JOURNAL OF MATHEMATICAL PHYSICS **58**, 032201 (2017)

Maximally symmetric stabilizer MUBs in even prime-power dimensions

Claudio Carmeli,[1] Jussi Schultz,[2] and Alessandro Toigo[3]

[1]*D.I.M.E., Università di Genova, Via Magliotto 2, Savona I-17100, Italy*
[2]*Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, Turku FI-20014, Finland*
[3]*Dipartimento di Matematica, Politecnico di Milano, Piazza Leonardo da Vinci 32, Milano I-20133, Italy and I.N.F.N., Sezione di Milano, Via Celoria 16, Milano I-20133, Italy*

(Received 5 November 2016; accepted 19 February 2017; published online 22 March 2017)

One way to construct a maximal set of mutually unbiased bases (MUBs) in a prime-power dimensional Hilbert space is by means of finite phase-space methods. MUBs obtained in this way are covariant with respect to some subgroup of the group of all affine symplectic phase-space transformations. However, this construction is not canonical: as a consequence, many different choices of covariance subgroups are possible. In particular, when the Hilbert space is 2^n dimensional, it is known that covariance with respect to the full group of affine symplectic phase-space transformations can never be achieved. Here we show that in this case there exist two essentially different choices of maximal subgroups admitting covariant MUBs. For both of them, we explicitly construct a family of 2^n covariant MUBs. We thus prove that, contrary to the odd dimensional case, maximally covariant MUBs are very far from being unique in even prime-power dimensions. *Published by AIP Publishing.* [http://dx.doi.org/10.1063/1.4977830]

I. INTRODUCTION

The phase-space approach to finite-dimensional quantum mechanics is a very powerful tool in describing quantum systems with finitely many degrees of freedom, and as such it has found numerous applications in quantum tomography and quantum information theory.[1–7] This approach works when the Hilbert space of the system is $\mathcal{H} = \ell^2(\mathbb{F})$, where $\mathbb{F}$ is any Galois field, and it employs the analogy of $\mathcal{H}$ with the Hilbert space $L^2(\mathbb{R})$ of a free quantum particle moving along the real line. The similarity is carried over by defining a finite dimensional counterpart of the usual Wigner map, and then using it to establish a correspondence between states on $\mathcal{H}$ and functions on the finite phase-space $\Omega = \mathbb{F}^2$.

The Wigner map is only one instance of the many objects that can be adapted from the infinite dimensional setting by simply turning the real numbers $\mathbb{R}$ into a finite field $\mathbb{F}$ with q elements. Other examples of this correspondence are the finite Heisenberg group and its Schrödinger representation on $\mathcal{H}$,[8–10] as well as the finite symplectic group and the associated metaplectic representation.[11–16] The construction we are primarily interested in is the one that replaces the quadrature observables on $L^2(\mathbb{R})$ with a set of $q + 1$ complementary orthonormal bases on $\mathcal{H}$. Since such bases constitute a set of $q + 1$ mutually unbiased bases (MUBs), the phase-space approach provides a method for constructing a maximal set of MUBs in the q-dimensional Hilbert space $\mathcal{H}$.[17–21]

Maximal sets of MUBs constructed on the model of quadrature observables are sometimes referred to as *stabilizer MUBs* in order to point out their special nature among the family of all maximal MUBs in $\mathcal{H}$. Their associated orthogonal projections are in a one-to-one correspondence with the set of the affine lines of Ω in such a way that (1) all lines parallel to a given direction correspond to projections onto a fixed basis and (2) two sets of parallel lines with different directions correspond to projections onto different bases. Since there are $q + 1$ directions in Ω and q parallel lines for each direction, all the $q(q + 1)$ basis vectors are thus achieved.

Being an affine space over $\mathbb{F}$, the finite phase-space Ω carries the action of the associated group of translations V; this action clearly descends to the set of the affine lines of Ω and hence to the corresponding stabilizer MUBs described in the previous paragraph. On the other hand, the group V is represented on $\mathcal{H}$ by means of the Schrödinger representation (usually called *Pauli* or *Weyl-Heisenberg group* in finite dimensions). Then, by their very definition, stabilizer MUBs are covariant with respect to such a representation.

However, many possible unitarily inequivalent stabilizer MUBs can be defined over the same phase-space Ω. The source of this ambiguity relies entirely on the fact that one has quite many degrees of freedom in the choice of the correspondence between the lines of Ω and the bases in the MUBs. It has been shown in Ref. 22 that each equivalence class of stabilizer MUBs can be identified by means of a suitable multiplier of V, called a *Weyl multiplier*, which is uniquely determined by the class at hand. One can thus access all the relevant information about some given stabilizer MUBs by simply looking at the properties of their associated Weyl multiplier. This is a single function on $V \times V$ compared to the $q(q + 1)$ vectors of the MUBs.

One further property usually required from stabilizer MUBs is covariance with respect to additional symmetries of Ω other than the phase-space translations. This comes from the fact that, being an affine symplectic space, the phase-space Ω also carries an action of the symplectic group $\mathrm{SL}(2, \mathbb{F})$ and its subgroups. Not all stabilizer MUBs are covariant with respect to such an extended action, but only some very restricted classes. In particular, if the field $\mathbb{F}$ has even characteristic, stabilizer MUBs that are covariant with respect to the full group $\mathrm{SL}(2, \mathbb{F})$ *do not exist at all*.[22,23]

However, covariance with respect to certain subgroups of $\mathrm{SL}(2, \mathbb{F})$ is often a very important requirement, which is at the basis of many recent applications to quantum error-correcting codes,[24–26] secure quantum key distributions,[27] entropic uncertainty relations,[28,29] MUB-balanced states,[30] sharply covariant MUBs,[31,32] and unitary designs.[33,34] Hence, in the even characteristic case, it is natural to look for all possible subgroups of $\mathrm{SL}(2, \mathbb{F})$ admitting covariant stabilizer MUBs.

In this paper, we solve this problem and show that in even characteristic, maximal covariance subgroups are divided into *two* disjoint conjugacy classes, which are the finite analogues of the *maximal split* and *maximal nonsplit* toruses of $\mathrm{SL}(2, \mathbb{R})$. As in the real case, these two kinds of groups have essentially different actions on the affine lines of Ω and, correspondingly, on their respective covariant stabilizer MUBs. Indeed, while a split torus permutes the lines preserving two fixed directions, a nonsplit one cycles all the directions, acting freely on them. On the MUB side, this means that only maximal nonsplit toruses have a transitive action on the set of bases and thus are the most feasible groups for applications.

The paper is organized as follows. In Section II we recall the essential facts about finite phase-spaces, covariant MUBs, and the relation between stabilizer MUBs and Weyl multipliers. In Section III, we review the classification of all subgroups of $\mathrm{SL}(2, \mathbb{F})$ given in Refs. 35–37 and search among them for those admitting covariant stabilizer MUBs in even characteristic. Section IV gives an explicit picture of such subgroups, and it shows that they are either the split or nonsplit toruses in $\mathrm{SL}(2, \mathbb{F})$. The paper concludes in Section V providing an explicit construction of some maximally covariant stabilizer MUBs in even characteristic. More precisely, we describe a family of q inequivalent such MUBs, thus proving in particular that maximally covariant MUBs are not unique. This points out a basic difference with the odd characteristic case, where a unique equivalence class of maximally covariant stabilizer MUBs is known to exist.

II. COVARIANT QUADRATURE SYSTEMS AND WEYL MULTIPLIERS

The present section is a brief exposition of the main facts of Ref. 22 that will be needed in the following. We refer to Lang's book[38] for further details on finite fields and Galois theory.

Throughout the paper, $\mathbb{F}$ is a finite field with characteristic p. This implies that $|\mathbb{F}| = p^n$ for some positive integer n, where we denote by $|\cdot|$ the cardinality of a set. Moreover, $\mathbb{F}$ is an n-dimensional vector space over its cyclic subfield $\mathbb{Z}_p$. In this section, the characteristic p may be either even or odd. However, our main results in Sections III–V will focus on the case $p = 2$.

The *trace* of $\mathbb{F}$ is the $\mathbb{Z}_p$-linear functional $\mathrm{Tr} : \mathbb{F} \to \mathbb{Z}_p$ with $\mathrm{Tr}\,\alpha = \sum_{k=0}^{n-1} \alpha^{p^k}$. We let ω_p be any p-root of unity in the complex field $\mathbb{C}$ and assume ω_p to be fixed throughout the paper. Note that $\omega_p^{\mathrm{Tr}\,\alpha}$ is a well defined quantity for all $\alpha \in \mathbb{F}$, and exactly $p - 1$ possible choices are available for ω_p.

A. Finite phase-space

In the following, the couple (Ω, V) is always a 2-dimensional affine space over the field $\mathbb{F}$, that is:

- V is a 2-dimensional vector space over $\mathbb{F}$;
- Ω is a set carrying an action of the additive Abelian group V;
- the action of V on Ω is free and transitive.

The translate of an element $x \in \Omega$ by means of a vector $\mathbf{v} \in V$ is denoted by $x + \mathbf{v}$. Clearly, $|\Omega| = |V| = |\mathbb{F}|^2$.

We let $\mathcal{D}$ be the *directions* of Ω, that is, the set of 1-dimensional subspaces of V,

$$\mathcal{D} = \{D \subset V \mid D = \{\alpha\mathbf{d} | \alpha \in \mathbb{F}\} \text{ for some nonzero } \mathbf{d} \in V\}\,.$$

If $x \in \Omega$, the *affine line* (or simply *line*) passing through x and parallel to the direction $D \in \mathcal{D}$ is the subset $x + D = \{x + \mathbf{d} \mid \mathbf{d} \in D\}$. There are $|\mathcal{D}| = |\mathbb{F}| + 1$ directions in Ω, hence $|\mathbb{F}| + 1$ different lines passing through x. Moreover, for a fixed direction $D \in \mathcal{D}$, there are $|\mathbb{F}|$ disjoint lines parallel to D, which form a partition $L_D(\Omega)$ of Ω. The set $L(\Omega) = \bigcup_{D\in\mathcal{D}} L_D(\Omega)$ is the collection of all the lines of Ω; its cardinality is $|L(\Omega)| = |\mathbb{F}|(|\mathbb{F}| + 1)$.

B. Quadrature systems

Suppose $\mathcal{H}$ is a finite dimensional Hilbert space with prime-power dimension $\dim \mathcal{H} = p^n$. A standard way to describe maximal sets of $p^n + 1$ MUBs in $\mathcal{H}$ is to take the field $\mathbb{F}$ with $|\mathbb{F}| \equiv p^n$ elements and label each vector of the maximal MUBs with a line of Ω, in such a way that

- the $|\mathbb{F}|$ vectors in the same basis correspond to the lines parallel to a fixed direction;
- different bases of the $|\mathbb{F}| + 1$ MUBs correspond to different directions.

Changing the labelings of the same MUBs clearly amounts to permuting the bases and the vectors within them. We remark that, in our approach, we regard MUBs with different labelings as *essentially distinct*. Anyway, we will not take care of irrelevant phase factors occurring in the vectors of the bases. For this purpose, the most convenient definition of MUBs is in terms of their associated rank-1 orthogonal projections as follows.

Definition 1. A quadrature system (*or simply* quadratures) *for the 2-dimensional affine space* (Ω, V) *over* $\mathbb{F}$ *and acting on the* $|\mathbb{F}|$*-dimensional Hilbert space* $\mathcal{H}$ *is a map* $\mathsf{Q} : L(\Omega) \to \mathcal{L}(\mathcal{H})$, *where* $\mathcal{L}(\mathcal{H})$ *is the set of the linear operators on* $\mathcal{H}$, *such that*

(i) $\mathsf{Q}(\mathfrak{l})$ *is a rank-*1 *orthogonal projection for all* $\mathfrak{l} \in L(\Omega)$*;*

(ii) for all $D \in \mathcal{D}$,

$$\sum_{\mathfrak{l}\in L_D(\Omega)} \mathsf{Q}(\mathfrak{l}) = \mathbb{1},$$

where $\mathbb{1} \in \mathcal{L}(\mathcal{H})$ *is the identity operator of* $\mathcal{H}$*;*

(iii) for all $D_1, D_2 \in \mathcal{D}$ *with* $D_1 \neq D_2$,

$$\mathrm{tr}\,[\mathsf{Q}(\mathfrak{l}_1)\mathsf{Q}(\mathfrak{l}_2)] = \frac{1}{|\mathbb{F}|} \qquad \textit{if } \mathfrak{l}_1 \in L_{D_1}(\Omega) \textit{ and } \mathfrak{l}_2 \in L_{D_2}(\Omega),$$

where $\mathrm{tr}\,[\cdot]$ *denotes the Hilbert space trace.*

If Q is a quadrature system for the affine space (Ω, V), its restriction $\mathsf{Q}_D = \mathsf{Q}|_{L_D(\Omega)}$ is a spectral map projecting onto an orthogonal basis, and the spectral maps Q_{D_1} and Q_{D_2} project onto two MUBs if $D_1 \neq D_2$. A quadrature system thus associates the $|\mathbb{F}| + 1$ directions of Ω with a maximal set of MUBs in $\mathcal{H}$.

We will regard two unitarily conjugate quadrature systems as essentially the same object. That is, if Q_1 and Q_2 are two quadratures for the same affine space (Ω, V), acting on possibly different Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, we say that Q_1 and Q_2 are *equivalent* if there is a unitary operator $U : \mathcal{H}_1 \to \mathcal{H}_2$ such that

$$\mathsf{Q}_2(\mathfrak{l}) = U\mathsf{Q}_1(\mathfrak{l})U^* \qquad \forall \mathfrak{l} \in L(\Omega)\,. \tag{1}$$

C. Symmetries

The natural symmetry group of the affine space (Ω, V) is the *affine group* $\mathrm{GL}(V) \rtimes V$, which is the semidirect product of the group $\mathrm{GL}(V)$ of all invertible $\mathbb{F}$-linear maps of V with the translation group V itself (where V is the normal factor). The action of $\mathrm{GL}(V) \rtimes V$ on Ω is the extension of the action of V by translations; it depends on the choice of an *origin* $o \in \Omega$ and, once o is fixed, it is given by

$$(A, \mathbf{v}) \cdot x = o + A(\mathbf{u}_{o,x} + \mathbf{v}) \qquad \forall x \in \Omega,\ (A, \mathbf{v}) \in \mathrm{GL}(V) \rtimes V,$$

where $\mathbf{u}_{o,x}$ is the unique vector such that $x = o + \mathbf{u}_{o,x}$. By means of this formula, we can also define an action of $\mathrm{GL}(V) \rtimes V$ on $L(\Omega)$, that is,

$$(A, \mathbf{v}) \cdot (x + D) = (A, \mathbf{v}) \cdot x + AD \qquad \forall x + D \in L(\Omega),\ (A, \mathbf{v}) \in \mathrm{GL}(V) \rtimes V\,.$$

Covariance of a quadrature system is then understood with respect to the latter group action.

*Definition 2. Let $G \subseteq \mathrm{GL}(V) \rtimes V$ be any subgroup. A quadrature system Q for the affine space (Ω, V) acting on the Hilbert space $\mathcal{H}$ is G-*covariant *if there exists a unitary projective representation U of G on $\mathcal{H}$ such that*

$$\mathsf{Q}(g \cdot \mathfrak{l}) = U(g)\mathsf{Q}(\mathfrak{l})U(g)^* \qquad \forall \mathfrak{l} \in L(\Omega),\ g \in G\,. \tag{2}$$

The choice of the unitary operator $U(g)$ in (2) is unique up to multiplication by an arbitrary phase factor depending on g (see Ref. 22, Proposition 3.3); this explains the necessity of dealing with projective representations. We denote by $\mathcal{Q}_G(\Omega)$ the set of all G-covariant quadrature systems for the affine space (Ω, V). If $G \equiv V$ is the group of phase space translations, a V-covariant quadrature system projects on a set of stabilizer MUBs (or states, codes) in the terminology of Refs. 24–26 and 31–33. Quite many different covariant quadrature systems are then known to exist in this case.[18,22] The essential point is that, by enlarging the covariance group G to include elements of $\mathrm{GL}(V)$, it may happen that the set $\mathcal{Q}_G(\Omega)$ becomes empty.

It is known that in characteristic $p \neq 2$ there is a unique maximal subgroup $G_0 \subseteq \mathrm{GL}(V)$ making the set $\mathcal{Q}_{G_0 \rtimes V}(\Omega)$ nonempty, that is, the group $G_0 = \mathrm{SL}(V)$ of unit determinant elements in $\mathrm{GL}(V)$ (see Ref. 18, Appendix B). In characteristic $p = 2$, however, we have $\mathcal{Q}_{\mathrm{SL}(V) \rtimes V}(\Omega) = \emptyset$ by Ref. 22, Theorem 7.5, and the problem of finding all the subgroups $G_0 \subset \mathrm{GL}(V)$ admitting $(G_0 \rtimes V)$ -covariant quadrature systems is open up to now. The objective of the present paper is to solve this question and thus completely determine the set

$$\mathcal{G} = \{G_0 \subset \mathrm{GL}(V) \mid G_0 \text{ is a subgroup and } \mathcal{Q}_{G_0 \rtimes V}(\Omega) \neq \emptyset\} \tag{3}$$

in even characteristic. Note that also in this case any $G_0 \in \mathcal{G}$ must be a subgroup of $\mathrm{SL}(V)$ by Ref. 22, Proposition 7.1. Moreover, the set $\mathcal{G}$ is nontrivial, since by Theorem 8.4 of the same reference, the *nonsplit toruses* of $\mathrm{SL}(V)$ are elements of $\mathcal{G}$. The contribution of the present paper is to show that nonsplit toruses actually do not exhaust the set $\mathcal{G}$, but they are just “one half” of it.

D. V-covariant quadratures and Weyl multipliers

Our approach to the problem of determining the set $\mathcal{G}$ relies on the classification of V-covariant quadrature systems by means of suitably defined associated multipliers, a topic that was extensively exposed in Ref. 22. Here we briefly recall the essential points.

Theorem 1 (Ref. 22, Propositions 4.2 and 4.6). *Suppose Q is a V-covariant quadrature system for the affine space (Ω, V) acting on the Hilbert space $\mathcal{H}$. Let $o \in \Omega$ be any point. Then there exists a unique projective unitary representation W_o of V on $\mathcal{H}$ such that*

(W.1) $W_o(\mathbf{v})\mathsf{Q}(\mathfrak{l})W_o(\mathbf{v})^* = \mathsf{Q}(\mathfrak{l}+\mathbf{v})$ *for all* $\mathfrak{l} \in L(\Omega)$ *and* $\mathbf{v} \in V$*;*

(W.2) $W_o(\boldsymbol{d})\mathsf{Q}(o+D) = \mathsf{Q}(o+D)$ *for all* $D \in \mathcal{D}$ *and* $\mathbf{d} \in D$*.*

The multiplier m of the projective representation W_o *does not depend on the choice of the point o, and it satisfies the following two relations:*

(M.1) for any $D \in \mathcal{D}$*,* $m(\boldsymbol{d}_1,\boldsymbol{d}_2) = 1$ *for all* $\mathbf{d}_1, \mathbf{d}_2 \in D$*;*

(M.2) $\overline{m(\mathbf{u},\mathbf{v})}m(\mathbf{v},\mathbf{u}) = \omega_p^{\operatorname{Tr} S(\mathbf{u},\mathbf{v})}$ *for all* $\mathbf{u},\mathbf{v} \in V$*, where S is a symplectic form*[44] *on V which is uniquely determined.*

We recall that the *multiplier* of W_o is the function $m : V \times V \to \{z \in \mathbb{C} \mid z\bar{z} = 1\}$ such that

$$W_o(\mathbf{u}+\mathbf{v}) = m(\mathbf{u},\mathbf{v})W_o(\mathbf{u})W_o(\mathbf{v}) \qquad \forall \mathbf{u},\mathbf{v} \in V\,.$$

It satisfies the cocycle relation

$$m(\mathbf{u}+\mathbf{v},\mathbf{w})m(\mathbf{u},\mathbf{v}) = m(\mathbf{u},\mathbf{v}+\mathbf{w})m(\mathbf{v},\mathbf{w}) \qquad \forall \mathbf{u},\mathbf{v},\mathbf{w} \in V\,.$$

By items (M.1) and (M.2), the projective representation W_o has the following two additional properties:

(W.3) the restriction $W_o|_D$ is an ordinary (i.e., nonprojective) representation of D for all $D \in \mathcal{D}$;

(W.4) W_o satisfies the commutation relation

$$W_o(\mathbf{u})W_o(\mathbf{v}) = \omega_p^{\operatorname{Tr} S(\mathbf{u},\mathbf{v})} W_o(\mathbf{v})W_o(\mathbf{u}) \qquad \forall \mathbf{u},\mathbf{v} \in V\,.$$

A projective unitary representation of V with properties (W.3) and (W.4) is called a *Weyl system* for the symplectic space (V,S). The Weyl system W_o satisfying the additional conditions (W.1) and (W.2) is then said to be *associated* with the V-covariant quadratures Q and *centered* at o. Accordingly, any multiplier m of the additive Abelian group V which satisfies items (M.1) and (M.2) of Theorem 1 is called a *Weyl multiplier* for the symplectic space (V,S). Theorem 1 then asserts that, through any associated centered Weyl system, an element $\mathsf{Q} \in \mathcal{Q}_V(\Omega)$ defines a symplectic form S on V and a Weyl multiplier m for (V,S) in an unambiguous way. We call such S and m the symplectic form and Weyl multiplier *associated* with Q. It is easy to check that if $\mathsf{Q}_1, \mathsf{Q}_2 \in \mathcal{Q}_V(\Omega)$ are equivalent in the sense of (1), then the symplectic forms and Weyl multipliers associated with Q_1 and Q_2 are the same. Remarkably, the converse of this fact also holds.

Theorem 2 (Ref. 22, Theorem 6.3). *Let S be a symplectic form on V, and m a Weyl multiplier for (V, S). Then there exists a unique equivalence class* $\mathcal{Q}_V(\Omega,S,m)$ *of V-covariant quadrature systems for* (Ω, V) *having S and m as the associated form and multiplier.*

For any symplectic form S on V, Weyl multipliers m for (V,S) exist by Ref. 22, Proposition 6.1 (see also (6) and Section V below for some explicit constructions of m). Hence the set $\mathcal{Q}_V(\Omega) \supset \mathcal{Q}_V(\Omega,S,m)$ is always nonempty. But what really matters in the equivalence class of a V-covariant quadrature system is its Weyl multiplier and not its associated symplectic form. In fact, it is easy to see that for the same symplectic space (V,S), there exist quite many different Weyl multipliers. In other words, if we write $\mathcal{Q}_V(\Omega,S)$ for the totality of V-covariant quadrature systems having S as the associated symplectic form, in the chain of inclusions $\mathcal{Q}_V(\Omega) \supset \mathcal{Q}_V(\Omega,S) \supset \mathcal{Q}_V(\Omega,S,m)$, only the latter set is made of a single equivalence class of quadratures.

Remark 1. According to our definition, two quadrature systems Q_1 *and* Q_2 *are equivalent if they are unitarily conjugate as functions* $\mathsf{Q}_i : L(\Omega) \to \mathcal{L}(\mathcal{H})$ *(see (1)). This condition is much stronger than only requiring the two sets of rank-1 projections* $\operatorname{ran} \mathsf{Q}_i = \{\mathsf{Q}_i(\mathfrak{l}) \mid \mathfrak{l} \in L(\Omega)\}$ $(i = 1,2)$ *to be unitarily conjugate. Actually, if* $\mathsf{Q}_1, \mathsf{Q}_2 \in \mathcal{Q}_V(\Omega)$*, then* $\operatorname{ran} \mathsf{Q}_1$ *and* $\operatorname{ran} \mathsf{Q}_2$ *are always unitarily conjugate as unordered sets, regardless of the associated symplectic forms and Weyl multipliers (see Ref. 22, Theorem 7.9).*

E. The explicit form of *V*-covariant quadratures

We assume that the quadrature system $\mathsf{Q} \in \mathcal{Q}_V(\Omega, S, m)$ is given and acts on the Hilbert space $\mathcal{H}$. In order to write down Q explicitly, we need to choose

— an origin $o \in \Omega$;
— a *symplectic basis* of (V,S), i.e., an $\mathbb{F}$-linear basis $\{\mathbf{e}_1, \mathbf{e}_2\}$ of V such that $S(\mathbf{e}_1, \mathbf{e}_2) = 1$;
— a unit vector $\phi_0 \in \mathcal{H}$ in the range of $\mathsf{Q}(o + \mathbb{F}\mathbf{e}_2)$, where $\mathbb{F}\mathbf{e}_2 = \{\alpha\mathbf{e}_2 \mid \alpha \in \mathbb{F}\}$ is the direction in V along $\mathbf{e}_2$.

After this preparation, if W_o is the Weyl system associated with Q and centered at o, we set

$$\phi_\gamma = W_o(\gamma\mathbf{e}_1)\phi_0 \qquad \forall\gamma \in \mathbb{F}\,.$$

We then have $\phi_\gamma \in \operatorname{ran}[W_o(\gamma\mathbf{e}_1)\mathsf{Q}(o + \mathbb{F}\mathbf{e}_2)] = \operatorname{ran}[\mathsf{Q}(o + \gamma\mathbf{e}_1 + \mathbb{F}\mathbf{e}_2)]$ by covariance of Q. Since $L_{\mathbb{F}\mathbf{e}_2}(\Omega) = \{o + \gamma\mathbf{e}_1 + \mathbb{F}\mathbf{e}_2 \mid \gamma \in \mathbb{F}\}$, by properties (i) and (ii) of a quadrature system, the vectors $\{\phi_\gamma | \gamma \in \mathbb{F}\}$ form an orthonormal basis of $\mathcal{H}$. In this basis, the Weyl system W_o is given by

$$W_o(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2)\phi_\gamma = m(\alpha_1\mathbf{e}_1, \alpha_2\mathbf{e}_2)\omega_p^{-\mathrm{Tr}\,\alpha_2\gamma}\phi_{\gamma+\alpha_1} \qquad \forall\alpha_1, \alpha_2 \in \mathbb{F}\,. \tag{4}$$

Indeed,

$$\begin{aligned} W_o(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2)\phi_\gamma &= m(\alpha_1\mathbf{e}_1, \alpha_2\mathbf{e}_2)W_o(\alpha_1\mathbf{e}_1)W_o(\alpha_2\mathbf{e}_2)W_o(\gamma\mathbf{e}_1)\phi_0 \\ &= m(\alpha_1\mathbf{e}_1, \alpha_2\mathbf{e}_2)\omega_p^{\mathrm{Tr}\,S(\alpha_2\mathbf{e}_2,\gamma\mathbf{e}_1)}W_o(\alpha_1\mathbf{e}_1)W_o(\gamma\mathbf{e}_1)W_o(\alpha_2\mathbf{e}_2)\phi_0 \\ &= m(\alpha_1\mathbf{e}_1, \alpha_2\mathbf{e}_2)\omega_p^{-\mathrm{Tr}\,\alpha_2\gamma}\phi_{\gamma+\alpha_1} \end{aligned}$$

since $W_o(\alpha_2\mathbf{e}_2)\phi_0 = \phi_0$ because W_o is centered at o (see item (W.2) of Theorem 1). By Ref. 22, Proposition 5.2, for all $\mathbf{u}, \mathbf{v} \in V$ with $\mathbf{u} \neq \mathbf{0}$,

$$\mathsf{Q}(o + \mathbf{v} + \mathbb{F}\mathbf{u}) = \frac{1}{|\mathbb{F}|}\sum_{\lambda\in\mathbb{F}}\omega_p^{\mathrm{Tr}\,S(\mathbf{v},\lambda\mathbf{u})}W_o(\lambda\mathbf{u}),$$

where $\mathbb{F}\mathbf{u}$ is the direction along $\mathbf{u}$, and hence,

$$\begin{gathered} \mathsf{Q}(o + \mathbf{v} + \mathbb{F}\mathbf{u})\phi_\gamma = \frac{1}{|\mathbb{F}|}\sum_{\lambda\in\mathbb{F}} m(\lambda\alpha_1\mathbf{e}_1, \lambda\alpha_2\mathbf{e}_2)\,\omega_p^{\mathrm{Tr}\,\lambda[\alpha_2(\beta_1-\gamma)-\alpha_1\beta_2]}\phi_{\gamma+\lambda\alpha_1} \\ \text{with} \qquad \mathbf{u} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2, \qquad \mathbf{v} = \beta_1\mathbf{e}_1 + \beta_2\mathbf{e}_2\,. \end{gathered} \tag{5}$$

In the converse direction, if m is any given Weyl multiplier for the symplectic space (V, S), one can pick a $|\mathbb{F}|$-dimensional Hilbert space $\mathcal{H}$, fix an orthonormal basis $\{\phi_\gamma \mid \gamma \in \mathbb{F}\}$ of $\mathcal{H}$, and define the maps W_o and Q as in (4) and (5). As W_o and Q are unitarily equivalent to the maps defined in the previous paragraph, we have $\mathsf{Q} \in \mathcal{Q}_V(\Omega, S, m)$ and W_o is its associated Weyl system centered at o.

F. More symmetries besides translations

We already noticed that $G_0 \subseteq \mathrm{SL}(V)$ is a necessary condition for the set $\mathcal{Q}_{G_0\rtimes V}(\Omega)$ to be nonempty; indeed, this follows since G_0 must preserve the symplectic form associated with any quadrature $\mathsf{Q} \in \mathcal{Q}_{G_0\rtimes V}(\Omega) \subseteq \mathcal{Q}_V(\Omega)$ (see Ref. 22, Proposition 7.1). In order to find a sufficient condition, we need the notion of G_0-*invariance* for a Weyl multiplier m, that is,

$$m(A\mathbf{u}, A\mathbf{v}) = m(\mathbf{u}, \mathbf{v}) \qquad \forall\mathbf{u}, \mathbf{v} \in V,\ A \in G_0\,.$$

The existence of G_0-invariant Weyl multipliers is equivalent to the set $\mathcal{Q}_{G_0\rtimes V}(\Omega)$ being nonempty. Indeed, we have the following fact.

Proposition 1 (*Ref. 22, Proposition 7.2*). *Let $G_0 \subseteq \mathrm{SL}(V)$ be any subgroup. A quadrature system $\mathsf{Q} \in \mathcal{Q}_V(\Omega)$ is $(G_0 \rtimes V)$ -covariant if and only if its associated Weyl multiplier is G_0-invariant.*

As a consequence, the set $\mathcal{G}$ of (3) coincides with

$$\mathcal{G} = \{G_0 \subseteq \mathrm{SL}(V) \mid \text{there exist } G_0\text{-invariant Weyl multipliers}\}\,.$$

In odd characteristic, the multiplier

$$m(\mathbf{u},\mathbf{v}) = \omega_p^{\mathrm{Tr}\, S(2^{-1}\mathbf{v},\mathbf{u})} \tag{6}$$

is a Weyl multiplier for the symplectic space (V,S) which is invariant with respect to the whole group $\mathrm{SL}(V)$ (see Ref. 22, Proposition 7.4); therefore, $\mathcal{G}$ is actually the set of all the subgroups of $\mathrm{SL}(V)$. However, in even characteristic such an m cannot be defined, and we need to look for subgroups $G_0 \subset \mathrm{SL}(V)$ admitting G_0-invariant Weyl multipliers case by case. This is done in Section III, and the detailed description of the set $\mathcal{G}$ in characteristic $p = 2$ is provided in Section IV (see Theorem 4).

III. ALL COVARIANT QUADRATURE SYSTEMS IN CHARACTERISTIC 2

From now on, we focus on characteristic $p = 2$. The following is then the key step towards our characterization of the set $\mathcal{G}$ in this case.

Lemma 1. Suppose $\mathbb{F}$ has characteristic $p = 2$. Then $\mathcal{Q}_{G_0 \rtimes V}(\Omega) = \emptyset$ for all subgroups $G_0 \subseteq SL(V)$ such that $|G_0|$ is even.

Before proving the lemma, observe that in characteristic $p = 2$ we have $+1 = -1$ in $\mathbb{F}$, and $\omega_2 = -1$ is the unique possible choice of a 2-root of unity in $\mathbb{C}$. Moreover, the square map $\alpha \mapsto \alpha^2$ is an automorphism of $\mathbb{F}$ over $\mathbb{Z}_2$. Its inverse is the map $\alpha \mapsto \alpha^{1/2} = \alpha^{|\mathbb{F}|/2}$.

Proof of Lemma 1. By Proposition 1, it is enough to show that, if G_0 has even order, there do not exist G_0-invariant Weyl multipliers. So, let us assume by contradiction that $|G_0|$ is even and m is a G_0-invariant Weyl multiplier. By Cauchy theorem (see Ref. 39, p. 97), there exists an order 2 element in G_0, that is, a symplectic map $A \in G_0$ such that $A \neq I$ and $A^2 = I$. Let $\mathbf{e}_2 \in V$ be such that $A\mathbf{e}_2 \neq \mathbf{e}_2$. Then $\mathbf{e}_1 = A\mathbf{e}_2 + \mathbf{e}_2 \neq 0$ because $+1 = 1$; moreover, $A\mathbf{e}_1 = \mathbf{e}_1$. Hence the vectors $\{\mathbf{e}_1, \mathbf{e}_2\}$ are linearly independent and thus form an $\mathbb{F}$-linear basis of V. In particular, $S(\mathbf{e}_1,\mathbf{e}_2) = \alpha \neq 0$ since $S \neq 0$. Possibly rescaling $\mathbf{e}_2$ by α^{-1}, we can assume that $\{\mathbf{e}_1, \mathbf{e}_2\}$ is a symplectic basis of (V,S). The two conditions $\det A = 1$ and $A\mathbf{e}_1 = \mathbf{e}_1$ imply that A is upper triangular with diagonal entries (1,1) in the basis $\{\mathbf{e}_1, \mathbf{e}_2\}$; that is, $A\mathbf{e}_2 = \beta\mathbf{e}_1 + \mathbf{e}_2$ for some $\beta \neq 0$.

Now, choose $\gamma \in \mathbb{F}$ such that $\mathrm{Tr}\,\gamma = 1$ (this is always possible by Ref. 38, Theorem VI.5.2). Let

$$\mathbf{f}_1 = (\beta\gamma)^{1/2}\,\mathbf{e}_1, \qquad \mathbf{f}_2 = (\beta^{-1}\gamma)^{1/2}\,\mathbf{e}_2 \,.$$

Then

$$A\mathbf{f}_1 = \mathbf{f}_1, \qquad A\mathbf{f}_2 = \mathbf{f}_1 + \mathbf{f}_2 \tag{7}$$

and

$$\mathrm{Tr}\, S(\mathbf{f}_1,\mathbf{f}_2) = 1 \,. \tag{8}$$

We have

$$\begin{aligned}
1 &= m(\mathbf{f}_1+\mathbf{f}_2, \mathbf{f}_1+\mathbf{f}_2) && \text{(property (M.1))}\\
&= m(\mathbf{f}_1+\mathbf{f}_2, \mathbf{f}_1+\mathbf{f}_2) m(\mathbf{f}_1,\mathbf{f}_2)\overline{m(\mathbf{f}_1,\mathbf{f}_2)}\\
&= m(\mathbf{f}_1+\mathbf{f}_2+\mathbf{f}_1, \mathbf{f}_2) m(\mathbf{f}_1+\mathbf{f}_2,\mathbf{f}_1)\overline{m(\mathbf{f}_1,\mathbf{f}_2)} && \text{(multiplier property)}\\
&= m(\mathbf{f}_2,\mathbf{f}_2) m(A\mathbf{f}_2, A\mathbf{f}_1)\overline{m(\mathbf{f}_1,\mathbf{f}_2)} && \text{(by (7))}\\
&= m(\mathbf{f}_2,\mathbf{f}_1)\overline{m(\mathbf{f}_1,\mathbf{f}_2)} && \text{(property (M.1) and } G_0\text{-invariance)}\\
&= (-1)^{\mathrm{Tr}\, S(\mathbf{f}_1,\mathbf{f}_2)} && \text{(property (M.2))}\\
&= -1 && \text{(by (8))}
\end{aligned}$$

which is the desired contradiction. □

The next step is to list all the possible subgroups of $\mathrm{SL}(V)$. By the previous result, for $p = 2$ all the subgroups having even order can be dropped from $\mathcal{G}$. The classification of the subgroups of the finite projective unimodular group $\mathrm{PSL}(V) = \mathrm{SL}(V)/\{I,-I\}$ goes back to the papers of Moore and Wiman,[35,36] which cover both the even and odd characteristic cases (see Ref. 37, pp. 285-286, for a summary of the subgroups found by Moore and Wiman). Note that $\mathrm{PSL}(V) = \mathrm{SL}(V)$ for $p = 2$, hence in our case Refs. 35–37 actually enumerate all the subgroups of SL(V). For the present purposes, we use here the more modern version of the classification of Moore and Wiman given in Suzuki's book.[39]

Theorem 3. *In characteristic $p = 2$, any subgroup of SL(V) is isomorphic to one of the following groups.*

(a) The dihedral groups of order $2(|\mathbb{F}| \pm 1)$ *and their subgroups.*
(b) A group H of order $|\mathbb{F}|(|\mathbb{F}| - 1)$ *and its subgroups. A Sylow 2-subgroup Q of H is isomorphic to $\mathbb{Z}_2^k$, Q is normal in H, and the factor group H/Q is a cyclic group of order* $|\mathbb{F}| - 1$.
(c) The alternating groups A_4 or A_5.
(d) SL(V'), where V' is a 2-dimensional vector space over a subfield $\mathbb{F}' \subseteq \mathbb{F}$.

Proof. This is an immediate application of Ref. 39, Theorem III.(6.25) and III.(6.26), when $q = |\mathbb{F}|$ is even, since PSL(V) = SL(V) in this case. In particular, each item follows from the corresponding one in Suzuki's Theorem III.(6.25) by observing that

(a,b) the greatest common divisor of 2 and $|\mathbb{F}| - 1$ is $d = 1$, and using Ref. 39, I.(9.14), for the characterization of the elementary Abelian 2-groups defined in II.(5.22) therein;
(c) SL(V) has no subgroups isomorphic to the symmetric group Σ_4 by Ref. 39, item (iii) of Theorem III.(6.26);
(d) if $\mathbb{F}'$ is any field such that $|\mathbb{F}'|^m = |\mathbb{F}|$, then $\mathrm{PGL}(2,\mathbb{F}') = \mathrm{PSL}(2,\mathbb{F}') = \mathrm{SL}(2,\mathbb{F}')$ since $\mathbb{F}'$ is a subfield of $\mathbb{F}$ and hence also has even characteristic.

□

Combining Lemma 1 and Theorem 3 we obtain the following conclusion.

Proposition 2. Let $p = 2$, and suppose S is any symplectic form on V. Then the set $\mathcal{Q}_{G_0\rtimes V}(\Omega, S) = \mathcal{Q}_{G_0\rtimes V}(\Omega) \cap \mathcal{Q}_V(\Omega, S)$ is not empty if and only if G_0 is a cyclic group with $|G_0|$ odd.

Proof. The proof of sufficiency is a straightforward adaptation of the proof of Ref. 22, Proposition 8.3. Indeed, suppose G_0 is a cyclic group with odd order. If m_0 is any Weyl multiplier for the symplectic space (V, S), let $m(\mathbf{u},\mathbf{v}) = \prod_{A\in G_0} m_0(A\mathbf{u}, A\mathbf{v})$. Then m is a multiplier of V, which clearly satisfies $m|_{D\times D} = 1$ for all $D \in \mathcal{D}$, since all its factors do it. Since $\overline{m_0(A\mathbf{u}, A\mathbf{v})}m_0(A\mathbf{v}, A\mathbf{u}) = (-1)^{\mathrm{Tr}\, S(A\mathbf{u},A\mathbf{v})} = (-1)^{\mathrm{Tr}\, S(\mathbf{u},\mathbf{v})}$ for every $A \in G_0$, we have

$$\overline{m(\mathbf{u}, \mathbf{v})}m(\mathbf{v}, \mathbf{u}) = (-1)^{|G_0|\mathrm{Tr}\, S(\mathbf{u},\mathbf{v})} = (-1)^{\mathrm{Tr}\, S(\mathbf{u},\mathbf{v})}$$

because $|G_0|$ is odd. Therefore, m satisfies items (M.1) and (M.2) of Theorem 1, that is, it is a Weyl multiplier for (V,S). For all $B \in G_0$,

$$m(B\mathbf{u}, B\mathbf{v}) = \prod_{A\in G_0} m_0(AB\mathbf{u}, AB\mathbf{v}) = \prod_{A\in G_0} m_0(A\mathbf{u}, A\mathbf{v}) = m(\mathbf{u}, \mathbf{v})$$

which shows that m is G_0-invariant. Hence $\mathcal{Q}_{G_0\rtimes V}(\Omega, S) \supset \mathcal{Q}_V(\Omega, S, m) \neq \emptyset$ by Theorem 2 and Proposition 1.

Conversely, if $\mathcal{Q}_{G_0\rtimes V}(\Omega, S) \neq \emptyset$, then $|G_0|$ is odd by Lemma 1. So, we need to check which ones of the groups listed in Theorem 3 have odd order. Since $|A_4| = 12$ and $|A_5| = 60$, the possibilities in item (c) of Theorem 3 are excluded. Moreover, by Ref. 39, p. 81, we have $|\mathrm{SL}(V')| = |\mathbb{F}'|(|\mathbb{F}'|^2 - 1)$, which is even when V' is a vector space over a subfield $\mathbb{F}' \subseteq \mathbb{F}$; hence G_0 cannot be as in item (d) of Theorem 3. Thus, items (a) and (b) are the only remaining possibilities.

The dihedral group D_{2n} is the semidirect product $\mathbb{Z}_2 \rtimes \mathbb{Z}_n$, where the nontrivial element $1 \in \mathbb{Z}_2$ acts on the normal factor $\mathbb{Z}_n$ as

$$(1, 0)(0, x)(1, 0)^{-1} = (0, -x) \qquad \forall x \in \mathbb{Z}_n .$$

If G_0 is a subgroup of $D_{2(|\mathbb{F}|\pm1)}$ and $(z, x) \in G_0$, then $z = 0$, as otherwise $(1, x)^2 = (0, -x + x) = (0, 0)$ implying that $|G_0|$ is even. It follows that $G_0 \subseteq \mathbb{Z}_{|\mathbb{F}|\pm1}$, hence G_0 is a cyclic group.

Finally, suppose $G_0 \subseteq H$, where H is as in item (b) of Theorem 3. Then the subgroup $Q_0 = Q \cap G_0$ is normal in G_0, and the quotient group G_0/Q_0 is naturally identified with a subgroup of H/Q. Since Q is a Sylow 2-subgroup of H, either Q_0 is trivial or its order is even; hence Q_0 is trivial because $|G_0|$ is odd. Since H/Q is cyclic of order $|\mathbb{F}| - 1$, also its subgroup $G_0/Q_0 = G_0$ is cyclic.

In conclusion, $|G_0|$ being odd implies that G_0 is cyclic, and this concludes the proof. □

IV. CYCLIC SUBGROUPS OF SL(V)

By Proposition 2,

$$\mathcal{G} = \{G_0 \subset \mathrm{SL}(V) \mid G_0 \text{ is cyclic and with odd order}\} \quad \text{in characteristic } p = 2\,.$$

We will shortly see that the cyclic subgroups $G_0 \subset \mathrm{SL}(V)$ divide into three types, each type being determined by the eigenvalues of any of its generators. Recall that the eigenvalues of an arbitrary symplectic map $A \in \mathrm{SL}(V)$ are the roots of its characteristic polynomial

$$p_A(X) = \det(A - XI) = X^2 - \mathrm{tr}(A)X + 1 \tag{9}$$

and thus they are two possibly coinciding elements ξ_1 and ξ_2 of the quadratic extension $\tilde{\mathbb{F}}$ of $\mathbb{F}$. Since p_A has coefficients in $\mathbb{F}$, either $\xi_1, \xi_2 \in \mathbb{F}$ or $\xi_1, \xi_2 \in \tilde{\mathbb{F}} \setminus \mathbb{F}$, and in the latter case $\xi_2 = \overline{\xi_1}$, where $\overline{\xi_1} = \xi_1^{|\mathbb{F}|}$ is the conjugate of ξ_1. Both of the eigenvalues are nonzero, and they satisfy the relations $\xi_1 + \xi_2 = \mathrm{tr}\,(A)$ and $\xi_1\xi_2 = 1$. In particular, in even characteristic the equality $\xi_1 = \xi_2$ holds if and only if $\xi_1 = \xi_2 = 1$, and in this case $\mathrm{tr}\,(A) = 0$.

Again, for the remaining of the section we restrict ourselves to even characteristic. The following terminology then summarizes all the possibilities for an element $A \in \mathrm{SL}(V)$ (see, e.g., Ref. 40, p. 95).

Definition 3. In characteristic $p = 2$, an element $A \in \mathrm{SL}(V)$ is said to be

- split, *if $A = I$ or A has two different eigenvalues $\xi, \xi^{-1} \in \mathbb{F}$;*
- nonsplit, *if A has two different eigenvalues $\xi, \xi^{-1} \in \tilde{\mathbb{F}} \setminus \mathbb{F}$, with $\xi^{-1} = \overline{\xi}$;*
- unipotent, *if $A \neq I$ and 1 is the sole eigenvalue of A.*

A is semisimple *if it is either split or nonsplit.*

Let us fix a basis of V over $\mathbb{F}$ and write any element $A \in \mathrm{SL}(V)$ as a unit determinant 2×2 matrix with entries in $\mathbb{F}$ with respect to such a basis. If $A \in \mathrm{SL}(V)$ is semisimple and $\xi, \xi^{-1} \in \tilde{\mathbb{F}}$ are its two eigenvalues, then

$$A = U \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} U^{-1} \qquad \text{for some } 2 \times 2 \text{ matrix } U \text{ with entries in } \tilde{\mathbb{F}}\,.$$

All the entries of U can be chosen in $\mathbb{F}$ if and only if A is split. In any case, $A^k = I$ if and only if $\xi^k = \xi^{-k} = 1$, that is, the order k_0 of A and ξ coincide. Hence, we have the following:

- if A is split, then k_0 divides the order of the cyclic multiplicative group $\mathbb{F}_*$ of the nonzero elements of $\mathbb{F}$, which is $|\mathbb{F}_*| = |\mathbb{F}| - 1$;
- if A is nonsplit, then k_0 divides the order of the cyclic group $M = \{\xi \in \tilde{\mathbb{F}}_* \mid \xi\overline{\xi} = 1\}$, which is $|\mathbb{F}| + 1$ (see Ref. 22, Section 8, for a simple proof).

Finally, for $0 < k < k_0$, the eigenvalues of A^k are ξ^k and ξ^{-k}. Therefore, if A is semisimple, then also A^k is semisimple for all $0 < k < k_0$.

On the other hand, if A is unipotent, there is a nonzero $\mathbf{e}_1 \in V$ such that $A\mathbf{e}_1 = \mathbf{e}_1$. To find the order of A, pick a vector $\mathbf{e}_2 \in V$ linearly independent of $\mathbf{e}_1$. Then $A\mathbf{e}_2 = \alpha\mathbf{e}_2 + \beta\mathbf{e}_1$, with $\alpha = 1$ by the unit determinant condition, and $\beta \neq 0$ because $A \neq I$. Moreover, we have $A^2\mathbf{e}_1 = \mathbf{e}_1$ and $A^2\mathbf{e}_2 = \mathbf{e}_2 + 2\beta\mathbf{e}_1 = \mathbf{e}_2$, hence $A^2 = I$. In particular, the order of A is 2.

This discussion shows that the next definition is consistent and exhausts all the cyclic subgroups of SL(V).

Definition 4. A cyclic subgroup of SL(V) *is a* torus *[respectively, a* split torus, nonsplit torus, unipotent subgroup*] if it is generated by a semisimple [respectively, split, nonsplit, unipotent] element of* SL(V).

Definitions 3 and 4 can be easily extended to odd p. It is then a general fact, valid in all characteristics, that there exists a maximal split [respectively, nonsplit] torus $T \subset \mathrm{SL}(V)$, and all split [respectively, nonsplit] toruses of SL(V) are conjugate to subgroups of T. Moreover, all the unipotent subgroups of SL(V) are conjugate in even characteristic, and they are divided into four conjugacy classes when $p \neq 2$. Indeed, this follows from Ref. 35, Section 6 (see also Ref. 37, pp. 262–268, and 39, III.(6.23)). Here we report the following elementary proof in characteristic $p = 2$.

Proposition 3. Suppose $p = 2$.

(a) There exists a split [respectively, nonsplit] torus $T \subset \mathrm{SL}(V)$ such that $|T| = |\mathbb{F}| - 1$ [respectively, $|T| = |\mathbb{F}| + 1$]. Any split [respectively, nonsplit] torus has odd order and is conjugated to a subgroup of T. In particular, all toruses of the same order are conjugated.

(b) There exists a unique conjugacy class of unipotent subgroups in SL(V)*. All unipotent subgroups have order* 2.

Proof. We preliminarily prove that if $\xi \in \tilde{\mathbb{F}}$ is such that $\xi + \xi^{-1} \in \mathbb{F}$, then the conjugacy class of the symplectic map

$$A_\xi = \begin{pmatrix} \xi + \xi^{-1} & 1 \\ 1 & 0 \end{pmatrix} \tag{10}$$

is the set

$$C(A_\xi) = \{A \in \mathrm{SL}(V) \setminus \{I\} \mid \xi \text{ and } \xi^{-1} \text{ are the eigenvalues of } A\}\,.$$

Indeed, by (9) the latter set is $C(A_\xi) = \{A \in \mathrm{SL}(V) \setminus \{I\} \mid \mathrm{tr}\,(A) = \xi + \xi^{-1}\}$. Therefore, $A_\xi \in C(A_\xi)$, and it suffices to show that any $A \in \mathrm{SL}(V) \setminus \{I\}$ is such that

$$A = U \begin{pmatrix} \mathrm{tr}\,(A) & 1 \\ 1 & 0 \end{pmatrix} U^{-1} \qquad \text{for some } U \in \mathrm{SL}(V)\,.$$

Writing A in matrix form

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \text{with} \qquad \alpha, \beta, \gamma, \delta \in \mathbb{F},\ \alpha\delta + \beta\gamma = 1,$$

it can be directly verified that a possible choice of U is

$$U = \begin{cases} \begin{pmatrix} 0 & \beta^{1/2} \\ \beta^{-1/2} & \alpha\beta^{-1/2} \end{pmatrix} & \text{if } \beta \neq 0 \\ \begin{pmatrix} \gamma^{-1/2} & \delta\gamma^{-1/2} \\ 0 & \gamma^{1/2} \end{pmatrix} & \text{if } \gamma \neq 0 \\ (1+\alpha)^{-1} \begin{pmatrix} \alpha & 1 \\ 1 & \alpha \end{pmatrix} & \text{if } \beta = \gamma = 0 \text{ and } \delta = \alpha^{-1} \end{cases},$$

thus proving the claim.

In order to prove (a), observe first of all that $\mathbb{F}_* = \{1\}$ if and only if $\mathbb{F} = \mathbb{Z}_2$, and the claims for split toruses are trivial in this case since $T = \{I\}$ is the unique split torus of SL(V). Next, suppose $\xi \neq 1$ is a generator of the cyclic group $\mathbb{F}_*$ [respectively, $M = \{\xi \in \tilde{\mathbb{F}}_* \mid \xi\overline{\xi} = 1\}$] and define A_ξ as in (10). Then A_ξ is a split [respectively, nonsplit] element of the same order as ξ, that is, A_ξ generates a split [respectively, nonsplit] torus T of order $|T| = |\mathbb{F}_*| = |\mathbb{F}| - 1$ [respectively, $|T| = |M| = |\mathbb{F}| + 1$]. If T' is any split [respectively, nonsplit] torus generated by a split [respectively, nonsplit] element $A' \in \mathrm{SL}(V)$, either $A' = I$ or A' has two different eigenvalues ξ' and ξ'^{-1} with $\xi' \in \mathbb{F}_*$ [respectively, $\xi' \in M$]. It follows that $\xi' = \xi^k$ for some k, hence $A' \in C(A_\xi^k)$ by the previous claim. Therefore, T' is conjugated to the cyclic subgroup of T generated by A_ξ^k. Since T has a unique cyclic subgroup of each order dividing $|T|$ (see Ref. 38, Proposition I.4.2 and I.4.3(iv)), all split [respectively, nonsplit] toruses of the same order are conjugated among them and with a unique subgroup of T. Finally, $|\mathbb{F}| - 1 = 2^r - 1$ and $|\mathbb{F}| + 1 = 2^r + 1$ are relatively prime; hence two toruses T_1 and T_2 such that $|T_1| = |T_2|$ are either both split or both nonsplit, and so they are conjugated.

The proof of (b) follows since by definition any unipotent element $B \in \mathrm{SL}(V)$ is such that $B \neq I$ and $\xi = \xi^{-1} = 1$ are the two eigenvalues of B; all unipotent B's are then conjugated to

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

by the claim at the beginning of the proof. Since $A_1^2 = I$, the same holds for B. □

Remark 2. The proof of Proposition 3 also yields an explicit expression for a symplectic map A generating a maximal cyclic subgroup of $\mathrm{SL}(V)$*. Indeed, such a map is given by* (10) *with ξ a generator of either $\mathbb{F}_*$ or M in the case of a maximal torus, or $\xi + \xi^{-1} = 0$ for unipotent subgroups.*

We are now in position to state and prove the main result of the paper.

Theorem 4. *In characteristic $p = 2$ and for any symplectic form S, the set $\mathcal{Q}_{G_0 \rtimes V}(\Omega, S)$ is nonempty if and only if G_0 is a torus. The maximal subgroups $G_0 \subset SL(V)$ admitting $(G_0 \rtimes V)$ -covariant quadrature systems are either maximal split or maximal nonsplit toruses.*

Proof. The theorem immediately follows by combining Propositions 2 and 3. □

Remark 3. If T_1 [respectively, T_2] is a maximal split [respectively, maximal nonsplit] torus and $\mathsf{Q}_i \in \mathcal{Q}_{T_i \rtimes V}(\Omega, S)$, then the unitary operators $U_i(g)$ such that

$$\mathsf{Q}_i(g \cdot \mathfrak{l}) = U_i(g)\mathsf{Q}_i(\mathfrak{l})U_i(g)^* \qquad \forall \mathfrak{l} \in L(\Omega),\ g \in T_i$$

permute the corresponding unlabeled projections $\mathrm{ran}\,\mathsf{Q}_i = \{\mathsf{Q}_i(\mathfrak{l}) \mid \mathfrak{l} \in L(\Omega)\}$ *($i = 1, 2$). By Remark 1,* $\mathrm{ran}\,\mathsf{Q}_1$ *and* $\mathrm{ran}\,\mathsf{Q}_2$ *are unitarily conjugate; representing them on a common Hilbert space, this amounts to saying that we can always assume* $\mathrm{ran}\,\mathsf{Q}_1 = \mathrm{ran}\,\mathsf{Q}_2 \equiv \mathcal{R}$ *(although of course $\mathsf{Q}_1 \neq \mathsf{Q}_2$). In this way, both the projective unitary groups* $\mathrm{ran}\,U_i = \{U_i(g) \mid g \in T_i\}$ *permute the same set of rank-1 projections $\mathcal{R}$. However, Theorem 4 says that one can not relabel the elements of $\mathcal{R}$ in order to make all the unitaries* $\mathrm{ran}\,U_1 \cup \mathrm{ran}\,U_2$ *act as phase-space transformations. Equivalently, if we want to regard one of the two unitary groups as a torus in* $\mathrm{SL}(V)$*, with its natural action on the phase-space lines $L(\Omega) \simeq \mathcal{R}$, we cannot do the same with the other group.*

V. MAXIMALLY INVARIANT WEYL MULTIPLIERS

Up to now, we have considered the existence problem for $(G_0 \rtimes V)$ -covariant quadrature systems. However, when the set $\mathcal{Q}_{G_0 \rtimes V}(\Omega, S)$ is nonempty, we have neither investigated whether it is made up of a unique equivalence class of quadratures, nor have we explicitly written down any of its elements.

In this section, we fill this gap in the case where $G_0 \equiv T$ is a maximal torus in even characteristic, providing many examples of inequivalent elements in $\mathcal{Q}_{T \rtimes V}(\Omega, S)$. Moreover, for all these examples we exhibit a unitary projective representation U of $G = T \rtimes V$ yielding the covariance relation (2).

By Theorem 2 and Proposition 1, the equivalence classes of quadratures in the set $\mathcal{Q}_{T \rtimes V}(\Omega, S)$ are in one-to-one correspondence with the T-invariant Weyl multipliers for the symplectic space (V,S). If such a multiplier m is given, Section II E provides the construction of the corresponding quadrature system in terms of m (see (5)). The main difficulty is then to write down an explicit expression for a T-invariant Weyl multiplier.

Note that an explicit formula for the multiplier m also allows one to construct the projective representation U of T yielding the T-covariance of Q. This follows from the next theorem.

Theorem 5 (Ref. 22, Theorem 8.5). *In any characteristic, let T be a maximal torus, and suppose $\mathsf{Q} \in \mathcal{Q}_{T \rtimes V}(\Omega)$. Let W_o be the Weyl system associated with Q and centered at the point $o \in \Omega$*

such that $GL(V)\cdot o = \{o\}$, and let m be its Weyl multiplier. Then a possible choice for the projective representation U of T appearing in (2) is

$$U(A) = \frac{1}{|\mathbb{F}|}\sum_{\mathbf{u}\in V} m(\mathbf{u},(A-I)^{-1}\mathbf{u})W_o(\mathbf{u}) \qquad \forall A\in T\setminus\{I\}\,. \tag{11}$$

Proof. If T is nonsplit, this is Theorem 8.5 of Ref. 22. The proof of the latter result uses only the two facts that $A-I$ is invertible on V, and $-I\in T$. These facts are still true if T is split, hence the same proof works without any change also in the split case. □

The operators $W_o(\mathbf{u})$ appearing in Theorem 5 are explicitly given in formula (4), which again only depends on the Weyl multiplier m associated with Q.

For the remaining part of the section, we then turn to the problem of characterizing the T-invariant Weyl multipliers in characteristic $p = 2$. We remark that the present discussion is a refinement of Ref. 22, Appendix B, which outlines how to find a T-invariant Weyl multiplier by averaging a noninvariant one over T, but does not contain a compact formula for the result.

First of all, observe that, although in odd characteristic there is the natural choice of the Weyl multiplier (6), which takes its values in the set of the p-roots of unity and is actually invariant with respect to the whole group SL(V), when $p = 2$, a more elaborate construction is required. The key difference is that in the latter case there is no ±1-valued Weyl multiplier at all. Indeed, if m were such a multiplier, then, for $\mathbf{f}_1,\mathbf{f}_2\in V$ with $\mathrm{Tr}\,S(\mathbf{f}_1,\mathbf{f}_2)=1$, we would get the contradiction

$$\begin{aligned}1 &= m(\mathbf{f}_1+\mathbf{f}_2,\mathbf{f}_1+\mathbf{f}_2) = m(\mathbf{f}_1+\mathbf{f}_2,\mathbf{f}_1+\mathbf{f}_2)m(\mathbf{f}_1,\mathbf{f}_2)^2\\ &= m(\mathbf{f}_1,\mathbf{f}_2+\mathbf{f}_1+\mathbf{f}_2)m(\mathbf{f}_2,\mathbf{f}_1+\mathbf{f}_2)m(\mathbf{f}_1,\mathbf{f}_2)\\ &= m(\mathbf{f}_1,\mathbf{f}_1)m(\mathbf{f}_2,\mathbf{f}_1+\mathbf{f}_2)(-1)^{\mathrm{Tr}\,S(\mathbf{f}_2,\mathbf{f}_1)}m(\mathbf{f}_2,\mathbf{f}_1)\\ &= -m(\mathbf{f}_2,\mathbf{f}_2+\mathbf{f}_1)m(\mathbf{f}_2,\mathbf{f}_1) = -m(\mathbf{f}_2+\mathbf{f}_2,\mathbf{f}_1)m(\mathbf{f}_2,\mathbf{f}_2)\\ &= -1\,.\end{aligned}$$

Actually, in the even characteristic case the minimal possible choice of a Weyl multiplier is

$$m(\mathbf{u},\mathbf{v}) = i^{g(\mathbf{u},\mathbf{v})}$$

for some function $g: V\times V\to\mathbb{Z}_4$. The function g must clearly be a $\mathbb{Z}_4$-valued multiplier. Moreover, properties (M.1) and (M.2) of a Weyl multiplier become as follows:

(M'.1) for any $D\in\mathcal{D}$, $g(\mathbf{d}_1,\mathbf{d}_2) = 0$ for all $\mathbf{d}_1,\mathbf{d}_2\in D$;

(M'.2) $g(\mathbf{v},\mathbf{u}) - g(\mathbf{u},\mathbf{v}) = 2\mathrm{Tr}\,S(\mathbf{u},\mathbf{v})$ for all $\mathbf{u},\mathbf{v}\in V$, where the map $z\mapsto 2z$ goes from $\mathbb{Z}_2$ to $\mathbb{Z}_4$.

The additional condition that m is T-invariant then requires that $g(A\mathbf{u},A\mathbf{v}) = g(\mathbf{u},\mathbf{v})$ for some generator A of T and all $\mathbf{u},\mathbf{v}\in V$.

In order to construct g, we need the fact that in even characteristic there exists a linear basis $\{\omega_1,\omega_2,\ldots,\omega_n\}$ of $\mathbb{F}$ over $\mathbb{Z}_2$ such that $\mathrm{Tr}\,(\omega_i\omega_j) = \delta_{i,j}$ for all $i,j\in\{1,2,\ldots,n\}$ (see Ref. 41, Theorem 4). After choosing such a basis, we also fix a sequence $r_1,r_2,\ldots,r_n$ in $\mathbb{Z}_4$ with $r_i = \pm1$. Then we define the following map $h:\mathbb{F}\to\mathbb{Z}_4$:

$$h\left(\sum_{i=1}^n z_i\omega_i\right) = \sum_{i=1}^n r_i z_i^2 \qquad \forall z_1,\ldots,z_n\in\mathbb{Z}_2\,.$$

Note that h is well defined, since the map $z\mapsto z^2$ is well defined from $\mathbb{Z}_2$ to $\mathbb{Z}_4$. Clearly, $h(0) = 0$. Moreover, if $\alpha = \sum_i z_i\omega_i$ and $\beta = \sum_i t_i\omega_i$, then

$$h(\alpha+\beta) = h(\alpha) + h(\beta) + 2\mathrm{Tr}\,\alpha\beta\,. \tag{12}$$

The construction of g is slightly different in the two cases in which the maximal torus T is split or nonsplit.

A. The split case

Let A be a generator of T with eigenvalues $\xi,\xi^{-1}\in\mathbb{F}$, and let $\{\mathbf{e}_1,\mathbf{e}_2\}$ be vectors of V such that $A\mathbf{e}_1 = \xi\mathbf{e}_1$ and $A\mathbf{e}_2 = \xi^{-1}\mathbf{e}_2$. Possibly rescaling $\mathbf{e}_2$, we can assume that $\{\mathbf{e}_1,\mathbf{e}_2\}$ is a symplectic basis of (V,S). We use this basis to define the following two $\mathbb{F}$-bilinear forms B_+ and B_- on V:

$$B_+(\mathbf{u},\mathbf{v}) = B_-(\mathbf{v},\mathbf{u}) = S(\mathbf{u},\mathbf{e}_1)\,S(\mathbf{v},\mathbf{e}_2) \qquad \forall \mathbf{u},\mathbf{v}\in V .$$

Since $B_+(\mathbf{u},\mathbf{u}) = B_-(\mathbf{u},\mathbf{u})$ for all $\mathbf{u}\in V$, the sum $B_+ + B_-$ is a symplectic form on V. Because $(B_+ + B_-)\,(\mathbf{e}_1,\mathbf{e}_2) = 1$, actually

$$B_+ + B_- = S .$$

Moreover, since $S(A\mathbf{u},\mathbf{e}_1) = S\left(\mathbf{u},A^{-1}\mathbf{e}_1\right) = \xi^{-1}S(\mathbf{u},\mathbf{e}_1)$ and similarly $S(A\mathbf{u},\mathbf{e}_2) = \xi S(\mathbf{u},\mathbf{e}_2)$, the bilinear forms B_+ and B_- are T-invariant, that is,

$$B_+(A\mathbf{u},A\mathbf{v}) = B_+(\mathbf{u},\mathbf{v}) \qquad \text{and} \qquad B_-(A\mathbf{u},A\mathbf{v}) = B_-(\mathbf{u},\mathbf{v}) \qquad \forall \mathbf{u},\mathbf{v}\in V .$$

We then define a $\mathbb{Z}_4$-valued multiplier g_0 on V, given by

$$g_0(\mathbf{u},\mathbf{v}) = 2\mathrm{Tr}\, B_+(\mathbf{u},\mathbf{v}) = 2\mathrm{Tr}\, B_-(\mathbf{v},\mathbf{u}) .$$

(The fact that g_0 is a multiplier follows from its biadditivity property $g_0(\mathbf{u}_1 + \mathbf{u}_2,\mathbf{v}) = g_0(\mathbf{u}_1,\mathbf{v}) + g_0(\mathbf{u}_2,\mathbf{v})$ and $g_0(\mathbf{u},\mathbf{v}_1 + \mathbf{v}_2) = g_0(\mathbf{u},\mathbf{v}_1) + g_0(\mathbf{u},\mathbf{v}_2)$.) Condition (M'.2) holds for g_0. However, to make also condition (M'.1) satisfied, we need to introduce the equivalent $\mathbb{Z}_4$-valued multiplier g, with

$$g(\mathbf{u},\mathbf{v}) = h(B_+(\mathbf{u}+\mathbf{v},\mathbf{u}+\mathbf{v})^{1/2}) - h(B_+(\mathbf{u},\mathbf{u})^{1/2}) - h(B_+(\mathbf{v},\mathbf{v})^{1/2}) + g_0(\mathbf{u},\mathbf{v}) . \tag{13}$$

Indeed, for all $\lambda,\mu\in\mathbb{F}$, by the property (12) of h,

$$\begin{aligned} g(\lambda\mathbf{u},\mu\mathbf{u}) &= h((\lambda+\mu)B_+(\mathbf{u},\mathbf{u})^{1/2}) - h(\lambda B_+(\mathbf{u},\mathbf{u})^{1/2}) - h(\mu B_+(\mathbf{u},\mathbf{u})^{1/2}) \\ &\quad +2\mathrm{Tr}\,\lambda\mu B_+(\mathbf{u},\mathbf{u}) \\ &= 0 . \end{aligned}$$

Finally, from the analogous property of B_+, it immediately follows that $g(A\mathbf{u},A\mathbf{v}) = g(\mathbf{u},\mathbf{v})$ for all $\mathbf{u},\mathbf{v}\in V$, hence g is T-invariant.

We have thus found the T-invariant Weyl multiplier $m = i^g$. We can use the construction of Section II E, with the symplectic basis $\{\mathbf{e}_1,\mathbf{e}_2\}$ given by the above eigenbasis of A, in order to exhibit the quadrature system $\mathsf{Q}\in\mathcal{Q}_{T\rtimes V}(\Omega,S)$ having m as its associated multiplier. To this aim, it is enough to evaluate

$$m(\alpha_1\mathbf{e}_1,\alpha_2\mathbf{e}_2) = i^{h\left((\alpha_1\alpha_2)^{1/2}\right)} \tag{14}$$

and insert it into (4) and (5) to get

$$\mathsf{Q}(o+\mathbf{v}+\mathbb{F}\mathbf{u})\phi_\gamma = \frac{1}{|\mathbb{F}|}\sum_{\lambda\in\mathbb{F}} i^{h(\lambda(\alpha_1\alpha_2)^{1/2})}(-1)^{\mathrm{Tr}\,\lambda[\alpha_2(\beta_1+\gamma)+\alpha_1\beta_2]}\phi_{\gamma+\lambda\alpha_1}$$
$$\text{with} \qquad \mathbf{u} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2, \qquad \mathbf{v} = \beta_1\mathbf{e}_1 + \beta_2\mathbf{e}_2$$

with its associated centered Weyl system

$$W_o(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2)\phi_\gamma = i^{h\left((\alpha_1\alpha_2)^{1/2}\right)}(-1)^{\mathrm{Tr}\,\alpha_2\gamma}\phi_{\gamma+\alpha_1} .$$

In order to determine the unitary operator $U(A)$ yielding the T-covariance, we can either use (11) or simply notice that $U(A)\phi_0 = c\phi_0$ for some scalar $c\in\mathbb{C}$, since $U(A)\mathsf{Q}(o+\mathbb{F}\mathbf{e}_2) = \mathsf{Q}(o+\mathbb{F}\mathbf{e}_2)U(A) \equiv c\mathsf{Q}(o+\mathbb{F}\mathbf{e}_2)$ by T-covariance. On the other basis vectors,

$$U(A)\phi_\gamma = U(A)W_o(\gamma\mathbf{e}_1)\phi_0 = W_o(\gamma A\mathbf{e}_1)U(A)\phi_0 = cW_o(\gamma\xi\mathbf{e}_1)\phi_0 = c\phi_{\gamma\xi} .$$

U becomes an ordinary representation of T by setting $c = 1$.

B. The nonsplit case

Let A and ξ,ξ^{-1} be as in the previous case. Now, $\xi,\xi^{-1}\in\tilde{\mathbb{F}}\setminus\mathbb{F}$ with $\xi^{-1} = \overline{\xi}$, and A is diagonalized in the extension $\tilde{V} = \tilde{\mathbb{F}}\otimes_{\mathbb{F}} V$ of V to the scalars $\tilde{\mathbb{F}}$. Let $\mathbf{e}\in\tilde{V}$ be a nonzero vector such that $A\mathbf{e} = \xi\mathbf{e}$. Then $A\overline{\mathbf{e}} = \overline{A\mathbf{e}} = \overline{\xi}\overline{\mathbf{e}}$, where we still denote by $\overline{\cdot}$ the $\tilde{\mathbb{F}}$-antilinear map on $\tilde{V}$ which restricts to the identity on V. The $\mathbb{F}$-bilinear form S uniquely extends to a symplectic form on $\tilde{V}$. Note that $S(\overline{\mathbf{u}},\overline{\mathbf{v}}) = \overline{S(\mathbf{u},\mathbf{v})}$.

In particular, $S\,(\mathbf{e},\bar{\mathbf{e}})\in\mathbb{F}$; hence, possibly rescaling both $\mathbf{e}$ and $\bar{\mathbf{e}}$ by the factor $S(\mathbf{e},\bar{\mathbf{e}})^{-1/2}$, we can assume that $\{\mathbf{e},\bar{\mathbf{e}}\}$ is a symplectic basis of $(\tilde{V},S)$. Now, as in the split case, we define the $\tilde{\mathbb{F}}$-bilinear forms on $\tilde{V}$,

$$B_+(\mathbf{u},\mathbf{v})=B_-(\mathbf{v},\mathbf{u})=S\,(\mathbf{u},\mathbf{e})\,S\,(\mathbf{v},\bar{\mathbf{e}})\qquad\forall\mathbf{u},\mathbf{v}\in\tilde{V}\,.$$

Again, $B_+(\mathbf{u},\mathbf{u})=B_-(\mathbf{u},\mathbf{u})$ for all $\mathbf{u}\in\tilde{V}$, $B_++B_-=S$, and the forms B_+ and B_- are T-invariant. Moreover, although B_+ and B_- are $\tilde{\mathbb{F}}$-valued bilinear forms, the corresponding quadratic forms restrict to $\mathbb{F}$-valued forms on V: $B_+(\mathbf{u},\mathbf{u})=B_-(\mathbf{u},\mathbf{u})\in\mathbb{F}$ for all $\mathbf{u}\in V$. Let $\widetilde{\mathrm{Tr}}:\tilde{\mathbb{F}}\to\mathbb{Z}_2$ be any $\mathbb{Z}_2$-linear extension of Tr to $\tilde{\mathbb{F}}$. (For example, if ζ is any element of $\tilde{\mathbb{F}}\setminus\mathbb{F}$, we can set $\widetilde{\mathrm{Tr}}(\alpha+\beta\zeta)=\mathrm{Tr}\,\alpha$ for all $\alpha,\beta\in\mathbb{F}$.) We then define the following $\mathbb{Z}_4$-valued biadditive multiplier g_0 on V:

$$g_0(\mathbf{u},\mathbf{v})=2\widetilde{\mathrm{Tr}}\,B_+(\mathbf{u},\mathbf{v})=2\widetilde{\mathrm{Tr}}\,B_-(\mathbf{v},\mathbf{u})\qquad\forall\mathbf{u},\mathbf{v}\in V$$

and its equivalent multiplier g as in formula (13). Since g_0 satisfies condition (M'.2), so does g. Moreover, g also fulfills (M'.1) and is T-invariant, the computation being the same as in the split case. In conclusion, $m=i^g$ is a T-invariant Weyl multiplier on V.

As in Section V A, we are now going to explicitly exhibit the $T\rtimes V$-covariant quadrature system $\mathsf{Q}\in\mathcal{Q}_V(\Omega,S,m)$ along the lines of Section II E. In the present case, we fix the following symplectic basis $\{\mathbf{e}_1,\mathbf{e}_2\}$ of V:

$$\mathbf{e}_1=\bar{\varepsilon}\mathbf{e}+\varepsilon\bar{\mathbf{e}},\qquad\mathbf{e}_2=\varepsilon\mathbf{e}+\bar{\varepsilon}\bar{\mathbf{e}}\qquad\text{with}\qquad\varepsilon=(\xi+1)^{-1/2}\,.\tag{15}$$

Moreover, we choose the extension $\widetilde{\mathrm{Tr}}$ such that $\widetilde{\mathrm{Tr}}\,\varepsilon^2=0$. Then, with some manipulations (reported in the Appendix),

$$m(\alpha_1\mathbf{e}_1,\alpha_2\mathbf{e}_2)=i^{h\left((\alpha_1\alpha_2)^{1/2}\right)}(-1)^{\mathrm{Tr}\left[\alpha_1\alpha_2\varepsilon\bar{\varepsilon}+(\alpha_1+\alpha_2)(\alpha_1\alpha_2\varepsilon\bar{\varepsilon})^{1/2}\right]},\tag{16}$$

$$\begin{aligned}&m(\alpha_1\mathbf{e}_1+\alpha_2\mathbf{e}_2,\ (A+I)^{-1}(\alpha_1\mathbf{e}_1+\alpha_2\mathbf{e}_2))=\\&\quad=i^{-\left[h\left(\alpha_1(\varepsilon\bar{\varepsilon})^{1/2}\right)+h\left(\alpha_2(\varepsilon\bar{\varepsilon})^{1/2}\right)+h\left((\alpha_1\alpha_2)^{1/2}\right)\right]}(-1)^{\mathrm{Tr}\left[\alpha_1\alpha_2\varepsilon\bar{\varepsilon}+(\alpha_1+\alpha_2)(\alpha_1\alpha_2\varepsilon\bar{\varepsilon})^{1/2}\right]}\,.\end{aligned}\tag{17}$$

By (4) and (5),

$$\begin{aligned}\mathsf{Q}(o+\mathbf{v}+\mathbb{F}\mathbf{u})\phi_\gamma&=\frac{1}{|\mathbb{F}|}\sum_{\lambda\in\mathbb{F}}i^{h\left(\lambda(\alpha_1\alpha_2)^{1/2}\right)}\\&\qquad\times(-1)^{\mathrm{Tr}\,\lambda\left\{\lambda\left[\alpha_1\alpha_2\varepsilon\bar{\varepsilon}+(\alpha_1+\alpha_2)(\alpha_1\alpha_2\varepsilon\bar{\varepsilon})^{1/2}\right]+\alpha_2(\beta_1+\gamma)+\alpha_1\beta_2\right\}}\phi_{\gamma+\lambda\alpha_1}\,,\\W_o(\mathbf{u})\phi_\gamma&=i^{h\left((\alpha_1\alpha_2)^{1/2}\right)}(-1)^{\mathrm{Tr}\left[\alpha_1\alpha_2\varepsilon\bar{\varepsilon}+(\alpha_1+\alpha_2)(\alpha_1\alpha_2\varepsilon\bar{\varepsilon})^{1/2}+\alpha_2\gamma\right]}\phi_{\gamma+\alpha_1}\\&\qquad\qquad\text{with}\qquad\mathbf{u}=\alpha_1\mathbf{e}_1+\alpha_2\mathbf{e}_2\qquad\mathbf{v}=\beta_1\mathbf{e}_1+\beta_2\mathbf{e}_2\,.\end{aligned}$$

Moreover, by (11),

$$\begin{aligned}U(A)\phi_\gamma&=\frac{1}{|\mathbb{F}|}\sum_{\alpha_1,\alpha_2\in\mathbb{F}}m(\alpha_1\mathbf{e}_1+\alpha_2\mathbf{e}_2,\ (A+I)^{-1}(\alpha_1\mathbf{e}_1+\alpha_2\mathbf{e}_2))\\&\qquad\times W_o(\alpha_1\mathbf{e}_1+\alpha_2\mathbf{e}_2)\phi_\gamma\\&=\frac{1}{|\mathbb{F}|}\sum_{\alpha_1,\alpha_2\in\mathbb{F}}i^{-\left[h\left(\alpha_1(\varepsilon\bar{\varepsilon})^{1/2}\right)+h\left(\alpha_2(\varepsilon\bar{\varepsilon})^{1/2}\right)\right]}(-1)^{\mathrm{Tr}\,\alpha_2\gamma}\phi_{\gamma+\alpha_1}\,.\end{aligned}$$

As a final consideration, observe that in both the split and nonsplit cases, our construction provides a quite big amount of different T-invariant Weyl multipliers. Indeed, for a fixed choice of the orthonormal basis $\{\omega_1,\omega_2,\ldots,\omega_n\}$ of $\mathbb{F}$ over $\mathbb{Z}_2$, changing the sequence of signs $r_1,r_2,\ldots,r_n$ in the definition of h yields 2^n different Weyl multipliers m; this can be seen by direct inspection of (14) and (16). Consequently, the set $\mathcal{Q}_{T\rtimes V}(\Omega,S)$ contains at least 2^n inequivalent quadratures. This shows that in even characteristic, there exists a large degree of arbitrarity in the choice of a maximally covariant quadrature system.

VI. CONCLUSIONS

We have found all the extended symmetries of stabilizer MUBs in even prime-power dimensions beyond the basic group V of phase-space translations. We have proved that only two inequivalent such extensions are possible, namely, by means of either a split or a nonsplit torus $T \subset \mathrm{SL}(V)$. In particular, it turns out that both of the possibilities give rise to whole families of inequivalent maximally symmetric stabilizer MUBs, contrasting with the case in odd prime-power dimensions, where the maximal symmetry requirement points out a single class of stabilizer MUBs. For each of the two extensions, we have focused on a particular family of inequivalent maximally symmetric stabilizer MUBs, providing both the explicit form of the MUBs (more precisely, of their associated rank-1 projections that we named *quadrature system*) and the expression of the covariance operators.

In the applications, one is usually interested in finding the smallest groups of unitary operators cycling all the bases in a given maximal set of MUBs.[27–29,31,32] For maximally symmetric stabilizer MUBs, this corresponds to requiring a maximal nonsplit torus as the extra symmetry group (see Ref. 22, Section 8), since split toruses do not cycle the two bases corresponding to the directions they keep fixed.

As a final consideration, in our approach the symmetry properties of stabilizer MUBs are essentially related to their labelings with the phase-space lines. Indeed, we stressed in Remarks 1 and 3 that, for any pair of V-covariant quadratures Q_1 and Q_2, the two sets of rank-1 projections $\mathrm{ran}\,\mathsf{Q}_i = \{\mathsf{Q}_i(\mathfrak{l}) \mid \mathfrak{l} \in L(\Omega)\}$ $(i = 1, 2)$ are always unitarily conjugated, although of course Q_1 and Q_2 may not be equivalent in the sense of (1). Now, we essentially dealt with the problem of how to arrange the phase-space labeling of stabilizer MUBs in order to make them "as covariant as possible" under the natural symmetries of the phase-space. Our definition of covariance (actually, the only possible one) is expressed by (2). However, as pointed out in Ref. 22, Remark 7.8, the operators $U(g)$ satisfying (2) do not exhaust all unitaries preserving the (unlabeled) set of projections $\mathrm{ran}\,\mathsf{Q}$ of some $\mathsf{Q} \in \mathcal{Q}_{G_0 \rtimes V}(\Omega)$. In fact, the full Clifford transform group defined in Refs. 42 and 43 still leaves the set $\mathrm{ran}\,\mathsf{Q}$ invariant,[23,31,33,34] although its action on MUBs cannot be related to any phase-space structure by Theorem 4.

ACKNOWLEDGMENTS

The authors wish to thank Professor Markus Grassl for suggesting the problem. J.S. acknowledges financial support from the EU through the Collaborative Projects QuProCS (Grant Agreement No. 641277).

APPENDIX: AUXILIARY CALCULATIONS

Here we provide the explicit calculations leading to (16) and (17). For the $\mathbb{Z}_4$-valued multiplier g found in Section V B, in the basis (15) and for $\alpha_1, \alpha_2 \in \mathbb{F}$, we have

$$\begin{aligned}
g(\alpha_1\mathbf{e}_1, \alpha_2\mathbf{e}_2) = {} & h\left(\left[S(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2, \mathbf{e})\, S(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2, \overline{\mathbf{e}})\right]^{1/2}\right) \\
& - h\left(\left[S(\alpha_1\mathbf{e}_1, \mathbf{e})\, S(\alpha_1\mathbf{e}_1, \overline{\mathbf{e}})\right]^{1/2}\right) - h\left(\left[S(\alpha_2\mathbf{e}_2, \mathbf{e})\, S(\alpha_2\mathbf{e}_2, \overline{\mathbf{e}})\right]^{1/2}\right) \\
& + 2\widetilde{\mathrm{Tr}}\, S(\alpha_1\mathbf{e}_1, \mathbf{e})\, S(\alpha_2\mathbf{e}_2, \overline{\mathbf{e}}) \\
= {} & h\left(\left[(\alpha_1\varepsilon + \alpha_2\overline{\varepsilon})(\alpha_1\overline{\varepsilon} + \alpha_2\varepsilon)\right]^{1/2}\right) \\
& - h\left(\alpha_1(\varepsilon\overline{\varepsilon})^{1/2}\right) - h\left(\alpha_2(\overline{\varepsilon}\varepsilon)^{1/2}\right) + 2\widetilde{\mathrm{Tr}}\, \alpha_1\alpha_2\varepsilon^2 \\
= {} & h\left(\left[(\alpha_1^2 + \alpha_2^2)\varepsilon\overline{\varepsilon} + \alpha_1\alpha_2\right]^{1/2}\right) && \text{because } \varepsilon^2 + \overline{\varepsilon}^2 = 1 \\
& - h\left(\alpha_1(\varepsilon\overline{\varepsilon})^{1/2}\right) - h\left(\alpha_2(\overline{\varepsilon}\varepsilon)^{1/2}\right) && \text{because } \widetilde{\mathrm{Tr}}\,\varepsilon^2 = 0 \\
= {} & h\left((\alpha_1 + \alpha_2)(\varepsilon\overline{\varepsilon})^{1/2} + (\alpha_1\alpha_2)^{1/2}\right) && \text{by } \mathbb{Z}_2\text{-linearity of } \cdot^{\,1/2} \\
& - h\left(\alpha_1(\varepsilon\overline{\varepsilon})^{1/2}\right) - h\left(\alpha_2(\overline{\varepsilon}\varepsilon)^{1/2}\right) \\
= {} & h\left((\alpha_1\alpha_2)^{1/2}\right) + 2\mathrm{Tr}\left[\alpha_1\alpha_2\varepsilon\overline{\varepsilon} + (\alpha_1 + \alpha_2)(\alpha_1\alpha_2\varepsilon\overline{\varepsilon})^{1/2}\right] && \text{by (12).}
\end{aligned}$$

This proves (16). Concerning (17),

$$
\begin{aligned}
& g(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2,\ (A+I)^{-1}(\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2)) = \\
&\quad = g(\alpha\mathbf{e} + \overline{\alpha}\overline{\mathbf{e}},\ (A+I)^{-1}(\alpha\mathbf{e} + \overline{\alpha}\overline{\mathbf{e}})) && \text{with } \alpha = \alpha_1\overline{\varepsilon} + \alpha_2\varepsilon \\
&\quad = g(\alpha\mathbf{e} + \overline{\alpha}\overline{\mathbf{e}},\ \varepsilon^2\alpha\mathbf{e} + \overline{\varepsilon}^2\overline{\alpha}\overline{\mathbf{e}}) \\
&\quad = h\left(\left[S\left((1+\varepsilon^2)\alpha\mathbf{e} + (1+\overline{\varepsilon}^2)\overline{\alpha}\overline{\mathbf{e}}, \mathbf{e}\right) S\left((1+\varepsilon^2)\alpha\mathbf{e} + (1+\overline{\varepsilon}^2)\overline{\alpha}\overline{\mathbf{e}}, \overline{\mathbf{e}}\right)\right]^{1/2}\right) \\
&\qquad - h\left(\left[S\left(\alpha\mathbf{e} + \overline{\alpha}\overline{\mathbf{e}}, \mathbf{e}\right) S\left(\alpha\mathbf{e} + \overline{\alpha}\overline{\mathbf{e}}, \overline{\mathbf{e}}\right)\right]^{1/2}\right) \\
&\qquad - h\left(\left[S\left(\varepsilon^2\alpha\mathbf{e} + \overline{\varepsilon}^2\overline{\alpha}\overline{\mathbf{e}}, \mathbf{e}\right) S\left(\varepsilon^2\alpha\mathbf{e} + \overline{\varepsilon}^2\overline{\alpha}\overline{\mathbf{e}}, \overline{\mathbf{e}}\right)\right]^{1/2}\right) \\
&\quad = h\left(\left[(1+\overline{\varepsilon}^2)\overline{\alpha}(1+\varepsilon^2)\alpha\right]^{1/2}\right) - h\left((\overline{\alpha}\alpha)^{1/2}\right) - h\left(\left(\overline{\varepsilon}^2\overline{\alpha}\varepsilon^2\alpha\right)^{1/2}\right) \\
&\quad = -h\left((\overline{\alpha}\alpha)^{1/2}\right) && \text{because } \varepsilon^2 + \overline{\varepsilon}^2 = 1 \\
&\quad = -h\left(\left[(\alpha_1^2 + \alpha_2^2)\varepsilon\overline{\varepsilon} + \alpha_1\alpha_2\right]^{1/2}\right) && \text{because } \varepsilon^2 + \overline{\varepsilon}^2 = 1 \\
&\quad = -h\left((\alpha_1 + \alpha_2)(\varepsilon\overline{\varepsilon})^{1/2} + (\alpha_1\alpha_2)^{1/2}\right) && \text{by } \mathbb{Z}_2\text{-linearity of } \cdot^{\ 1/2} \\
&\quad = -\left[h\left(\alpha_1(\varepsilon\overline{\varepsilon})^{1/2}\right) + h\left(\alpha_2(\varepsilon\overline{\varepsilon})^{1/2}\right) + h\left((\alpha_1\alpha_2)^{1/2}\right)\right] \\
&\qquad + 2\mathrm{Tr}\left[\alpha_1\alpha_2\varepsilon\overline{\varepsilon} + (\alpha_1+\alpha_2)(\alpha_1\alpha_2\varepsilon\overline{\varepsilon})^{1/2}\right] && \text{by (12)}
\end{aligned}
$$

which gives (17).

[1] W. K. Wootters, "A Wigner-function formulation of finite-state quantum mechanics," Ann. Phys. **176**(1), 1–21 (1987).

[2] O. Cohendet, P. Combe, and M. Sirugue-Collin, "Fokker-Planck equation associated with the Wigner function of a quantum system with a finite number of states," J. Phys. A: Math. Gen. **23**(11), 2001–2011 (1990).

[3] U. Leonhardt, "Discrete Wigner function and quantum-state tomography," Phys. Rev. A **53**(5), 2998–3013 (1996).

[4] A. Vourdas, "Quantum systems with finite Hilbert space," Rep. Prog. Phys. **67**(3), 267–320 (2004).

[5] D. Gross, "Hudson's theorem for finite-dimensional quantum systems," J. Math. Phys. **47**(12), 122107 (2006).

[6] D. M. Appleby, I. Bengtsson, and S. Chaturvedi, "Spectra of phase point operators in odd prime dimensions and the extended Clifford group," J. Math. Phys. **49**(1), 012102 (2008).

[7] C. Ferrie, "Quasi-probability representations of quantum theory with applications to quantum information science," Rep. Prog. Phys. **74**(11), 116001 (2011).

[8] J. Schwinger, "Unitary operator bases," Proc. Natl. Acad. Sci. U.S.A. **46**(4), 570–579 (1960).

[9] L. Auslander and R. Tolimieri, "Is computing with the finite Fourier transform pure or applied mathematics?," Bull. Am. Math. Soc. **1**(6), 847–897 (1979).

[10] V. S. Varadarajan, "Variations on a theme of Schwinger and Weyl," Lett. Math. Phys. **34**(3), 319–326 (1995).

[11] R. E. Howe, "On the character of Weil's representation," Trans. Am. Math. Soc. **177**, 287–298 (1973).

[12] P. Gérardin, "Weil representations associated to finite fields," J. Algebra **46**(1), 54–101 (1977).

[13] R. Balian and C. Itzykson, "Observations sur la mécanique quantique finie," C. R. Acad. Sci. Paris Sér. I Math. **303**(16), 773–778 (1986).

[14] M. Neuhauser, "An explicit construction of the metaplectic representation over a finite field," J. Lie Theory **12**(1), 15–30 (2002).

[15] D. M. Appleby, "Symmetric informationally complete-positive operator valued measures and the extended Clifford group," J. Math. Phys. **46**(5), 052107 (2005).

[16] A. Vourdas, "Galois quantum systems," J. Phys. A: Math. Gen. **38**(39), 8453–8471 (2005).

[17] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, "A new proof for the existence of mutually unbiased bases," Algorithmica **34**(4), 512–528 (2002).

[18] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, "Discrete phase space based on finite fields," Phys. Rev. A **70**(6), 062101 (2004).

[19] R. Howe, "Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries,"Indagationes Math. **16**(3-4), 553–583 (2005).

[20] P. Šulc and J. Tolar, "Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions," J. Phys. A: Math. Theory **40**(50), 15099–15111 (2007).

[21] T. Durt, B.-G. Englert, I. Bengtsson, and K. Yczkowski, "On mutually unbiased bases," Int. J. Quantum Inf. **8**(4), 535–640 (2010).

[22] C. Carmeli, J. Schultz, and A. Toigo, "Covariant mutually unbiased bases," Rev. Math. Phys. **28**(4), 1650009 (2016).

[23] H. Zhu, "Permutation symmetry determines the discrete Wigner function," Phys. Rev. Lett. **116**(4), 040501 (2016).

[24] J. Dehaene and B. De Moor, "Clifford group, stabilizer states, and linear and quadratic operations over *GF*(2)," Phys. Rev. A **68**(4), 042318 (2003).

[25] M. Grassl, M. Rötteler, and T. Beth, "Efficient quantum circuits for non-qubit quantum error-correcting codes," Int. J. Found. Comput. Sci. **14**(5), 757–775 (2003).

[26] D. Schlingemann, "Cluster states, algorithms and graphs," Quantum Inf. Comput. **4**(4), 287–324 (2004).
[27] H. F. Chau, "Unconditionally secure key distribution in higher dimensions by depolarization," IEEE Trans. Inf. Theory **51**(4), 1451–1468 (2005).
[28] W. K. Wootters and D. M. Sussman, "Discrete phase space and minimum-uncertainty states," in *Proceedings of the Eighth International Conference on Quantum Communication, Measurement and Computing* (NICT Press, 2007); e-print arXiv:0704.1277.
[29] D. M. Sussman, "Minimum-uncertainty states and rotational invariance in discrete phase space," B.A. thesis, William College, 2007.
[30] D. Appleby, I. Bengtsson, and H. Dang, "Galois unitaries, mutually unbiased bases, and MUB-balanced states," Quantum Inf. Comput. **15**(15-16), 1261–1269 (2015).
[31] H. Zhu, "Sharply covariant mutually unbiased bases," e-print arXiv:1503.00003.
[32] H. Zhu, "Nonexistence of sharply covariant mutually unbiased bases in odd prime dimensions," Phys. Rev. A **92**(3), 032301 (2015).
[33] H. Zhu, "Mutually unbiased bases as minimal Clifford covariant 2-designs," Phys. Rev. A **91**(6), 060301(R) (2015).
[34] H. Zhu, "Multiqubit Clifford groups are unitary 3-designs," e-print arXiv:1510.02619.
[35] E. H. Moore, *The Subgroups of the Generalized Finite Modular Group* (Dicennial Publications of the University of Chicago, 1904), Vol. 9(12), pp. 141–190.
[36] A. Wiman, "Bestimmung aller untergruppen einer doppelt unendlichen reihe von einfachen gruppen," Stockh. Akad. Bihang **25**(2), 1–47 (1899).
[37] L. E. Dickson, *Linear Groups, with an Exposition of the Galois Field Theory* (Dover Publications, Inc., New York, 1958).
[38] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, No. 211 (Springer-Verlag, New York, 2002).
[39] M. Suzuki, *Group Theory. I,* Grundlehren der Mathematischen Wissenschaften (Springer-Verlag, Berlin, New York, 1982).
[40] J. E. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, No. 21 (Springer-Verlag, New York, Heidelberg, 1975).
[41] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," SIAM J. Comput. **9**(4), 758–767 (1980).
[42] B. Bolt, T. G. Room, and G. E. Wall, "On the Clifford collineation, transform and similarity groups. I," J. Aust. Math. Soc. **2**(1), 60–79 (1961).
[43] B. Bolt, T. G. Room, and G. E. Wall, "On the Clifford collineation, transform and similarity groups. II," J. Aust. Math. Soc. **2**(1), 80–96 (1961).
[44] A *symplectic form* is a nonzero $\mathbb{F}$-bilinear map $S : V \times V \to \mathbb{F}$ such that $S(\mathbf{v}, \mathbf{v}) = 0$ for all $\mathbf{v} \in V$. Such a form is symmetric in characteristic $p = 2$ and antisymmetric in characterisitc $p \neq 2$. Moreover, since V is 2-dimensional, S is uniquely determined up to multiplication by a scalar in $\mathbb{F}_* = \mathbb{F} \setminus \{0\}$.