Structure of Clifford groups of composite finite quantum systems

Miroslav Korbelář
(a joint work with J. Tolar)

Faculty of Electrical Engineering
Czech Technical University in Prague

korbemir@fel.cvut.cz

XLIII Workshop on Geometric Methods in Physic
Białystok

The same group appears in different areas of physics, mathematics and quantum computing under different names:

- group of symmetries of quantum kinematics in finite-dimensional quantum mechanics
- normalizer of the Weyl-Heisenberg group
- group of symmetries of the Pauli grading of the operator algebra
- Clifford group (introduced in 1998 by D. Gottesmann in his investigation of quantum error-correcting codes.)

We will use the viewpoint of the *finite-dimensional quantum mechanics* for the definition.

Finite-dimensional mechanics is motivated by approximating the configuration space of the real line ($\mathbb{R}$) by a finite set of points ($\mathbb{Z}_n$). This is the single n-level system with the Hilbert space $\mathbb{C}^n$.

More generally, the configuration space is identified with a finite abelian group $A = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. This is the composite $(n_1, \ldots, n_k)$-level system (of mutually independent subsystems) with the Hilbert space $\mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_k}$ of dimension $N = n_1 \cdots n_k$.

What are the position and momentum operators?

NOTICE: Since in finite-dimen. space no self-adjoint operators $\hat{Q}$ and $\hat{P}$ fulfill the identity $[\hat{Q},\hat{P}] = \mathbf{i}\hbar\hat{I}$ (as $\mathrm{Tr}(\hat{Q}\hat{P}-\hat{P}\hat{Q}) = 0 \neq \mathrm{Tr}(\mathbf{i}\hbar\hat{I})$), the unitary operators, fulfilling an analogical group commutator relation, are rather used.

In the single n-level system ($A = \mathbb{Z}_n$): the position and the momentum unitary operators have the following forms in the standard basis:

$$Q_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \omega_n & 0 & \dots & 0 \\ 0 & 0 & \omega_n^2 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \omega_n^{n-1} \end{pmatrix}, P_n = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

where $\omega_n = e^{2\pi\mathbf{i}/n}$, and their group commutator relation is

$$[P_n, Q_n] = P_n Q_n P_n^{-1} Q_n^{-1} = \omega_n I_n.$$

In the general composite $(n_1,\dots,n_k)$-level system (with $A = \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}$) the i-th component, for $i = 1,\dots,k$, has the position and momentum unitary operators of the form

$$I_{n_1} \otimes \dots \otimes I_{n_{i-1}} \otimes P_{n_i} \otimes I_{n_{i+1}} \otimes \dots \otimes I_{n_k}$$
$$I_{n_1} \otimes \dots \otimes I_{n_{i-1}} \otimes Q_{n_i} \otimes I_{n_{i+1}} \otimes \dots \otimes I_{n_k}$$

where $\otimes$ is the Kronecker product of matrices.

The *Heisenberg group* (sometimes called *generalized Pauli group*) is defined as

$$\mathcal{H}_{(n_1,\ldots,n_k)} = \{\lambda \cdot P_{n_1}^{i_1} Q_{n_1}^{j_1} \otimes \cdots \otimes P_{n_k}^{i_k} Q_{n_k}^{j_k} \,|\, i_1, j_1, \ldots, i_k, j_k \in \mathbb{Z}, \lambda \in \mathrm{U}(1)\},$$

and it is a subgroup of the unitary group $\mathrm{U}(N)$ for $N = n_1 \ldots n_k$.

The *Clifford group* consists of all unitary operators U such that their action of inner automorphisms leaves the group $\mathcal{H}_{(n_1,\ldots,n_k)}$ invariant:

$$\mathcal{C}_{(n_1,\ldots,n_k)} = \{U \in \mathrm{U}(N) |\, U \cdot \mathcal{H}_{(n_1,\ldots,n_k)} \cdot U^{-1} = \mathcal{H}_{(n_1,\ldots,n_k)}\}$$

i.e., it is the *normalizer* of the Heisenberg group $\mathcal{H}_{(n_1,\ldots,n_k)}$ in the unitary group $\mathrm{U}(N)$.

Since these inner automorphisms (Clifford operations), are not affected by phase factors, it is natural to study the *projective Clifford group* as the quotient

$$\overline{\mathcal{C}}_{(n_1,\ldots,n_k)} = \mathcal{C}_{(n_1,\ldots,n_k)} / \sim$$

where $\sim$ means the equivalence of matrices up to a scalar multiple. Similarly we define the *projective Heisenberg group*

$$\overline{\mathcal{H}}_{(n_1,\ldots,n_k)} = \mathcal{H}_{(n_1,\ldots,n_k)} / \sim$$

that is isomorphic to $\mathbb{Z}_{n_1}^2 \oplus \cdots \oplus \mathbb{Z}_{n_k}^2$.

The acting of $\overline{\mathcal{C}}_{(n_1,\dots,n_k)}$ on $\overline{\mathcal{H}}_{(n_1,\dots,n_k)} \cong \mathbb{Z}_{n_1}^2 \oplus \cdots \oplus \mathbb{Z}_{n_k}^2$ can be described by a matrix group, a sort of symplectic group, that we denote as $\mathrm{Sp}_{[n_1,\dots,n_k]}$. It holds that

$$\mathcal{C}_{(n_1,\dots,n_k)}/\mathcal{H}_{(n_1,\dots,n_k)} \cong \overline{\mathcal{C}}_{(n_1,\dots,n_k)}/\overline{\mathcal{H}}_{(n_1,\dots,n_k)} \cong \mathrm{Sp}_{[n_1,\dots,n_k]}$$

and we obtain the (natural) short exact sequences

$$1 \to \mathcal{H}_{(n_1,\dots,n_k)} \xrightarrow{\nu} \mathcal{C}_{(n_1,\dots,n_k)} \xrightarrow{\pi} \mathrm{Sp}_{[n_1,\dots,n_k]} \to 1$$

and

$$1 \to \overline{\mathcal{H}}_{(n_1,\dots,n_k)} \xrightarrow{\overline{\nu}} \overline{\mathcal{C}}_{(n_1,\dots,n_k)} \xrightarrow{\overline{\pi}} \mathrm{Sp}_{[n_1,\dots,n_k]} \to 1.$$

A natural question for such sequences is:

Is the middle group a semidirect product of the groups on the egdes?

Several important symmetry groups have a structure of a semidirect product:

1. Galilean group (symmetries of classical mechanics)
2. Fedorov groups (symmetries of crystal lattices)
3. Poincaré group (symmetries of Minkowski spacetime in special relativity)
4. Poincaré-Heisenberg group (describing quantum mechanical systems under relativistic symmetries)

and other groups (Bondi-Metzner-Sachs group in general relativity and string theory, gauge-spacetime symmetry groups etc.)

It is well known, that for an abelian group $A = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ of an odd order, i.e., when $|A| = n_1 \cdots n_k$ is odd, the Clifford and the projective Clifford group admit the semidirect structure.

For $|A|$ even, the answer seemed to be known also, as this case in the literature is usually treated with help of a metaplectic group (a double cover of the symplectic group) and half-integer lattices states ("ghost states") are used. There are also special results confirming the non-existence of the semidirect structure (e.g., for $n_1 = \cdots = n_k$, $k \geq 2$). But a general proof seemed to be missing....

Theorem (K, Tolar 2023)

$\overline{\mathcal{C}}_n$ is a semid. product related to its natural exact sequence iff $n \neq 0 \pmod 4$.

Conjecture (K, Tolar 2023)

Let A be a finite abelian group of an even order. Then the following conditions are equivalent:

- $\mathcal{C}_{(n_1,\ldots,n_k)}$ is a semidirect product related to its natural exact sequence (with $\mathcal{H}_{(n_1,\ldots,n_k)}$).
- $\overline{\mathcal{C}}_{(n_1,\ldots,n_k)}$ is a semidirect product related to its natural exact sequence (with $\overline{\mathcal{H}}_{(n_1,\ldots,n_k)}$).
- $|A| = 2 \pmod 4$.

Definition (of the semidirect product)

Let H and S be groups and $\varphi : S \to Aut(H)$ be a group homomorphism into the group $Aut(H)$ of all automorphisms of H.
The (outer) semidirect product $H \rtimes_\varphi S$ is defined as a group with the underlying set $H \times S$ and the multiplication defined by the formula

$$(u, a) \cdot (v, b) = (u \cdot \varphi(a)(v), ab)$$

for all $(u, a), (v, b) \in H \times S$.

Example: The group $\mathrm{Aff}(V)$ of all affine symmetries of a vector space V

is generated by all linear symmetries and all translations, i.e., a general symmetry is

$$f_{\vec{u},A}(\vec{x}) = \vec{u} + A\vec{x} \quad \forall \vec{x} \in V$$

where $\vec{u} \in V$ and $A \in GL(V)$. There is an isomorphism

$$\mathrm{Aff}(V) \cong V \rtimes_\varphi GL(V), \quad \text{where} \quad \varphi(A)(\vec{u}) = A\vec{u}$$

$$f_{\vec{u},A} \mapsto (\vec{u}, A)$$

because

$$f_{\vec{u},A} \circ f_{\vec{v},B}(\vec{x}) = \vec{u} + A(\vec{v} + B\vec{x}) = (\vec{u} + A\vec{v}) + AB\vec{x} = f_{\vec{u}+\varphi(A)(\vec{v}),AB}(\vec{x}).$$

For a short exact sequence of groups

$$1 \longrightarrow H \xrightarrow{\nu} G \xrightarrow{\pi} S \longrightarrow 1$$

the following are equivalent:

(i) There is a group homomorphism $\varphi : S \to Aut(H)$ and a group isomorphism $\Phi : H \rtimes_\varphi S \to G$ such that $\Phi(u,1) = \nu(u)$ and $\pi(\Phi(1,a)) = a$ for every $u \in H$ and $a \in S$.

(ii) The sequence is right-splitting, i.e., there is a homomorphism $\vartheta : S \to G$ such that $\pi \circ \vartheta = id_S$.

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "\nu"] & G \arrow[r, "\pi"] & S \arrow[r] \arrow[l, bend right, dashed, "\vartheta"'] & 1 \end{tikzcd}$$

In particular, φ can then be expressed by means of ϑ in the form

$$\varphi(a)(u) = \nu^{-1}(\vartheta(a) \cdot \nu(u) \cdot \vartheta(a)^{-1})$$

for all $u \in H$ and $a \in S$.

Theorem (K, Tolar 2026)

The Conjecture holds, i.e.,

for $|A|$ even, both Clifford and projective Clifford groups are natural semidirect products if and only if $|A| = 2m$, where m is an odd number.

The key parts of the proof:

1. exact sequence for Clifford group splits $\Rightarrow$ exact sequence for projective Clifford group splits
2. reducing the number of components of the system:
   For $1 \leq \ell < k$: exact sequence for $\overline{\mathcal{C}}_{(n_1,\ldots,n_k)}$ splits $\Rightarrow$ exact sequence for $\overline{\mathcal{C}}_{(n_1,\ldots,n_\ell)}$ splits
3. exact sequence for $\overline{\mathcal{C}}_{(n,m)}$ does NOT split for $n = 2 \pmod 4$ and $m = 2 \pmod 4$
   This was proved with help of relations between 5 generators of the symplectic group $\mathrm{Sp}_{[n,m]}$.
4. exact sequence for $\overline{\mathcal{C}}_{(n)}$ does NOT split for $n = 0 \pmod 4$ (proved in 2023)

Note: In the course of finishing the manuscript we found a paper by C. Galindo (2026) in which our Conjecture is proved using methods of finite group cohomology.

Some related comments:

- Systems of different dimensions in their subsystems are considered in asymmetric entanglement theory (Horodecki 1997) or quantum cryptography (Bechmann-Pasquinucci and Tittel 2000).
- It has been proven by Raussendorf, Okay, Zurel, Feldmann (2023) that a standard discrete Wigner function constructed from an operator basis is strictly Clifford-covariant and simultaneously represent Pauli measurements positively iff the dimension is odd.
  This shows that the existence of a semidirect structure of Clifford groups and the existence of Clifford-covariant Wigner functions are NOT equivalent notions. The case when these notions do not coincide is the case of dimension $2m$, with m being an odd number.
- It was proved by Feng and Luo (2024) that the Clifford orbit approach and the stabilizer group approach are equivalent if and only if the system dimension is square-free.

So the special single case of the dimension $2m$, where m is odd, raises the question of which other theoretical relations and applications (apart from the semidirect structure) this case may allow.

Bechmann-Pasquinucci H, Tittel W 2000 Quantum Cryptography using larger alphabets *Phys. Rev. A* **61** 062308.

Feng L, Luo S 2024 Clifford orbits and stabilizer states *J. Phys. A: Math. Theor.* **57** 395304.

Galindo C 2026 Splitting of Clifford groups associated to finite abelian groups. arxiv: 2603.24743

Horodecki P 1997 Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A* **232(5)** 333–339.

Korbelář M, Tolar J 2012 Symmetries of the finite Heisenberg group for multipartite systems. *J. Phys. A: Math. Theor.* **45** 285305 (18pp). arXiv: 1210.6167 [quant-ph]

Korbelář M, Tolar J 2023 Clifford group is not a semidirect product in dimensions N divisible by four. *J. Phys. A: Math. Theor.* **56** 275304 (28pp). arXiv: 2305.13178 [quant-ph]

Raussendorf R, Okay C, Zurel M, Feldmann P 2023 The role of cohomology in quantum computation with magic states. *Quantum* **7**. `https://doi.org/10.22331/q-2023-04-13-979`

Thank you for your attention!

Definition of the symplectic group $\mathrm{Sp}_{[n_1,\dots,n_k]}$

Let $\mathcal{S}_{[n_1,\dots,n_k]}$ be a set consisting of $k \times k$ matrices $\mathbb{H}$ composed of 2×2 blocks of the form

$$(\mathbb{H})_{ij} = \tfrac{n_i}{\gcd(n_i,n_j)} A_{ij}, \quad \text{where } A_{ij} \text{ are } 2 \times 2 \text{ matrices over } \mathbb{Z}.$$

An adjoint $\mathbb{H}^* \in \mathcal{S}_{[n_1,\dots,n_k]}$ of $\mathbb{H} \in \mathcal{S}_{[n_1,\dots,n_k]}$ is defined by

$$(\mathbb{H}^*)_{ij} = \tfrac{n_i}{\gcd(n_i,n_j)} A_{ji}^T, \text{ for } i,j \in \{1,\dots,k\}.$$

We consider $\mathcal{S}_{[n_1,\dots,n_k]}$ as a monoid with the usual multiplication of matrices and a congruence $\equiv$ defined as

$$\mathbb{H} \equiv \mathbb{G} \ \Leftrightarrow \ \mathbb{D}\mathbb{H} = \mathbb{D}\mathbb{G} \pmod{\mathrm{lcm}(n_1,\dots,n_k)} \quad \text{for} \quad \mathbb{H}, \mathbb{G} \in \mathcal{S}_{[n_1,\dots,n_k]}$$

where $\mathbb{D} = \mathrm{diag}\left(\frac{\mathrm{lcm}(n_1,\dots,n_k)}{n_1} I_2, \dots, \frac{\mathrm{lcm}(n_1,\dots,n_k)}{n_k} I_2\right)$. Denote by $[\mathbb{H}]$ the congruence class of $\mathbb{H}$.

The *symplectic group* $\mathrm{Sp}_{[n_1,\dots,n_k]}$ is now defined as

$$\mathrm{Sp}_{[n_1,\dots,n_k]} = \{\ [\mathbb{H}] \mid \ \mathbb{H} \in \mathcal{S}_{[n_1,\dots,n_k]}, \ \ \mathbb{H}^*\mathbb{J}\mathbb{H} \equiv \mathbb{J}\}.$$

where $\mathbb{J} = \mathrm{diag}(J_2, \dots, J_2) \in \mathcal{S}_{[n_1,\dots,n_k]}$ and $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.