{G} \quad \text{and all} \quad a \in \boldsymbol{N}, \tag{14}$$

because $a = a^{-1}$. Cancelling x^2 shows that (14) holds precisely when $\boldsymbol{N}$ is in the centre of $\boldsymbol{G}$. Hence, we also have to impose Condition 3 to be valid.

Conversely, with all five conditions at hand we obtain that the mapping Q in (12) is indeed well defined. We notice that under these circumstances

$$\{e\} = \boldsymbol{N}^{(2)} \neq \{e, g\} = \boldsymbol{G}' = \boldsymbol{G}^{(2)} \trianglelefteq \boldsymbol{N} \trianglelefteq \boldsymbol{K} \trianglelefteq Z(\boldsymbol{G}) \triangleleft \boldsymbol{G} \tag{15}$$

is satisfied. We are now in a position to describe the mapping Q in detail.

Theorem 4. *Suppose that the group $\boldsymbol{G}$ and the normal subgroup $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ satisfy Conditions* 1–5 *for $p = 2$. Then the following assertions hold:*

(a) *The mapping $Q : V \to \mathrm{GF}(2)$ given by* (12) *is a quadratic form.*

(b) *The polar form of Q equals to the alternating bilinear form given in* (8)*. Consequently, Q is non-zero.*

(c) *The restriction of Q to the radical $V^\perp$ is a linear form $V^\perp \to \mathrm{GF}(2)$ with kernel $\boldsymbol{K}/\boldsymbol{N} \leq V^\perp$. Hence either $\boldsymbol{K}/\boldsymbol{N} = V^\perp$ or $\boldsymbol{K}/\boldsymbol{N}$ is a hyperplane of $V^\perp$.*

Proof. Ad (a) and (b): In order to show that Q is a quadratic form, we have to verify two conditions. Firstly, $Q(kv) = k^2 Q(v)$ for all $k \in \mathrm{GF}(2)$ and all $v \in V$. This follows from $Q(o) = \psi_g(e^2) = 0$ for $k = 0$ and is obviously true for $k = 1$. Secondly, it remains to establish that the mapping

$$V \times V \to \mathrm{GF}(2) :\ (v, w) \mapsto Q(v + w) - Q(v) - Q(w)$$

is biadditive and hence bilinear. Letting $v = x\boldsymbol{N}$, $w = y\boldsymbol{N}$ with $x, y \in \boldsymbol{G}$ gives

$$(xy)^2 x^{-2} y^{-2} = x^{-2}(xy)^2 y^{-2} = x^{-1}yxy^{-1} = [x^{-1}, y]. \tag{16}$$

[2]We refrain from writing Q_g, since there is only one choice for g, even though we maintain the notation $[\cdot,\cdot]_g$ from the previous section.

Here the first equation sign holds, because $\boldsymbol{G}^{(2)}$ is a commutative group by Remark 6, which allows to rearrange squares. Application of ψ_g permits us to express (16) as

$$Q(v+w) - Q(v) - Q(w) = [-v, w]_g = [v, w]_g. \tag{17}$$

Since $[\cdot,\cdot]_g$ is non-zero, so is Q. This completes the proof of (a) and (b).

Ad (c): The restriction of Q to the radical $V^\perp = Z(\boldsymbol{G})/\boldsymbol{N}$ is additive by (17). Hence $Q|V^\perp$ is a linear form in GF(2). By its definition, $Q|V^\perp$ vanishes precisely on the set $\boldsymbol{K}/\boldsymbol{N}$, which is therefore all $V^\perp$, or one of its hyperplanes. ■

Our final result of this section is in the spirit of Theorems 1 and 3:

Theorem 5. *Let $\boldsymbol{G}$ be a group such that Conditions* 2 *and* 4 *hold for $p = 2$. Furthermore, let at least one of the normal subgroups of $\boldsymbol{G}$ satisfy Conditions* 1, 3, *and* 5. *Then the following assertions hold:*

(a) *The normal subgroup $\boldsymbol{N}_0 = \boldsymbol{G}'\boldsymbol{G}^{(2)} = \boldsymbol{G}' = \boldsymbol{G}^{(2)} \trianglelefteq \boldsymbol{G}$ meets the requirements of Conditions* 1, 3, *and* 5. *It yields the vector space $V_0 = \boldsymbol{G}/\boldsymbol{N}_0$ over* GF(p), *the quadratic form Q_0 on V_0, and the subspace $\boldsymbol{K}/\boldsymbol{N}_0 \leq V_0^\perp$.*

(b) *The set of vector spaces $\boldsymbol{G}/\boldsymbol{N}$, where $\boldsymbol{N}$ is subject to Conditions* 1, 3, *and* 5, *is precisely the set of factor spaces V_0/S, where S is any subspace of $\boldsymbol{K}/\boldsymbol{N}_0$, up to the canonical identification from* (5).

(c) *In terms of the identification from* (5) *the quadratic form Q on a vector space $\boldsymbol{G}/\boldsymbol{N} \equiv V_0/S$ as in* (b) *is inherited from the quadratic form Q_0 on V_0.*

Proof. Ad (a): By the hypotheses of the theorem and (15), $\boldsymbol{G}' = \boldsymbol{G}^{(2)} = \boldsymbol{N}_0 \trianglelefteq \boldsymbol{K} \trianglelefteq Z(\boldsymbol{G})$, whence (a) is fulfilled.

Ad (b): A subgroup $\boldsymbol{N} \leq \boldsymbol{G}$ satisfies Conditions 1, 3 and 5 if, and only if, $\boldsymbol{N}_0 \leq \boldsymbol{N} \leq \boldsymbol{K}$ which in turn is equivalent to

$$\boldsymbol{N}_0 \leq \boldsymbol{N} \qquad \text{and} \qquad S = \boldsymbol{N}/\boldsymbol{N}_0 \leq \boldsymbol{K}/\boldsymbol{N}_0.$$

Ad (c): The quadratic form Q_0 induces a well-defined quadratic form on V_0/S for any subspace $S \leq \boldsymbol{K}/\boldsymbol{N}_0$ via $v + S \mapsto Q_0(v)$, because $Q_0(v+s) = Q_0(v) + Q_0(s) + [v,s]_{g_0} = Q_0(v)$ for all $s \in S$. This induced form coincides with Q by its definition. ■

Under the assumptions of Theorem 5 suppose that $\boldsymbol{K} < Z(\boldsymbol{G})$. Then there exists a subgroup $\boldsymbol{N}$ with $\boldsymbol{K} < \boldsymbol{N} \leq Z(\boldsymbol{G})$, whence Condition 5 is violated, whereas Conditions 1–3 are satisfied. This means that the vector space $\boldsymbol{G}/\boldsymbol{N}$ is endowed with an alternating bilinear form by Theorem 3, but there exists no quadratic form on $\boldsymbol{G}/\boldsymbol{N}$ as in Theorem 5; see Examples 1 and 2 in Section 9.

7 Symplectic polar spaces

Our results from the preceding sections allow a natural interpretation in terms of projective geometry. Let V be an $(n+1)$-dimensional[3] vector space over a field F. Recall that the *points* of the *projective space* on V are its one-dimensional subspaces ("rays through the origin"). We write $\mathbb{P}(V)$ for the set of all such points. Likewise, each subspace S of V gives rise to a set $\mathbb{P}(S)$ of points. If $\dim S = k+1$ then $\mathbb{P}(S) \subseteq \mathbb{P}(V)$ is called a *k-flat* or *k-dimensional projective subspace*. In particular, $\mathbb{P}(V)$ is the only n-flat, i.e., its projective dimension is n. We use the familiar

[3]We restrict ourselves to the finite-dimensional case even though several results from below could be carried over – *mutatis mutandis* – to spaces of infinite dimension.

terminology for low-dimensional flats: *lines*, *planes*, and *solids* have projective dimension 1, 2, and 3, respectively. *Hyperplanes* of $\mathbb{P}(V)$ are those flats $\mathbb{P}(S)$ where S has codimension 1 in V.

Assume now that $\big(V, [\cdot,\cdot]\big)$ is a *symplectic vector space*. So it is endowed with a non-degenerate alternating bilinear form $[\cdot,\cdot]$, and $n+1 =: 2r$ is even. For each subset $W \subseteq V$ we denote by $W^\perp$ its *orthogonal subspace*, i.e. the set of all vectors in V which are orthogonal to every vector in W. In particular, $v^\perp$ is a subspace with codimension 1 for each vector $v \in V \setminus \{o\}$. In projective terms we obtain a *null polarity*[4], i.e. the mapping which assigns to each point Fv its *null hyperplane* $\mathbb{P}(v^\perp)$. More generally, one can associate with each k-flat $\mathbb{P}(S)$ the $(n-k-1)$-flat $\mathbb{P}(S^\perp)$; it equals the intersection of all hyperplanes $\mathbb{P}(v^\perp)$, as Fv ranges over all points of $\mathbb{P}(S)$. A subspace $S \leq V$ is called *totally isotropic* if $S \leq S^\perp$. We use the same terminology for the flat $\mathbb{P}(S)$. The *symplectic polar space* associated with $\big(V, [\cdot,\cdot]\big)$ is the point set $\mathbb{P}(V)$ together with the set of all totally isotropic flats. All maximal totally isotropic flats have projective dimension $r-1$. It is common to denote this polar space by $\mathcal{W}_{2r-1}(F)$ and, in particular $\mathcal{W}_{2r-1}(q)$ if $F = \mathrm{GF}(q)$ is a Galois field. For each r and each F there is a unique symplectic polar space to within isomorphisms; see [28, 29], and the references therein.

Two (not necessarily distinct) points Fv, Fw of $\mathcal{W}_{2r-1}(F)$ are said to be *conjugate* if $v \in w^\perp$ (or $w \in v^\perp$). In other words: Two points are conjugate if one of them is in the null hyperplane of the other. Two distinct points are conjugate precisely when they are on a common totally isotropic line. Each point is self-conjugate.

It is now a straightforward task to establish a neat connection between our previous results and symplectic polar spaces:

Theorem 6. *Suppose that a group $\boldsymbol{G}$ and its centre $Z(\boldsymbol{G}) =: \boldsymbol{N}$ satisfy Conditions* 1–3 *for some prime number p. Furthermore, let $V := \boldsymbol{G}/Z(\boldsymbol{G})$ be finite and let an alternating bilinear form $[\cdot,\cdot]_g$ be defined as in* (8)*. Then the following hold:*

(a) *$\big(V, [\cdot,\cdot]_g\big)$ gives rise to a finite symplectic polar space $\mathcal{W}_{2r-1}(p)$.*

(b) *The totally isotropic flats of $\mathcal{W}_{2r-1}(p)$ have the form $\mathbb{P}\big(\boldsymbol{C}/Z(\boldsymbol{G})\big)$, where $\boldsymbol{C}$ ranges over the set of all commutative subgroups of $\boldsymbol{G}$ which contain the centre $Z(\boldsymbol{G})$. In particular, the points of $\mathcal{W}_{2r-1}(p)$ have the form $\boldsymbol{C}/Z(\boldsymbol{G})$, where $\boldsymbol{C} := \langle x\rangle Z(\boldsymbol{G})$ and $x \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$.*

(c) *Two elements $x, y \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$ commute if, and only if, the corresponding points of $\mathcal{W}_{2d-1}(p)$ are conjugate.*

Proof. Ad (a): By Theorem 2 (c), the form $[\cdot,\cdot]_g$ is non-degenerate. Therefore $\dim V =: 2r$ is even and the assertion follows.

Ad (b): By (4), any subspace of V has the form $\boldsymbol{S}/Z(\boldsymbol{G})$ with $Z(\boldsymbol{G}) \leq \boldsymbol{S} \leq \boldsymbol{G}$ and *vice versa*. The subspace $\boldsymbol{S}/Z(\boldsymbol{G})$ is totally isotropic if, and only if, $[\cdot,\cdot]_g$ vanishes identically on $\boldsymbol{S}/Z(\boldsymbol{G})$. This holds precisely when the subgroup $\boldsymbol{S}$ is commutative. The points of $\mathcal{W}_{2r-1}(p)$ are the one-dimensional subspaces of V, i.e. the subgroups of $\boldsymbol{G}/Z(\boldsymbol{G})$ which are generated by a single element $xZ(\boldsymbol{G})$ with $x \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$. Hence they have the asserted form.

Ad (c): This holds according to our definition of $[\cdot,\cdot]_g$ and the definition of conjugate points. ■

The structure of the space $\mathcal{W}_{2r-1}(p)$ from above "is" the structure of commuting elements of $\boldsymbol{G}$. Note that any $x \in \boldsymbol{G} \setminus Z(\boldsymbol{G})$ clearly commutes with all powers of x and with all elements of $Z(\boldsymbol{G})$. It is therefore natural to "condense" the commutative subgroup $\langle x\rangle Z(\boldsymbol{G}) \leq \boldsymbol{G}$ to a single entity – a point of $\mathcal{W}_{2r-1}(p)$. Also, it is natural that all elements from the centre $Z(\boldsymbol{G})$ have no meaning for $\mathcal{W}_{2r-1}(p)$, as they commute with every element of $\boldsymbol{G}$. We add in passing that the polar space $\mathcal{W}_{2r-1}(p)$ does not depend on the choice of the generator g of $\boldsymbol{G}'$ which is used to define $[\cdot,\cdot]_g$.

[4]Other names for this mapping are *symplectic polarity* and *null system*.

Remark 7. The results from Theorem 6 can be easily generalised to the settings of Theorem 2. Under these circumstances the factor space $V/V^\perp$ together with the alternating bilinear form, which is inherited from V, takes over the role of the symplectic vector space from above. This means that one gets a symplectic polar space in the projective space $\mathbb{P}(V/V^\perp)$. A k-flat of $\mathbb{P}(V/V^\perp)$ has, by definition, the form $\mathbb{P}(S/V^\perp)$ with $V^\perp \le S \le V$ and $\dim(S/V^\perp) = k+1$. It will be convenient to identify this flat with the flat $\mathbb{P}(S)$ of the projective space $\mathbb{P}(V)$. From this point of view the flats of $\mathbb{P}(V/V^\perp)$ are the flats of $\mathbb{P}(V)$ which contain $\mathbb{P}(V^\perp)$. Note that such a flat now has *two projective dimensions*. Its dimension with respect to $\mathbb{P}(V)$ is $\dim S - 1$, while its dimension with respect to $\mathbb{P}(V/V^\perp)$ is $\dim(S/V^\perp) - 1$; see Example 1.

8 Orthogonal polar spaces

In view of Section 6 we adopt the following: Let V be an $(n+1)$-dimensional vector space over a field F with characteristic 2. Let $Q : V \to F$ be a quadratic form and $[\cdot,\cdot]$ be its (alternating bilinear) polar form. We assume Q to be *non-singular*, which means that $Q(v) \neq 0$ for all non-zero vectors in the radical $V^\perp$. A subspace $S \le V$ is said to be *singular* if Q vanishes identically on S. We use the same terminology for the flat $\mathbb{P}(S)$. The singular points of $\mathbb{P}(V)$ constitute a *non-singular quadric* $\mathcal{Q}$ of $\mathbb{P}(V)$. The *orthogonal polar space* associated with (V, Q) is the point set $\mathcal{Q}$ together with all singular flats [28, 29]. This orthogonal polar space mirrors the "intrinsic geometry" of the quadric $\mathcal{Q}$, since the singular flats are precisely those flats which are entirely contained in $\mathcal{Q}$. For our purposes also the "extrinsic geometry", i.e. the points of the ambient space $\mathbb{P}(V)$ off the quadric, will be important.

All maximal singular flats of $\mathcal{Q}$ have the same projective dimension $r-1$, but the integer $r \ge 0$ depends heavily on the ground field F, the dimension of V, and the quadratic form Q. We need here only the case $F = \mathrm{GF}(2)$. It is well known that to within projective transformations only the following cases occur [28, p. 58], [30, pp. 121–126]:

n	$r-1$	Symbol	# Point set	Name
$2k$	$k-1$	$\mathcal{Q}_{2k}(2)$	$2^{2k}-1$	parabolic
$2k+1$	k	$\mathcal{Q}^+_{2k+1}(2)$	$2^{2k+1}+2^k-1$	hyperbolic
$2k+1$	$k-1$	$\mathcal{Q}^-_{2k+1}(2)$	$2^{2k+1}-2^k-1$	elliptic

For $n = 2k$ the polar form of Q is degenerate, $\dim V^\perp = 1$. Hence $V^\perp$ is a distinguished point, called *nucleus*, in the ambient projective space of $\mathcal{Q}_{2k}(2)$, but it is not a point of $\mathcal{Q}_{2k}(2)$. Otherwise the polar form of Q is non-degenerate. Below we use $\mathcal{Q}(2)$ to denote any of the quadrics from the above table.

Theorem 7. *Suppose that a group $\boldsymbol{G}$ and its subgroup $\boldsymbol{K} =: \boldsymbol{N}$ given by* (11) *satisfy Conditions* 1–5 *for $p = 2$. Furthermore, let $V := \boldsymbol{G}/\boldsymbol{K}$ be finite and let a quadratic form Q be defined as in* (12)*. Then the following hold:*

(a) *Q gives rise to a non-singular quadric $\mathcal{Q}(2)$ of $\mathbb{P}(V)$.*

(b) *The totally singular flats of $\mathcal{Q}(2)$ have the form $\mathbb{P}(\boldsymbol{T}/\boldsymbol{K})$, where $\boldsymbol{T}$ ranges over the set of all subgroups of $\boldsymbol{G}$ which have exponent* 2 *and contain $\boldsymbol{K}$. In particular, the points of $\mathcal{Q}(2)$ have the form $\boldsymbol{T}/\boldsymbol{K}$, where $\boldsymbol{T} := \langle x \rangle \boldsymbol{K}$ with $x \in \boldsymbol{G} \setminus \boldsymbol{K}$ and $x^2 = e$.*

Proof. Ad (a): By Theorem 4 (c), the restriction of the quadratic form Q to $V^\perp = Z(\boldsymbol{G})/\boldsymbol{K}$ has the kernel $\boldsymbol{K}/\boldsymbol{K}$. This is the zero-subspace of $V^\perp$, so that Q is non-singular.

Ad (b): By (4), any subspace of V has the form $\boldsymbol{S}/\boldsymbol{K}$ with $\boldsymbol{K} \le \boldsymbol{S} \le \boldsymbol{G}$ and *vice versa*. The subspace $\boldsymbol{S}/\boldsymbol{K}$ is singular if, and only if, Q vanishes identically on $\boldsymbol{S}/\boldsymbol{K}$. This holds precisely when the subgroup $\boldsymbol{S}$ has exponent 2. The points of $\mathcal{Q}(2)$ are the one-dimensional subspaces of V, i.e. the subgroups of $\boldsymbol{G}/\boldsymbol{K}$ which are generated by a single element $x\boldsymbol{K}$ with $x \in \boldsymbol{G} \setminus \boldsymbol{K}$ and $x^2 = e$. Hence they have the asserted form. ■

The structure of the polar space which is based on the quadric $\mathcal{Q}(2)$ from above "is" the structure of elements with order 2 of the group $\boldsymbol{G}$. Note that for any $x \in \boldsymbol{G}\setminus\boldsymbol{K}$ with order 2 the complex product $\langle x\rangle\boldsymbol{K}$ is a subgroup of $\boldsymbol{G}$ with exponent 2. It is therefore natural to "condense" the subgroup $\langle x\rangle\boldsymbol{K} \leq \boldsymbol{G}$ to a single entity – a point of $\mathcal{Q}(2)$. In our further discussion we have to distinguish two cases:

If $n = 2k+1$ is odd then the polar form of Q is non-degenerate which implies $\boldsymbol{K} = Z(\boldsymbol{G})$. So the results of Theorems 6 and 7 can be merged immediately. We obtain a symplectic polar space which is "refined" by an orthogonal one. The fact that subgroups of exponent 2 are commutative is mirrored in the fact that singular subspaces are totally isotropic.

If $n = 2k$ is even then $\boldsymbol{K} \neq Z(\boldsymbol{G})$. The point $V^\perp = Z(\boldsymbol{G})/\boldsymbol{K}$ is the nucleus of the quadric $\mathcal{Q}_{2k}(2)$. We have here the orthogonal polar space given by $\mathcal{Q}_{2k}(2)$ and the symplectic polar space $\mathcal{W}_{2k-1}(2)$ which is defined in $\mathbb{P}(V/V^\perp)$ according to Remark 7. It is well known that these two spaces are isomorphic. An isomorphism is given by "joining the quadric with its nucleus": If $\mathbb{P}(S)$ is a singular subspace of $\mathcal{Q}_{2k}(2)$ then its join with the point $V^\perp$, i.e. $\mathbb{P}(S+V^\perp)$, is a totally isotropic subspace of $\mathbb{P}(V/V^\perp)$ and *vice versa*. In algebraic terms this gives the following bijection from the set of all subgroups $\boldsymbol{T}$ with exponent 2 and $\boldsymbol{K} \leq \boldsymbol{T} \leq \boldsymbol{G}$ onto the set of all commutative subgroups $\boldsymbol{C}$ with $Z(\boldsymbol{G}) \leq \boldsymbol{C} \leq \boldsymbol{G}$:

$$\boldsymbol{T} \mapsto \boldsymbol{C} := \boldsymbol{T}Z(\boldsymbol{G}).$$

9 Illustrative examples from quantum theory

Example 1. We consider the *complex Pauli matrices*

$$\sigma_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{18}$$

The matrices $i^\alpha\sigma_\beta$ with $\alpha \in \{0,1,2,3\}$ and $\beta = \{0,x,y,z\}$ constitute the *Pauli group* of order 16, which is now our $\boldsymbol{G}$. It acts on the two-dimensional complex Hilbert space of a single qubit. In our terminology (with $p := 2$) we have $Z(\boldsymbol{G}) = \{\pm\sigma_0, \pm i\sigma_0\}$, $\boldsymbol{G}' = \boldsymbol{G}^{(2)} = \boldsymbol{K} = \{\pm\sigma_0\}$ and $g = -\sigma_0$. The group $\boldsymbol{G}$ satisfies Conditions 2 and 4.

The normal subgroup $\boldsymbol{K} = \boldsymbol{N}_0$ satisfies Conditions 1, 3, and 5. The factor group $\boldsymbol{G}/\boldsymbol{K}$ has 2^3 elements; it gives rise to a three-dimensional vector space V_0 over GF(2) as in Theorem 2 (a) with a degenerate alternating bilinear form $[\cdot,\cdot]_{g,0}$. The projective space $\mathbb{P}(V_0)$ is the *Fano plane*; see Fig. 1. The points of the Fano plane fall into three classes: The three *dark-shaded* points form a non-degenerate quadric $\mathcal{Q}_2(2)$ (i.e. a conic). They correspond to those elements of $\boldsymbol{G} \setminus \boldsymbol{K}$ whose square is σ_0 (i.e. Hermitian matrices). The three *light-shaded* points represent the elements of $\boldsymbol{G}\setminus\boldsymbol{K}$ whose square is $-\sigma_0$ (i.e. skew-Hermitian matrices). The remaining point, which is depicted by a *double circle*, is the only point of $\mathbb{P}(V_0^\perp)$ or, in other words, the nucleus of $\mathcal{Q}_2(2)$. It represents the matrices of $Z(\boldsymbol{G})\setminus\boldsymbol{K}$, which are also skew-Hermitian. The three lines through the nucleus (bold-faced) are to be identified with the three "points" of the symplectic polar space $\mathbb{P}(V_0/V_0^\perp) \cong \mathcal{W}_1(2)$ (Fig. 2), which has projective dimension one. Its null-polarity is the identity mapping. Two operators of $\boldsymbol{G} \setminus \boldsymbol{K}$ commute if, and only if, their corresponding points are on a common line through the nucleus.

The normal subgroup $Z(\boldsymbol{G})$ satisfies Conditions 1 and 3, but not 5. The factor group $\boldsymbol{G}/Z(\boldsymbol{G})$ has 2^2 elements; it gives rise to a two-dimensional symplectic vector space V over GF(2) and the symplectic polar space $\mathcal{W}_1(2) = \mathbb{P}(V)$; see Fig. 2. The factor space $V_0/V_0^\perp$ from above and V are isomorphic (as symplectic vector spaces). Each point of $\mathcal{W}_1(2)$ is totally isotropic. We have no

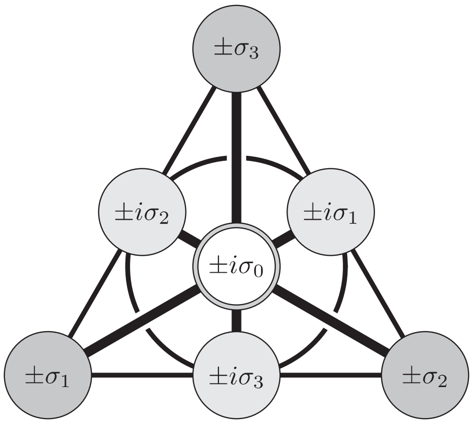

Figure 1. The fine structure of the complex single-qubit Pauli group in terms of the Fano plane.

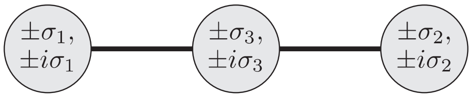

Figure 2. A coarser representation, $\mathcal{W}_1(2)$, *aka* the projection from the nucleus of the conic.

quadratic form on V. Two operators of $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ commute if, and only if, their corresponding points are identical.

Example 2. We exhibit the group comprising the Kronecker products $i^\alpha \sigma_\beta \otimes \sigma_\gamma$ with $\beta, \gamma \in \{0, x, y, z\}$; cf. (18). This group acts on the four-dimensional Hilbert space of two qubits. In contrast to Example 1, the symbol $\boldsymbol{G}$ denotes now this group of order 64. In our terminology (with $p := 2$) we have $Z(\boldsymbol{G}) = \{\pm\sigma_0 \otimes \sigma_0, \pm i\sigma_0 \otimes \sigma_0\}$, $\boldsymbol{G}' = \boldsymbol{G}^{(2)} = \boldsymbol{K} = \{\pm\sigma_0 \otimes \sigma_0\}$, and $g = -\sigma_0 \otimes \sigma_0$. Up to a change of dimensions, the situation here completely parallels that of the preceding example:

The factor group $\boldsymbol{G}/\boldsymbol{K}$ gives rise to a four-dimensional projective space $\mathbb{P}(V_0)$ over GF(2) and a non-degenerate quadric $\mathcal{Q}_4(2)$. We are not familiar with any neatly arranged picture of this projective space with its 31 points and 155 lines. However, the 15 points and 15 singular lines of $\mathcal{Q}_4(2)$, together with its nucleus and several points/lines of its ambient space, can be illustrated as in Fig. 3. There are 15 lines joining the nucleus $\mathbb{P}(V_0^\perp)$ with the points of the quadric $\mathcal{Q}_4(2)$; these lines become the "points" of the factor space $\mathbb{P}(V/V^\perp) \cong \mathcal{W}_3(2)$.

The factor group $\boldsymbol{G}/Z(\boldsymbol{G})$ yields a four-dimensional symplectic vector space V and the symplectic polar space $\mathcal{W}_3(2)$ with $\mathbb{P}(V)$ as set of points. It is depicted in Fig. 4 which is known as the *doily*[5]. We have no quadratic form on V. Two operators of $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ commute if, and only if, their corresponding points are on a totally isotropic line.

Example 3. The real orthogonal matrices $\pm I$, $\pm X$, $\pm Y$, $\pm Z$, where

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

constitute the *real Pauli group* $\boldsymbol{G}$. It acts on the Hilbert space $\mathbb{R}^2$ of a real single qubit. In our terminology (with $p := 2$) we have $\boldsymbol{G}' = \boldsymbol{G}^{(2)} = \boldsymbol{K} = Z(\boldsymbol{G}) = \{\pm I\}$ and $g = -I$. Hence there is only one possibility for factorisation, namely $\boldsymbol{G}/Z(\boldsymbol{G})$. This gives the symplectic polar space $\mathcal{W}_1(2)$ based on the projective line over GF(2) which we already encountered in Example 1. However, now this space is refined by an orthogonal polar space based on a hyperbolic quadric $\mathcal{Q}_1^+(2)$. The two points of this quadric represent those matrices in $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ whose square is I (i.e. symmetric matrices), the remaining point corresponds to matrices in $\boldsymbol{G}$ with square $-I$ (i.e. skew-symmetric matrices); see Fig. 5.

[5]Another remarkable illustration of $\mathcal{W}_3(2)$ exhibiting, like the doily, a pentagonal cyclic symmetry is the so-called *Cremona–Richmond configuration*.

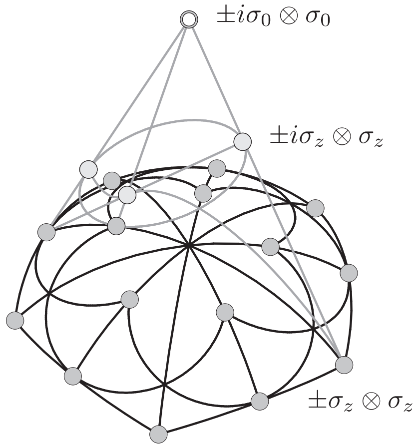

Figure 3. $\mathcal{Q}_4(2)$, its nucleus, and a portion of its ambient space as the geometry behind the complex two-qubit Pauli group.

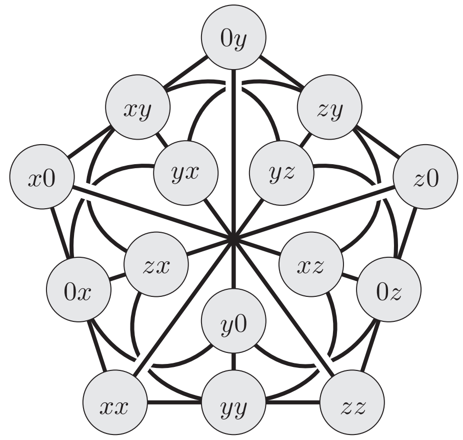

Figure 4. A coarser view in terms of $\mathcal{W}_3(2)$; xy is a short-hand for $i^{\alpha}\sigma_x \otimes \sigma_y$, $\alpha \in \{0, 1, 2, 3\}$, etc.

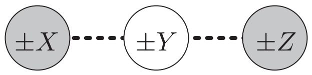

Figure 5. $\mathcal{W}_1(2)$ and $\mathcal{Q}_1^+(2)$ (shaded) of the real single-qubit Pauli group.

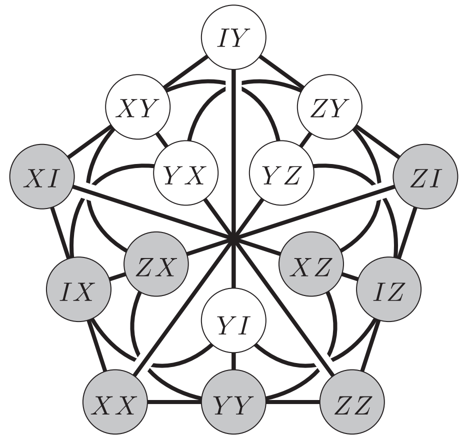

Figure 6. $\mathcal{W}_3(2)$ and $\mathcal{Q}_3^+(2)$ (shaded) of the real two-qubit Pauli group. XY is a short-hand for $\pm X \otimes Y$, etc.

Example 4. Here we deal with the group comprising the Kronecker products of the matrices from Example 3. We change notation as now this group of order 32 is denoted by $\boldsymbol{G}$. With $p := 2$ we have $\boldsymbol{G}' = \boldsymbol{G}^{(2)} = \boldsymbol{K} = Z(\boldsymbol{G}) = \{\pm I \otimes I\}$. Up to a change of dimensions, the situation here completely parallels that of the preceding example: The factor group $\boldsymbol{G}/Z(\boldsymbol{G})$ gives rise to the symplectic polar space $\mathcal{W}_3(2)$ which is refined by an orthogonal polar space based on a hyperbolic quadric $\mathcal{Q}_3^+(2)$. The nine points of this quadric represent matrices in $\boldsymbol{G} \setminus Z(\boldsymbol{G})$ whose square is $I \otimes I$ (i.e. symmetric matrices), the remaining points correspond to matrices in $\boldsymbol{G}$ which square to $-I \otimes I$ (i.e. skew-symmetric matrices); see Fig. 6.

Example 5. Finally, we mention the ($p = 3$) case of *two-qutrit* Pauli group (see also [19]). This group $\boldsymbol{G}$ possesses 3^5 elements, which can be written in the form $\omega^a X^b Y^c \otimes X^d Y^e$, where $a, b, c, d, e \in \{0, 1, 2\}$, ω is a primitive 3-rd root of unity, and X and Z are so-called shift and clock operators given by

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix},$$

respectively (see, e. g., [14, 18]). Its factor group $\boldsymbol{G}/Z(\boldsymbol{G})$ is of cardinality $3^4 = 81$ and generates the symplectic polar space $\mathcal{W}_3(3)$ of 40 points/lines, with 4 points on each line and, dually, 4 lines through each point. This case is noteworthy in two crucial aspects. First, it is one of the simplest instances where a single point of the associated polar space represents not only a single operator (up to complex multiples), but encompasses the *two distinct powers* of an operator (up to complex multiples). Second, it leads to far-reaching physical implications for the so-called black-hole analogy (see, e.g., [31]). As per the latter fact, it has recently been shown [22] that the $E_{6(6)}$ symmetric entropy formula describing black holes and black strings in $D = 5$ is intimately tied to the geometry of the generalised quadrangle $\mathrm{GQ}(2,4)$, where 27 black-hole charges correspond to the points and 45 terms in the entropy formula to the lines of $\mathrm{GQ}(2,4)$. And there exists a very intimate connection between $\mathcal{W}_3(3)$ and $\mathrm{GQ}(2,4)$ [32]. Given any point U of $\mathcal{W}_3(3)$, we can "derive" $\mathrm{GQ}(2,4)$ as follows. The points of $\mathrm{GQ}(2,4)$ are all the points of $\mathcal{W}_3(3)$ not collinear with U, whereas the lines of $\mathrm{GQ}(2,4)$ are on the one side the lines of $\mathcal{W}_3(3)$ not containing U and on the other hand hyperbolic lines through U (natural incidence). Hence, this link between the two finite geometries not only unveils the mystery why $D = 5$ black hole solutions are related with qutrits, but knowing that each point of $\mathcal{W}_3(3)$ comprises a couple $(p-1 = 3-1 = 2)$ of elements of $\boldsymbol{G}/Z(\boldsymbol{G})$, it also provides a straightforward recipe for labelling the 45 members of the entropy formula in terms of all elements of the two-qutrit Pauli group $\boldsymbol{G}$.

Following these examples the interested reader should be able to find out the symplectic and orthogonal polar spaces behind any (multiple-)qudit Pauli group as long as the rank d of the qudit is a prime number.

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. The authors are grateful to Wolfgang Herfort (Vienna) for his suggestions.

References

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

[2] Shaw R., Finite geometries and Clifford algebras, *J. Math. Phys.* **30** (1989), 1971–1984.

[3] Shaw R., Clifford algebras, spinors and finite geometries, in Group Theoretical Methods in Physics (Moscow, 1990), *Lecture Notes in Phys.*, Vol. 382, Springer, Berlin, 1991, 527–530.

[4] Shaw R., Finite geometries and Clifford algebras. III, in Clifford Algebras and Their Applications in Mathematical Physics (Montpellier, 1989), *Fund. Theories Phys.*, Vol. 47, Kluwer Acad. Publ., Dordrecht, 1992, 121–132.

[5] Shaw R., Finite geometry and the table of real Clifford algebras, in Clifford Algebras and Their Applications in Mathematical Physics (Deinze, 1993), *Fund. Theories Phys.*, Vol. 55, Kluwer Acad. Publ., Dordrecht, 1993, 23–31.

[6] Shaw R., Finite geometry, Dirac groups and the table of real Clifford algebras, in Clifford Algebras and Spinor Structures, *Math. Appl.*, Vol. 321, Kluwer Acad. Publ., Dordrecht, 1995, 59–99.

[7] Shaw R., Jarvis T.M., Finite geometries and Clifford algebras. II, *J. Math. Phys.* **31** (1990), 1315–1324.

[8] Gordon N.A., Jarvis T.M., Maks J.G., Shaw R., Composition algebras and $\mathrm{PG}(m,2)$, *J. Geom.* **51** (1994), 50–59.

[9] Planat M., Saniga M., Kibler M.R., Quantum entanglement and projective ring geometry, *SIGMA* **2** (2006), 066, 14 pages, quant-ph/0605239.

[10] Saniga M., Planat M., Finite geometries in quantum theory: from Galois (fields) to Hjelmslev (rings), *Internat. J. Modern Phys. B* **20** (2006), 1885–1892.

[11] Saniga M., Planat M., A projective line over the finite quotient ring $\mathrm{GF}(2)[x]/\langle x^3 - x\rangle$ and quantum entanglement: theoretical background, *Theoret. and Math. Phys.* **151** (2007), 474–481, quant-ph/0603051.

[12] Saniga M., Planat M., Minarovjech M., Projective line over the finite quotient ring $\mathrm{GF}(2)[x]/\langle x^3 - x\rangle$ and quantum entanglement: the Mermin "magic" square/pentagram, *Theoret. and Math. Phys.* **151** (2007), 625–631, quant-ph/0603206.

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

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

[15] Saniga M., Planat M., Pracna P., Havlicek H., The Veldkamp space of two-qubits, *SIGMA* **3** (2007), 075, 7 pages, arXiv:0704.0495.

[16] Planat M., Baboin A.-C., Qudits of composite dimension, mutually unbiased bases and projective ring geometry, *J. Phys. A: Math. Theor.* **40** (2007), F1005–F1012, arXiv:0709.2623.

[17] Planat M., Baboin A.-C., Saniga M., Multi-line geometry of qubit-qutrit and higher-order Pauli operators, *Internat. J. Theoret. Phys.* **47** (2008), 1127–1135, arXiv:0705.2538.

[18] Havlicek H., Saniga M., Projective ring line of an arbitrary single qudit, *J. Phys. A: Math. Theor.* **41** (2008), 015302, 12 pages, arXiv:0710.0941.

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

[20] Saniga M., Planat M., Pracna P., Projective ring line encompassing two-qubits, *Theoret. and Math. Phys.* **155** (2008), 905–913, quant-ph/0611063.

[21] Lévay P., Saniga M., Vrana P., Three-qubit operators, the split Cayley hexagon of order two and black holes, *Phys. Rev. D* **78** (2008), 124022, 16 pages, arXiv:0808.3849.

[22] Lévay P., Saniga M., Vrana P., Pracna P., Black hole entropy and finite geometry, *Phys. Rev. D* **79** (2009), 084036, 12 pages, arXiv:0903.0541.

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

[24] Thas K., Pauli operators of N-qubit Hilbert spaces and the Saniga–Planat conjecture, *Chaos, Solitons, Fractals*, to appear.

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

[26] Kirsch A., Beziehungen zwischen der Additivität und der Homogenität von Vektorraum-Abbildungen, *Math.-Phys. Semesterber.* **25** (1978), 207–210.

[27] Mayr U., Zur Definition der linearen Abbildung, *Math.-Phys. Semesterber.* **26** (1979), 216–222.

[28] Buekenhout F., Cameron P., Projective and affine geometry over division rings, in Handbook of Incidence Geometry, Editor F. Buekenhout, North-Holland, Amsterdam, 1995, 27–62.

[29] Cameron P.J., Projective and polar spaces, available at `http://www.maths.qmw.ac.uk/~pjc/pps/`.

[30] Hirschfeld J.W.P., Projective geometries over finite fields, 2nd ed., Clarendon Press, Oxford, 1998.

[31] Borsten L., Dahanayake D., Duff M.J., Ebrahim H., Rubens W., Black holes, qubits and octonions, *Phys. Rep.* **471** (2009), 113–219, arXiv:0809.4685.

[32] Payne S.E., Thas J.A., Finite generalized quadrangles, *Research Notes in Mathematics*, Vol. 110, Pitman (Advanced Publishing Program), Boston, MA, 1984.