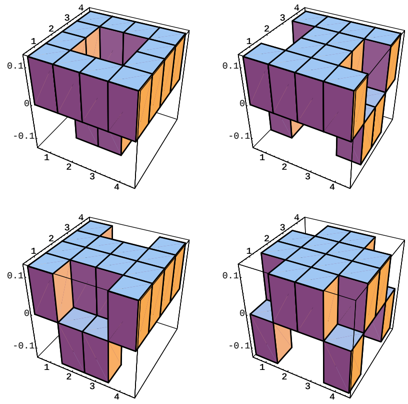
Finite Phase Space Methods in Quantum Information



David Gross

Diploma Thesis

Universität Potsdam 2005

Contents

1 Preface

This thesis is divided into two parts. In the first half, we will define and discuss notions as the *Heisenberg group*, the *characteristic function* and the *Wigner function* in the context of finite-dimensional quantum systems. As the purpose of this part is to *construct* and to *explain* these phase-space related concepts, it is written in a more narrative style. The second part of the thesis aims at contributing to a long-standing open problem in the theory of stabilizer codes. In order to achive rigour, a formal, mathematical style of presentation has been employed.

Part I

From the Heisenberg Group to Discrete Wigner Functions

2 Introduction

In Ref. [3] Wigner introduced a representation of hermitian operators on a complex Hilbert space by real functions on $\mathbb{R}^2$ to solve a thermodynamical problem. The Wigner functions associated to density operators have triggered fantasies of physicists ever since, because they resemble some features of classical probability distributions on phase space and allow for a visualization of quantum states. Beginning with the work of Wootters [4], the question arose of how Wigner functions could be defined for finite dimensional quantum systems. As any generalization of a concept is non-unique, a whole collection of different proposals appeared in the literature (see for example Ref. [4, 5, 6, 7, 8, 10]). The question that started of this work is, can we formulate the definition of the Wigner function using only terms that have a well-defined meaning in both the finite and the infinite setting? Candidates for such notions would be *algebraic fields*, *Fourier transformations* or *vector spaces with forms*. Such a formulation might lead to a somewhat canonic definition of the discrete offspring of the well-known concept. As a next step one can ask whether such a formulation facilitates the understanding of the connection of Wigner functions to other phase space related concepts, such as the *Weyl representation*, the *characteristic function* of a density operator or the *stabilizer formalism* used in quantum information theory.

The preceding paragraph lays down the road map for this first part. We will restrict our discussion to finite systems, but, at each point, it should be straight-forward to recover the well-known continuous definitions by substituting finite fields, vector spaces or Fourier transformations by their infinite cousins.

3 Mathematical Preliminaries

In this section, we will shortly comment on some mathematical concepts that are not generally used by physicists.

3.1 Fields

The notion of an *algebraic field* is basic to algebra and there should be no need to introduce it. Therefore, we will only list some useful facts on *finite fields*, mostly taken from Ref. [1].

1. All finite fields have prime-power order. Let $d = p^r$ be a power of a prime p. Then there is one unique finite field of order q, denoted by $\mathbb{F}_q$.
2. Fields of prime order p are isomorphic to the familiar *arithmetic modulo* p of residue classes $\mathbb{Z}/\langle p \rangle$.
3. Fields of prime power order $d = p^r$ can be constructed by *extending* $\mathbb{F}_p$. In this case, $\mathbb{F}_p$ is refered to as the *base field* of $\mathbb{F}_{p^r}$. There is a subfield in $\mathbb{F}_{p^r}$ which is isomorphic to the base field.
4. If $\mathbb{F}_d, d = p^r$ is an extension field of $\mathbb{F}_p$, then the *additive* structure of $\mathbb{F}_d$ is isomorphic to the r-fold Cartesian product of the base field $\mathbb{F}_p^r$. In that sense,

an extension field can be viewed as an r-dimensional vector space over the base field. Taking that point of view, it is natural to call a subset $B = \{f_i\}_{i=1\cdots r}$ of $\mathbb{F}_d$ a *basis* if the span of B with coefficients in the base field is all of $\mathbb{F}_d$.

5. A field is *cyclic* if every element a of $\mathbb{F}$ can be written as

$$a = 1 + \cdots + 1 \tag{1}$$

that is, if its additive structure is a cycle group. Using the Remarks 2 and 4 it is easy to see that a field is cyclic if and only if it is of prime order.

6. Let $\mathbb{F}_d, d = p^r$ be an extension field. The trace operator is defined by

$$\operatorname{Tr} f = \sum_{k=0}^{r-1} f^{d^k}. \tag{2}$$

The range of the trace is the base field and, further, Tr is $\mathbb{F}_p$-linear. Therefore, the function

$$\langle f, g\rangle \mapsto \operatorname{Tr}(fg) \tag{3}$$

is a bilinear form which can be checked to be non-degenerate. It thus defines a scalar product on $\mathbb{F}_d$ viewed as an $\mathbb{F}_p$-vector space.

7. Let $\{f_i\}$ be a basis of $\mathbb{F}_d$. There always exists a set $\{f^i\}$ such that

$$\langle f_i, f^j\rangle = \delta_i^j. \tag{4}$$

Such a set is called a *dual basis* of $\{f_i\}$. *Self-dual bases* do not always exist. However, for extensions of $\mathbb{F}_2$, their existence is guaranteed [1].

3.1.1 Computer Implementation

A set of packages for the computer algebra system Mathematica has been developed alongside with the theoretical work in this thesis[1]. At the end of each paragraph, we will present the computer routines that correspond to the newly introduced concepts. These 'Computer Implementation' sections serve both as examples to the abstract concepts and as a documentation of the computer program.

The computer implementation is distributed over a couple of *Mathematica* `.m`-Packages. The primary package is **`head.m`**, which must be loaded in the first line of any notebook that uses the library.

```
In[1]:= <<head.m
```

Next, load in the finite fields package. It extends *Mathematica's* built in finite fields support.

```
In[2]:= <<finiteFields.m
```

The package requires the global variables **`p`** and **`r`** to be set.

```
In[3]:= p = 3; r = 2;
```

[1] These packages are available for download at http://gross.qipc.org/.

It defines the global variable **F** which represents the extension field of order p^r over $\mathbb{F}_p$.

In[4]:= **F**
Out[4]= GF[3,{2,1,1}]

The following lines show how field elements are entered and printed. The format is explained in the documentation of *Mathematica*.

In[5]:= **F[{1,0}]**
Out[5]= $\{1,0\}_3$

The natural operations are addition...

In[6]:= **F[{1,1}] + F[{2,0}]**
Out[6]= $\{0,1\}_3$

...and multiplication.

In[7]:= **F[{1,1}]F[{2,0}]**
Out[7]= $\{2,2\}_3$

Unlike *Mathematica*, the **finiteFields** package supports *mixed* operations involving integers and field elements.

In[8]:= **2F[{1,1}] + 1**
Out[8]= $\{0,2\}_3$

The integers are converted to field elements by use of the function **enf[]** (which abbreviates 'enforce field'). It is a wrapper to *Mathematica's* **FromElementCode[]**.

In[9]:= **enf[2]**
Out[9]= $\{2,0\}_3$

The inverse of **fec[]** is **tec[]**, a wrapper for **ToElementCode[]**.

In[10]:= **tec[enf[2]]**
Out[10]= 2

The variable **inv** stands shorthand for the multiplicative inverse of two.

In[11]:= **inv**
Out[11]= $\{2,0\}_3$

In[12]:= **% F[{2,0}]**
Out[12]= $\{1,0\}_3$

Lastly, the trace has been implemented.

In[13]:= **Tr[F[{2,2}]]**
Out[13]= $\{2,0\}_3$

3.2 Characters

Let G be a finite abelian group. A *character* χ of G is a homomorphism from G into the *circle group* S^1, that is, the set of complex numbers of modulus one with multiplication of complex numbers as the group composition law. The pointwise product of two characters is again a character and – if the inverse is defined via $\chi^{-1} := \chi^*$ – the set of all characters of G becomes a group of its own. This group is called G's *dual group* and denoted by $\hat{G}$. The duality relation is symmetric in that an element of G can be viewed as a character of $\hat{G}$ by setting

$$g(\chi) := \chi(g) \tag{5}$$

for $g \in G, \chi \in \hat{G}$. To stress the symmetry between the group and its dual, we write

$$\langle \chi | g \rangle := \langle g | \chi \rangle := \chi(g). \tag{6}$$

Finite abelian groups have the pleasant property of being isomorphic to their respective dual groups. However, in general there is no *canonic* way of identifying G with $\hat{G}$. In the sequel we will construct isomorphisms $G \to \hat{G}$ for some specific examples.

The following fact should be kept in mind:

$$\sum_{g \in G} \langle \chi | g \rangle \langle g | \zeta \rangle \quad = \quad |G| \; \delta_{\chi, \zeta^{-1}}. \tag{7}$$

3.2.1 Characters of Finite Fields

If $\mathbb{F} = \mathbb{F}_p$ is of prime order, then

$$a \mapsto \chi_a(\cdot) := \omega^{a \cdot} \tag{8}$$

is an isomorphism $\mathbb{F} \to \hat{\mathbb{F}}$ for all non-trivial pth roots of unity ω. There is no loss of generality in choosing $\omega = e^{i \frac{2\pi}{p}}$.

If $\mathbb{F}_d$ is an extension of $\mathbb{F}_p$, then

$$b \mapsto \chi_b(\cdot) := \chi_{\mathbb{F}_p}(\mathrm{Tr}\, b \cdot) \tag{9}$$

is an isomorphism for all non-trivial characters $\chi_{\mathbb{F}_p}$ of the base field.

The maps presented in the last two paragraphs are certainly group homomorphisms. The fact that they are bijective (and thus isomorphisms) can be proven by a simple counting argument, making use of the fact that the additive structure of finite fields is abelian and thus isomorphic to its dual.

3.2.2 Computer Implementation

The following definitions of characters for finite fields are taken from the package **heisenberg.m**.

```
In[14]:= ω := N[Exp[I 2π/p]]
```

```
In[15]:= χ[x_?FieldOrNumericQ] := ω^Tr[x]
```

```
In[16]:= χ[x_?FieldOrNumericQ, y_?FieldOrNumericQ] := ω^Tr[x y]
```

The arguments to **χ** can either be elements of the finite field **F** or integers.

```
In[17]:= << heisenberg.m
```

```
In[18]:= qInit[1, 3]
```

```
In[19]:= χ[2]
Out[19]= -0.5 - 0.866025 i
```

```
In[20]:= χ[F[{2}], 2]
Out[20]= -0.5 + 0.866025 i
```

3.3 Finite Symplectic Geometry

We repeat some facts from the theory of finite vector spaces with a symplectic form. The standard reference of this section is Ref. [2].

A finite vector space V is called *symplectic* if it possesses a non-degenerate bilinear form $[\cdot,\cdot]$ which is anti-symmetric

$$[v, w] = -[w, v]. \tag{10}$$

Should V be defined over a field of characteristic two, then we additionally demand the form fulfills

$$[v, v] = 0. \tag{11}$$

Given a subspace M of V, the *symplectic complement* $M^\perp$ is the set of all $v \in V$ such that $[v, m] = 0$ for all $m \in M$. M is said to be *isotropic*, if the form vanishes on M, that is if $[m_1, m_2] = 0$ for all $m_1, m_2 \in M$.

The following assertions hold.

1. Any finite symplectic vector space is even-dimensional.

2. For any subspace M of V, $M^\perp$ is a subspace of V. Further,

$$\dim M + \dim M^\perp = \dim V. \tag{12}$$

3. There always exists a basis $\{p_1, \cdots, p_n, q^1, \cdots, q^n\}$ of V such that

$$\begin{aligned} [p_i, p_j] &= 0 \\ [q^i, q^j] &= 0 \\ [p_i, q^j] &= \delta_i^j. \end{aligned} \tag{13}$$

   A set of that kind is called a *symplectic basis*. The tuples $\langle p_i, q^i \rangle$ are *hyperbolic pairs*.

4. If M is isotropic then $M \subset M^\perp$. The maximum dimension of an isotropic space is $(\dim V)/2$. A space that reaches this limit is *maximal isotropic*. M is *maximal isotropic* if and only if $M^\perp = M$.

Symplectic vector spaces will subsequently be referred to as *phase spaces*. We reserve the letter V to stand for phase spaces.

3.4 Fourier Transformation and Convolution

Let G be a finite abelian group and let $L^1(G)$ denote the set of all complex valued functions on G. Then the Fourier operator on G is defined via

$$\begin{aligned} \mathcal{F} : L^1(G) &\rightarrow L^1(\hat{G}) \\ \hat{f}(\chi) &:= (\mathcal{F}f)(\chi) = \frac{1}{\sqrt{d}} \sum_{t \in G} f(t) \overline{\langle \chi | t \rangle}. \end{aligned} \tag{14}$$

The inverse is

$$\left(\mathcal{F}^{-1} \hat{f} \right)(t) = \frac{1}{\sqrt{d}} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \langle t | \chi \rangle \tag{15}$$

Using Eq. (7), it can easily be seen that $\mathcal{F} \circ \mathcal{F}^{-1} = \mathbb{1}$.

There are several mathematical structures that can naturally be associated to the set $L^1(G)$ [15]. Obviously, pointwise addition and scalar multiplication turn it into a vector space, while pointwise multiplication of functions makes it an algebra. There is a second natural possibility to define an algebra structure on $L^1(G)$, namely by using *convolution*. For two functions f, g on G, we define their convolution as

$$(f * g)(t) = \sum_{s \in G} f(s) g(ts^{-1}). \tag{16}$$

The same structure is of course present on $\hat{G}$.

The choice of coefficients in the above definition of the Fourier transformation is such that the transformation becomes an *isometry*. Indeed, define the norm of a function $f \in L^1(G)$ to be

$$||f||^2 := \sum_{g \in G} |f(g)|^2 \tag{17}$$

and similarly for functions on $\hat{G}$, then $||f|| = ||\hat{f}||$ (this relation is sometimes called the *Parseval formula*).

There would have been a different natural possibility to choose the pre-factors in Eq. (14). Indeed, it is easily checked that

$$\mathcal{F}(fg) = \frac{1}{\sqrt{d}} \mathcal{F}(f) * \mathcal{F}(g) \tag{18}$$

and thus $\mathcal{F}$ maps the product algebra of $L^1(G)$ to the convolution algebra of $L^1(\hat{G})$ *modulo* a factor of $\sqrt{d}$. In Ref. [13] it is noted that in the definition of the Fourier transform for functions on $\mathbb{R}^n$ pre-factors can be choosen in a way that makes $\mathcal{F}$ simultaneously an isometry and an algebra homomorphism. However, in the finite setting there seems to be no elegant means for that. In this document, we opted for preserving the isometry-property at the price of some factors in all formulas that make use of convolution.

The relation (18) is illustrated in the following diagram. We will frequently make use of such graphic representations in vague resemblance of *commutative diagrams* from category theory. Owing to a bad physicists' habit, we label the vertices not by objects or sets, but with 'representative' elements, such as $\hat{f}$ instead of $L^1(\hat{G})$.

$$\begin{tikzcd}
f, g \arrow[r, "\mathcal{F}"] \arrow[d, "\cdot"'] & \hat{f}, \hat{g} \arrow[d, "\frac{1}{\sqrt{d}}*"] \\
f \cdot g \arrow[r, "\mathcal{F}"] & \hat{f} * \hat{g} \frac{1}{\sqrt{d}}
\end{tikzcd}$$

If $w : G \to U(\mathcal{H})$ is a unitary representation of G, then w induces a representation of the convolution algebra $L^1(G)$ (see Ref. [15]) by setting, for all $f \in L^1(G)$,

$$w(f) := \sum_{a \in G} f(a) w(a). \tag{19}$$

Indeed, let $f, g \in L^1(G)$, then

$$\begin{aligned}
w(f * g) &= \sum_{a \in G} \left(\sum_{b \in G} f(ab^{-1}) g(b) \right) w(a) &(20)\\
&= \sum_{b} \sum_{x = ab^{-1}} f(x) g(b) w(xb)\\
&= \left(\sum_{x} f(x) w(x) \right) \left(\sum_{b} g(b) w(b) \right)\\
&= w(f) w(g).
\end{aligned}$$

As a last remark, making use of the isomorphism (8), we we can write the Fourier transform of an $f \in L^1(\mathbb{F})$ as a function on $\mathbb{F}$ itself once a faithful character χ of $\mathbb{F}$ has been fixed:

$$\hat{f}(a) := \hat{f}(\chi_a) = \frac{1}{\sqrt{d}} \sum_{b \in \mathbb{F}} \langle \chi | ab \rangle^* f(b). \tag{21}$$

3.4.1 Symplectic Fourier Transformation

Consider a symplectic vector space V over a finite field $\mathbb{F}$. Suppose a character χ of $\mathbb{F}$ has been chosen. χ immediately induces an isomorphism from V to $\hat{V}$ via

$$\chi_a(\cdot) \quad := \quad \chi([a, \cdot]) \tag{22}$$

for $a \in V$. Making use of the above relation, we can define a Fourier transformation for functions on V, which we will refer to as *symplectic Fourier transformation*. Specifically, for a vector space V of dimension $2n$ over a field $\mathbb{F}$ of order d, we set

$$\begin{aligned}
(\tilde{\mathcal{F}} F)(a) &:= \tilde{F}(a) &(23)\\
&:= \frac{1}{d^n} \sum_{b \in V} \langle \chi_a | b \rangle^* F(b)\\
&= \frac{1}{d^n} \sum_{b \in V} \chi([a, b])^* F(b).
\end{aligned}$$

The symplectic Fourier transformation is covariant under the action of the *Symplectic Group* $\mathrm{Sp}(\mathbb{F}^{2n})$:

$$\begin{aligned} \tilde{\mathcal{F}}(F \circ S)(a) &= \frac{1}{d^n} \sum_{b \in V} \chi([a,b])^* F(Sb) \qquad (24) \\ &= \frac{1}{d^n} \sum_{b \in V} \chi([a, S^{-1}b])^* F(b) \\ &= \frac{1}{d^n} \sum_{b \in V} \chi([Sa, SS^{-1}b])^* F(b) \\ &= \frac{1}{d^n} \sum_{b \in V} \chi([Sa, b])^* F(b) \\ &= \tilde{\mathcal{F}}(F)(Sa). \end{aligned}$$

It comes as no surprise, that multiplying a phase space function by a character corresponds to shifting its symplectic Fourier transform

$$\begin{aligned} \tilde{\mathcal{F}}(\chi([v,\cdot])F)(a) &= \frac{1}{d^n} \sum_{b \in V} \chi([a,b])^* \chi([v,b]) F(b) \\ &= \frac{1}{d^n} \sum_{b \in V} \chi([a-v,b])^* F(b) \\ &= (\tilde{\mathcal{F}}F)(a-v). \end{aligned}$$

Lastly, the symplectic Fourier transform is self-inverse

$$\tilde{\mathcal{F}} \circ \tilde{\mathcal{F}} = \mathbb{1} \qquad (25)$$

as can been seen as follows:

$$\begin{aligned} \tilde{\mathcal{F}}(\tilde{\mathcal{F}}F)(a) &= \frac{1}{d^{2n}} \sum_{b \in V} \chi([a,b])^* \sum_{c \in V} \chi([b,c])^* F(c) \qquad (26) \\ &= \frac{1}{d^{2n}} \sum_{c,b} \chi([a,b])^* \chi([c,b])^* F(c) \\ &= \frac{1}{d^{2n}} \sum_{c} d^{2n} \delta_{c,a} F(c) \\ &= F(a). \end{aligned}$$

3.4.2 Computer Implementation

The definition of the symplectic Fourier transformation from **heisenberg.m** reads

```
In[21]:= SFT[f_][P_,Q_] :=
           1
           -FSum[Conjugate@χ[P #2 - Q #1] f[#1,#2] &,2]
           d
```

It is a *functional*, that is, the argument **f** must be an *pure function* in the terminology of *Mathematica*. More precisely, **f** must be a phase space function, meaning: it must take two arguments from the finite field **F**. It can return an object of any type for which addition and scalar multiplication is defined. In the next example, **f** will return real numbers, but later on we will encouter an example of a Fourier transform of an operator valued functional.

```
In[22]:= <<heisenberg.m
```

The function **qInit[]** will be documented later.

```
In[23]:= qInit[1,3]
```

```
In[24]:= f = tec[#1] + tec[#2] &;
```

Our sample **f** converts its arguments to real numbers using **tec[]** from the package **finiteFields.m** and adds them together.

```
In[25]:= f[F[{1}],F[{2}]]
Out[25]= 3
```

We will often be concerned with pure functions on phase space (similar to **f**). Sometimes it is convenient to look at all their values at once. The function **f2a[]**, defined in **finiteFields.m**, converts a pure phase space function into an array.

```
In[26]:= f2a[f] //MatrixForm
         ⎛0  1  2⎞
Out[26]= ⎜1  2  3⎟
         ⎝2  3  4⎠
```

For the sake of completeness, here is the converse, **a2f[]**:

```
In[27]:= a2f[f2a[f]] [F[{1}],F[{2}]]
Out[27]= 3
```

It is time to see how **SFT** actually works:

```
In[28]:= SFT[f][0,0]
Out[28]= 6
```

Alternatively, in the spirit of what has been said before, we can look at all values of **SFT[f]** at once.

```
In[29]:= f2a[SFT[f][#1,#2] &] //MatrixForm
         ⎛        6            -1.5 - 0.866025 i   -1.5 + 0.866025 i ⎞
Out[29]= ⎜-1.5 + 0.866025 i           0                    0         ⎟
         ⎝-1.5 - 0.866025 i           0                    0         ⎠
```

4 The Heisenberg Group

4.1 Motivation

If a quantum system possesses a symmetry, then there should exist a unitary, irreducible, possibly projective representation of the symmetry group (see for example Ref. [11]). Probably the best-known example is the Galilei symmetry, that is the translational and boost invariance of a single free quantized mass point moving in $\mathbb{R}^n$. The associated classical symmetry group is of course $\mathbb{R}^{2n}$. The unitary irreducible projective representation of $\mathbb{R}^{2n}$ is given by the famous *Weyl representation* specified by the *canonical commutation relations*. Instead of seeing the Weyl representation as a projective representation of $\mathbb{R}^{2n}$, we can perceive the group generated by the operators of the Weyl representation as an abstract group of its own. The group obtained this way is commonly called the *Heisenberg group* and will be defined in this paragraph.

4.2 Definition

Let $\mathbb{F}$ be a field not of characteristic two. We define the *Heisenberg group* $H(\mathbb{F})$ abstractly by its composition law

$$\begin{aligned} & (p_1, q_1, t_1)(p_2, q_2, t_2) \\ = \; & (p_1 + p_2, q_1 + q_2, t_1 + t_2 + 2^{-1} \left[\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}, \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \right]) \end{aligned} \tag{27}$$

where p_i, q_i and t_i are elements of $\mathbb{F}$ and $[\cdot, \cdot]$ denotes the *standard symplectic inner product* on the vector space $\mathbb{F}^2$:

$$\begin{aligned} & \left[\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}, \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \right] \\ := \; & \begin{pmatrix} p_1 \\ q_1 \end{pmatrix}^T \mathcal{J} \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \\ \mathcal{J} \; := \; & \mathcal{J}_{\mathbb{F}^2} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \end{aligned} \tag{28}$$

In a physical context the *commutation relation* corresponding to the composition law (27) is often of interest. It is given by

$$\begin{aligned} & (p_1, q_1, t_1)(p_2, q_2, t_2) \\ = \; & (p_2, q_2, t_2)(p_1, q_1, t_1)(0, 0, \left[\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}, \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \right]). \end{aligned} \tag{29}$$

The Heisenberg group enters the quantum scene through the *Weyl representation* which maps the group to operators on the Hilbert space $\mathbb{C}^d$, where d is the order of $\mathbb{F}$. The representation is constructed as follows. Fix a character χ of $\mathbb{F}$, choose a basis $\{|\phi_1\rangle, \cdots, |\phi_d\rangle\}$ in $\mathcal{H}$. Define the *shift* and *clock* operators as

$$\begin{aligned} x(q) : |\phi_k\rangle & \mapsto |\phi_{k+q}\rangle \\ z(p) : |\phi_k\rangle & \mapsto \chi(pk)|\phi_k\rangle \end{aligned} \tag{30}$$

for all $k = 1 \cdots d$. Then the Weyl representation is

$$w(p,q,t) := \chi\left(t - 2^{-1}pq\right) z(p)x(q). \tag{31}$$

We call the image of w the set of *Weyl operators*. It is easy to see from (27) that two Weyl operators $w(p_1, q_1, t_2)$ and $w(p_2, q_2, t_2)$ commute if the symplectic inner product

$$\left[\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}, \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \right] \tag{32}$$

vanishes. The converse is true if the character χ is faithful (which is always the case if χ is non-trivial and $\mathbb{F}$ has prime order, but it can never be fulfilled for extension fields; see Section 7.6).

The definition of the Heisenberg group extends naturally to finite vector spaces $\mathbb{F}^n$. Indeed, if we define

$$\mathcal{J}_{\mathbb{F}^{2n}} = \bigoplus_{i=1}^{n} \mathcal{J}_{\mathbb{F}^2} \tag{33}$$

then the definition (27) makes sense if p_i and q_i are elements of $\mathbb{F}^n$. We denote the group defined this way by $H^n(\mathbb{F})$. The Weyl representation of $H^n(\mathbb{F})$ is defined as

$$(p,q,t) \mapsto \chi(t) w(p_1, q_1) \otimes \cdots \otimes w(p_n, q_n) \tag{34}$$

where $\{p_i\}, \{q_i\}$ are the components of p and q with respect to the natural basis in $\mathbb{F}^n$.

It is customary to choose coordinates in the symplectic vector space $\mathbb{F}^{2n}$ by mapping $(p_1, q_1)^T \oplus \cdots \oplus (p_n, q_n)^T$ to $(p_1, \cdots, p_n, q_1, \cdots, q_n)^T$. We call this convention *function coordinates*, as the primary sorting criterion for the coordinates is their *function* ($i.e.$ 'momentum' or 'position'). In contrast, when one is interested in questions concerning locality, it turns out to be advantageous to sort the coordinates first according to the *system* they act on. Thus, in this thesis we will write $(p_1, q_1, p_2, q_2, \cdots, p_n, q_n)^T$ for the direct sum mentioned above and refer to this notation as *system coordinates*. For example, in system coordinates, the symplectic matrix $\mathcal{J}$ takes on the form

$$\begin{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & & & \\ & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & & \\ & & \ddots & \\ & & & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{pmatrix}. \tag{35}$$

For future reference, we given the action of a Weyl operator on a state vector in coordinates. Let $|\psi\rangle$ be a state vector in $\mathcal{H}$ with expansion coefficients $\langle x|\psi\rangle =: \psi(x)$. Then

$$\left(w(p,q,t)\psi\right)(x) \quad = \quad \chi(t + px - 2^{-1}pq)\psi(x-q). \tag{36}$$

4.3 The Qbit Case

For fields of characteristic two, the definition (27) cannot be applied, as the symbol 2^{-1} has no meaning in this case. However, there still exists a projective representation of $\mathbb{F}_2$ defined in an analogous way. Specifically, we set

$$w(p,q) := i^{-pq} z(p) x(q) \tag{37}$$

for $p, q \in \mathbb{F}_2$ and extend this definition to multiple systems as in Eq. (34). The crucial difference to Eq. (31) lies in the fact that i is a 4th root of unity, as opposed to a 2nd. The group generated by $\{w(p,q)\}_{p,q}$ is called the *Pauli group*. We will also refer to it as the Heisenberg group for qbits, even though it does not fulfill the defining composition law (27). There is a formal analogy leading from Eq. (31) to Eq. (37). Namely, if the character χ equals $\chi(\cdot) = e^{\frac{2\pi}{d}\cdot}$ then the non-binary Weyl representation reads

$$w(p,q) = e^{-\frac{2\pi}{d}2^{-1}pq} z(p) x(q) \tag{38}$$

and Eq. (37) follows by replacing 2^{-1} by $\frac{1}{2}$, which is the inverse of 2 in $\mathbb{R}$ as opposed to $\mathbb{F}$.

The composition law for two binary Weyl operators can be checked to be

$$\begin{aligned} w(p_1,q_1)w(p_2,q_2) &= w(p_1+p_2, q_1+q_2) \\ &\quad i^{p_1 q_2 - p_2 q_1} \\ &\quad i^{(p_1+p_2)(q_1+q_2) \mod 4} \\ &\quad i^{-(p_1+p_2)(q_1+q_2) \mod 2} \end{aligned} \tag{39}$$

which reduces for single systems ($n = 1$) to

$$\begin{aligned} w(p_1,q_1)w(p_2,q_2) &= w(p_1+p_2, q_1+q_2) \\ &\quad i^{p_1 q_2 - p_2 q_1} \\ &\quad (-1)^{p_1 q_1 q_2 + p_2 q_1 q_2 + p_1 p_2 q_1 + p_2 p_2 q_1}. \end{aligned} \tag{40}$$

Technically speaking, the Heisenberg group for qbits is an extension of $\mathbb{Z}_4$ by $\mathbb{F}_2^{2n}$, while the non-binary Heisenberg group extends $\mathbb{F}_d$ by $\mathbb{F}_d^{2n}$.

For future use we define a variant of (37) (compare to Ref. [20]):

$$\begin{aligned} \tau(p,q) &:= z(p)x(q) \\ &= i^{pq} w(p,q). \end{aligned} \tag{41}$$

4.4 Computer Implementation

```
In[30]:= << head.m

         << qmatrixHead.m

         << heisenberg.m
```

```
package qmatrix, version 2.2.1
(C) Timo Felbinger (timo@felbinger.net), 1999, 2000, 2001
last modified : 20010430.210546utc by : timof@amadeus
This package is free software and you are welcome to
redistribute it; type qmatrix'license for the details.
Type qmatrix'help to get help on this package.
```

Before we turn to the describtion of the Weyl representation defined in the package **heisenberg.m**, let us briefly take a look at the general framework of the packages. The system presented here builds on Timo Felbinger's **qmatrix** package [16]. It is not loaded directly, but instead via the wrapper **qmatrixHead.m** which defines some additional functionality.

After the packages have been loaded, every notebook should start with a call to the function **qInit[]**. It initializes the **qmatrix** package to suit our needs. The first argument specifies how many systems to work with, the second argument gives the dimension of their respective Hilbert space.

```
In[31]:= qInit[2,3]
```

The subsystems are labled **q1** to **qn**.

```
In[32]:= system
Out[32]= {{q1,q2}}
```

However, in order to facilitate writting functions that address different systems automatically, the names of the systems can be entered as **q** with the number of the system given as a subscript.

```
In[33]:= q₁
Out[33]= q1
```

Among other useful functions, the package **qmatrixHead.m** defines the function **toAbstract[]** which gives a more readable output for state vectors and operators in terms of the computational basis.

```
In[34]:= matrix[{1,0,I},{ket[q1]}] //toAbstract
Out[34]= |0 > +i |2 >
```

We go on to introduce the implementation of the Weyl representation.

The *shift operator* **X** takes two arguments. First the number of the system it acts on and second the field element specifiying the shift.

```
In[35]:= X[1,F[{1}]]
          ⎛0.  0.  1. ⎞
Out[35]=  ⎜1.  0.  0. ⎟
          ⎝0.  1.  0. ⎠
         {ket[q1],bra[q1]}
```

Alternatively, we can specify the shift by an integer which will be converted to a field element using the **enf[]** function from **finiteFields.m**.

```
In[36]:= X[1,1]
          ⎛0.  0.  1. ⎞
Out[36]=  ⎜1.  0.  0. ⎟
          ⎝0.  1.  0. ⎠
         {ket[q1],bra[q1]}
```

The *clock* operators and, finally, the Weyl operators are defined in the same fashion.

```
In[37]:= Z[1,1]
          ⎛1.        0.                 0.          ⎞
Out[37]=  ⎜0.  -0.5 + 0.866025 i        0.          ⎟
          ⎝0.        0.         -0.5 - 0.866025 i   ⎠
         {ket[q1],bra[q1]}
```

```
In[38]:= W[1,1,1]
                0.         0.   -0.5 + 0.866025 i
Out[38]= -0.5 - 0.866025 i  0.         0.
                0.         1.         0.
         {ket[q1],bra[q1]}
```

The next step is to look at *two* systems.

```
In[39]:= qInit[2,3]
```

If two **`List[]`**s are passed to **`W`**, then the first list will be interpreted as the momentum coordinates and the second list as the position coordinates. This agrees with the convention of *function coordinates*.

```
In[40]:= W[{0,0},{1,2}]
         0.  0.  0.  0.  0.  0.  0.  1.  0.
         0.  0.  0.  0.  0.  0.  0.  0.  1.
         0.  0.  0.  0.  0.  0.  1.  0.  0.
         0.  1.  0.  0.  0.  0.  0.  0.  0.
Out[40]= 0.  0.  1.  0.  0.  0.  0.  0.  0.
         1.  0.  0.  0.  0.  0.  0.  0.  0.
         0.  0.  0.  0.  1.  0.  0.  0.  0.
         0.  0.  0.  0.  0.  1.  0.  0.  0.
         0.  0.  0.  1.  0.  0.  0.  0.  0.
         {ket[q1],ket[q2],bra[q1],bra[q2]}
```

Alternatively, if the argument is a single **`List[]`**, then it will be treated as specifying *system coordinates.*

```
In[41]:= W[{0,1,0,2}]
         0.  0.  0.  0.  0.  0.  0.  1.  0.
         0.  0.  0.  0.  0.  0.  0.  0.  1.
         0.  0.  0.  0.  0.  0.  1.  0.  0.
         0.  1.  0.  0.  0.  0.  0.  0.  0.
Out[41]= 0.  0.  1.  0.  0.  0.  0.  0.  0.
         1.  0.  0.  0.  0.  0.  0.  0.  0.
         0.  0.  0.  0.  1.  0.  0.  0.  0.
         0.  0.  0.  0.  0.  1.  0.  0.  0.
         0.  0.  0.  1.  0.  0.  0.  0.  0.
         {ket[q1],ket[q2],bra[q1],bra[q2]}
```

Let us test the implementation using two random vectors.

```
In[42]:= m1 = Table[Random[Integer, d],{i,2n}]

         m2 = Table[Random[Integer, d],{i,2n}]
Out[42]= {1,3,3,2}
Out[42]= {1,3,1,2}
```

Their symplectic inner product can be computed as

```
In[43]:= symp[m1,m2]
Out[43]= 4
```

Therefore, the following line tests whether the Weyl operators fulfill the composition law of the Heisenberg group.

```
In[44]:= W[m1] * *W[m2] == χ[inv symp[m1,m2]] W[m1 + m2]
Out[44]= True
```

The second argument tells **qInit** which field to use. If it is an integer **p**, the package assumes that **p** is a prime and uses the field **GF[p]** (see the *Mathematica* documentation). Else, one can supply a list **{p, r}**. In that case, the extension field **GF[{p, r}]** is used.

```
In[45]:= qInit[2,{3,2}]

In[46]:= F
Out[46]= GF[3,{2,1,1}]

In[47]:= X[1,1]
         ⎛0.  0.  1.  0.  0.  0.  0.  0.  0. ⎞
         ⎜1.  0.  0.  0.  0.  0.  0.  0.  0. ⎟
         ⎜0.  1.  0.  0.  0.  0.  0.  0.  0. ⎟
         ⎜0.  0.  0.  0.  0.  1.  0.  0.  0. ⎟
Out[47]= ⎜0.  0.  0.  1.  0.  0.  0.  0.  0. ⎟
         ⎜0.  0.  0.  0.  1.  0.  0.  0.  0. ⎟
         ⎜0.  0.  0.  0.  0.  0.  0.  0.  1. ⎟
         ⎜0.  0.  0.  0.  0.  0.  1.  0.  0. ⎟
         ⎝0.  0.  0.  0.  0.  0.  0.  1.  0. ⎠
         {ket[q1],bra[q1]}
```

In order to increase the performance, the Weyl operators are *cached*. That means, the first call to **W[]** computes the matrix and stores the result for subsequent use. Therefore, if one works in large dimensions, the first call to **W[]** might take notablely longer then later ones.

```
In[48]:= qInit[2,13]

In[49]:= Timing[W[{1,1},{1,1}];]
Out[49]= {0.18 Second,Null}

In[50]:= Timing[W[{1,1},{1,1}];]
Out[50]= {0.06 Second,Null}
```

4.5 The Role of the Symplectic Group

This section is devoted to the study of the automorphisms of the Heisenberg group. In the following, we write elements of $H^n(\mathbb{F})$ as (a, t) for $a \in V$.

Lemma 1 *Let α be an automorphism of $H^n(\mathbb{F})$ for some finite field $\mathbb{F}$. Then α is of the form*

$$\alpha(a, t) = (A(a), T(a, t))$$

for two functions $A : \mathbb{F} \to \mathbb{F}$ and $T : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$. Further, A and T are compatible with addition in $\mathbb{F}$, that is,

$$\begin{aligned} A(a+b) &= A(a) + B(a) \\ T(a+b, t) &= T(a,t) + T(b,t) \\ T(a, s+t) &= T(a,s) + T(a,t). \end{aligned}$$

Proof. First, note that any automorphism maps the center of a group to the center. The center $Z(H^n(\mathbb{F}))$ of the Heisenberg group is the set

$$\{(0,t)\}_{t\in\mathbb{F}}$$

as can be seen easily from Eq. (27). Thus

$$\alpha(0,t) = (0, T(0,t)).$$

It is obvious that functions A and T exist such that

$$\alpha(a,t) = (A(a,t), T(a,t)).$$

But, using the remarks above, we find that

$$\begin{aligned}
(A(a,t), T(a,t)) &= \alpha(a,t) \\
&= \alpha\left((a,0)\circ(0,t)\right) \\
&= \alpha\left((a,0)\right)\circ\alpha\left((0,t)\right) \\
&= (A(a,0), T(a,0))\circ(0, T(0,t)) \\
&= (A(a,0), T(a,0)+T(0,t))
\end{aligned}$$

which shows that

$$A(a,t) = A(a,0)$$

proving the first claim of the lemma. To see that the second assertion holds, write

$$\begin{aligned}
\alpha\left((a,0)\circ(b,0)\right) &= (A(a), t_1)\circ(A(b), t_2) \\
&= (A(a)+A(b), t_3)
\end{aligned}$$

where the t_i are some unimportant phases. Simultaneously, it is true that

$$\begin{aligned}
\alpha\left((a,0)\circ(b,0)\right) &= \alpha(a+b, t_4) \\
&= (A(a+b), t_5).
\end{aligned}$$

Comparing the last lines of the preceding two formulas, one sees that

$$A(a+b) = A(a) + A(b).$$

Turning to T, we already know that $T(a,b) = T(a,0) + T(0,b)$ so it suffices to show the compatibility of $T(\cdot,0)$ and $T(0,\cdot)$ with addition in $\mathbb{F}$, which is done along similar lines as for A. □

Note that $A(a+b) = A(a) + A(b)$ is in general not sufficient to conclude that A is $\mathbb{F}$-linear, because A might fail to be compatible with *scalar multiplication* by elements λ of $\mathbb{F}: A(\lambda a) \neq \lambda A(a)$. However, if the field $\mathbb{F}$ is *cyclic*, that is, if every element λ can be written as

$$\lambda = 1 + \cdots + 1 \tag{42}$$

then

$$\begin{aligned}
A(\lambda a) &= A((1+\cdots+1)a) \qquad (43)\\
&= A(a+\cdots+a) \\
&= A(a)+\cdots+A(a) \\
&= \lambda A(a)
\end{aligned}$$

and linearity of A follows. By Remark 5 in Section 3.1, a field is cyclic if and only if it is of prime order. For the sake of simplicity, we will now restrict our attention to cyclic fields. We'll comment on the general case in Section 7.6.

There are a couple of automorphism groups of $H^n(\mathbb{F})$ which can be identified by inspection. We list three of them, slightly adapting an enumeration from Ref. [13] to the finite case.

1. Let $S \in \mathrm{Sp}(V)$ be a *symplectic map*. Then

   $$(a,t) \mapsto (Sa,t) \tag{44}$$

   is an automorphism of H. Denote the group of all automorphisms of this form by G_1.

2. G_2 denotes the *inner morphism* that is, mappings of the form

   $$(a,t) \cdot (a,t)^{-1}. \tag{45}$$

3. The group of *dilations* $\delta(r), r \in \mathbb{F}^\sharp$ with composition law $\delta(r)\delta(s) = \delta(rs)$ is defined to act on $H^n(\mathbb{F})$ by

   $$\delta(r)(a,t) = (a,rt). \tag{46}$$

   $\mathbb{F}^\sharp$ is the set of non-zero elements in $\mathbb{F}$. Dilations can be checked to be automorphisms and are jointly denoted by G_3.

Theorem 2 ([13]) *Any automorphism α of $H^n(\mathbb{F})$, for cyclic $\mathbb{F}$, can be written as*

$$\alpha = \alpha_1\alpha_2\alpha_3$$

where $\alpha_i \in G_i$.

Proof. Using Lemma 1 the proof of Theorem 1.22 in Ref. [13] can easily be adapted to the finite case. □

It is now natural to ask which of the automorphisms can be represented by the action of unitaries on the Weyl representation. That is, for which subset of the automorphism group exist unitary operators $U(\alpha)$ such that

$$Uw(a,t)U^\dagger = w \circ \alpha(a,t) \tag{47}$$

or, weaker, if we allow for a 'projective action', for which α can

$$Uw(a,t)U^\dagger = e^{i\phi_a} w \circ \alpha(a,t) \tag{48}$$

be fulfilled?

Firstly, since the center of the Heisenberg group is mapped to multiples of the identity operator

$$w(0,t) = \chi(t)\mathbb{1} \tag{49}$$

the center must be pointwise invariant under the action of unitaries by conjugation. It follows that G_3 cannot be implemented within the framework of the Weyl representation.[2] Hence, all admissible αs must be elements of $G_1 G_2$. Now, G_2, has an obvious operator representation: the conjugation by elements of H^n corresponds of course to conjugation by Weyl operators. The case of G_1 is not as easily decided. In the case $\mathbb{F} = \mathbb{R}$, the statement that all symplectic mappings have an operator representation acting on the Weyl group is the famous Stone-von Neumann-Theorem. For finite $\mathbb{F}$ explicit constructions for a mapping $\mu : \mathrm{Sp}(V) \to U(\mathcal{H})$ are known such that

$$\mu(S) w(a,t) \mu(S)^\dagger = e^{i\phi_a} w(Sa,t). \tag{50}$$

Refer to Ref. [12] for the case of odd characteristic and to Ref. [20] for fields of characteristic two. The mapping μ which turns out to be a projective representation[3] of Sp is sometimes called the *metaplectic representation*.

For the rest of the Section we will pursue the question of what can be said about the phases $e^{i\phi_a}$ that appear in Eq. (48).

The composition law of the Weyl representation is of the form

$$w(a)w(b) = f(a,b) w(a+b) \tag{51}$$

for $a, b \in \mathbb{F}$ and a function $f : \mathbb{F} \times \mathbb{F} \to \mathbb{C}$. In the language of group extension theory, the function f is a *factor system*. The explicit form of f is given by the formulas (27) and (39) for non-binary and binary systems respectively.

Now let U be any unitary operator that maps Weyl operators to multiples of Weyl operators under conjugation:

$$U w(a,t) U^\dagger = e^{i\phi_a} w(Sa). \tag{52}$$

In the context of quantum information theory, such operators are called *Clifford operations*. Because conjugation by unitary operators preserves the multiplicative structure, S must be an automorphism of the Heisenberg group. Because it fixes the center, S is symplectic by Theorem 2.

Define $c(a) := e^{i\phi_a}$. We have on the one hand

$$\begin{aligned} U w(a) U^\dagger U w(b) U^\dagger &= w(Sa) w(Sb) c(a) c(b) \\ &= f(Sa, Sb) w(S(a+b)) c(a) c(b) \end{aligned} \tag{53}$$

and on the other hand

$$\begin{aligned} U w(a) U^\dagger U w(b) U^\dagger &= U w(a) w(b) U^\dagger \\ &= f(a,b) U w(a+b) U^\dagger \\ &= f(a,b) w(S(a+b)) c(a+b), \end{aligned} \tag{54}$$

which together yields

$$\frac{f(Sa,Sb)}{f(a,b)} = \frac{c(a+b)}{c(a)c(b)}. \tag{55}$$

[2] However, if one allows for *anti-unitary* operators, then $\delta(-1)$ can be represented [34].

[3] In the case of finite fields of odd order, μ can be chosen to be a non-projective representation [12]. This fact will however not play a role in this document.

For every symplectic mapping S, the condition (55) determines c modulo a character of V. Indeed, let U and V be unitaries such that

$$\begin{aligned} Uw(a)U^\dagger &= c_U(a)w(Sa) \\ Vw(a)V^\dagger &= c_V(a)w(Sa). \end{aligned} \tag{56}$$

Define a 'difference function' δ by $c_V(\cdot) =: c_U(\cdot)\delta(\cdot)$, then

$$\begin{aligned} & \frac{c_V(a+b)}{c_V(a)c_V(b)} = \frac{f(Sa,Sb)}{f(a,b)} = \frac{c_U(a+b)}{c_U(a)c_U(b)}. \\ \Rightarrow \quad & \frac{c_V(a+b)}{c_V(a)c_V(b)} = \frac{c_V(a+b)\delta(a+b)}{c_V(a)c_V(b)\delta(a)\delta(b)} \\ \Leftrightarrow \quad & \frac{\delta(a+b)}{\delta(a)\delta(b)} = 1. \end{aligned} \tag{57}$$

Looking again at Eq. (55) we see that the phases c deviate from being a character of V if and only if the factor set f fails to be invariant under symplectic operations.

If $\mathbb{F}$ is not of characteristic two, then

$$f(a,b) = \chi(-2^{-1}[a,b]) \tag{58}$$

and thus $f(a,b) = f(Sa,Sb)$ because S is symplectic. We conclude that c must be a character of V. But then there is a vector $v \in V$ such that

$$c(\cdot) = \chi([v,\cdot]). \tag{59}$$

Define $V := Uw(-v)$. It holds that

$$\begin{aligned} Vw(a)V^\dagger &= Uw(-v)w(a)w(-v)^\dagger U^\dagger \\ &= c(a)^* Uw(a)U^\dagger \\ &= w(Sa) \end{aligned} \tag{60}$$

for all $a \in V$. We conclude that the mapping $\mu : \mathrm{Sp}(V) \to U(\mathcal{H})$ can be chosen such that Eq. (47) is fulfilled, that is, no phase factors c appear. The discussion of the unitary automorphisms of the Weyl operators for non-binary systems will be continued in Section 7.2.

For qbits however, the factor system cleary fails to be invariant under the action of symplectic mappings S as can be seen from Eq. (39). All that can easily be established about the phases $c(\cdot)$ is that they must be real, for binary Weyl opeators are hermitian and conjugation by unitary operators preserves hermiticity. So, by use of Eq. (55) we have in general

$$\frac{c(a+b)}{c(a)c(b)} = \pm 1. \tag{61}$$

There is thus no canonic way of choosing $\mu(S)$ as was the case for non-binary systems, where a specific representation $\mu(S)$ was singled out by the property that it allowed for a trivial $c(\cdot)$.

4.5.1 Computer Implementation

```
In[51]:= << head.m

         << qmatrixHead.m

         << heisenberg.m

  package qmatrix, version 2.2.1
  (C) Timo Felbinger (timo@felbinger.net), 1999, 2000, 2001
  last modified : 20010430.210546utc by : timof@amadeus
  This package is free software and you are welcome to
  redistribute it; type qmatrix'license for the details.
  Type qmatrix'help to get help on this package.

In[52]:= qInit[1,3]
```

Define any symplectic **2x2**-matrix.

```
In[53]:= (S = {{2,1},{1,1}}) //MatrixForm
Out[53]= (2  1 )
         (1  1 )
```

mu[] returns the metaplectic representation of its argument. However, it works only for single systems. It is based on a formula by Vourdas.

```
In[54]:= B = μ[S]
         ( 0. - 0.57735 i     -0.5 + 0.288675 i   -0.5 + 0.288675 i )
Out[54]= (0.5 + 0.288675 i   -0.5 + 0.288675 i    0.5 + 0.288675 i )
         (0.5 + 0.288675 i    0.5 + 0.288675 i   -0.5 + 0.288675 i )
         {ket[q1],bra[q1]}
```

Test the representation.

```
In[55]:= μ[S] ** W[{1,0}] ** hc[μ[S]] == W[S.{1,0}]
Out[55]= True
```

5 Non-Binary Stabilizer Codes

We now consider the image of entire subspaces M of $\mathbb{F}_d^{2n}$ under the Weyl representation. The set $w(M)$ consists of $d^{\dim M}$ operators, which commute mutualy if M is isotropic. In that case, $w{\restriction}M$ is a representation of M viewed as an abelian group. As a consequence of Schur's lemma, this representation decomposes the Hilbert space into an orthogonal sum of one-dimensional subspaces, each invariant under $w{\restriction}m$. Indeed, w acts on each of these subspaces as a *character* of M. If k denotes the dimension of M, it can be shown, that the d^k characters of M occur with equal multiplicity [19] in the decomposition of $w{\restriction}M$ and thus each character is connected to a 2^{d-k}-dimensional subspace of the Hilbert space $\mathcal{H}$.

The space defined in this way by an isotropic subspace M and a character $\chi : M \to S^1$ is the *stabilizer code* associated to M and χ. The projection operator onto this space will be denoted as $\rho(M, \chi)$. In the special case that M is maximal isotropic, the code becomes one-dimensional and hence singles out a ray in Hilbert space. Modulo phases, this ray corresponds to a state vector which we refer to as $|M, \chi\rangle$. We write $\rho(M)$ shorthand for $\rho(M, \mathbb{1})$ where $\mathbb{1}$ is the trivial character, sending all elements of M to 1.

An isotropic subspace can be specified by a basis $\{m_1, \cdots, m_k\}$. The character in turn is fixed, once we know its values $\{\chi(m_1), \cdots, \chi(m_k)\}$ on the base vectors. The base vectors can be gathered together as the *columns* of a matrix, which is called the *generator matrix* of M (this is because the images of the base vectors under w *generate* the stabilizer group). We denote the generator matrix of a subspace with the corresponding calligraphic letter. Note that we are still using system coordinates and thus, in the generator matrix of M,

$$\mathcal{M} = \begin{pmatrix} m_{1,1} & \cdots & m_{1,n} \\ \vdots & & \vdots \\ m_{2n,1} & \cdots & m_{2n,n} \end{pmatrix} \tag{62}$$

two consecutive rows belong to one system.

Given M, χ, the mapping

$$m \mapsto \chi^*(m) w(m) \tag{63}$$

is a another faithful representation of M in $\mathcal{H}$. The set

$$\{\chi^*(m) w(m)\}_{m \in M} =: S(M, \chi) \tag{64}$$

is thus an abelian group, called the *stabilizer group* associated to the given data.

There is an explicit formula for the projection operator onto a stabilizer code:

$$\begin{aligned} \rho(M, \chi) &= \frac{1}{d^k} \sum_{m \in M} \chi^*(m) w(m) \qquad (65) \\ &= \frac{1}{d^k} \sum_{s \in S} s. \end{aligned}$$

Indeed, ρ defined as above can be checked to be idempotent, self-adjoint and further, for $m' \in M$,

$$\begin{aligned} w(m')\rho(M,\chi) &= w(m')\frac{1}{d^k}\sum_{m\in M}\chi(m)^* w(m) \\ &= \frac{1}{d^k}\sum_{m\in M}\chi(m)^* w(m+m') \\ &= \frac{1}{d^k}\sum_{m\in M}\chi(m-m')^* w(m) \\ &= \frac{1}{d^k}\sum_{m\in M}\chi(m')\chi^*(m) w(m) \\ &= \chi(m')\rho(M,\chi) \end{aligned} \tag{66}$$

and thus $w{\restriction}M$ acts as the multiplication operator by χ on range(ρ).

It follows that a state vector $|\psi\rangle$ belongs to the stabilizer code associated to M, χ if and only if

$$\chi^*(m)w(m)|\psi\rangle = |\psi\rangle \tag{67}$$

for all $m \in M$. In other words: $|\psi\rangle$ is a common eigenvector of all elements of the stabilizer group $S(M,\chi)$ to the eigenvalue 1. This fact is sometimes taken as the definition of stabilizer codes [26].

It is easy to see that for all characters χ, ξ of M, there is a Weyl operator mapping $\rho(M,\chi)$ to $\rho(M,\xi)$ under conjugation. Since the Weyl operators are local (see Eq. (34)) any two stabilizer codes belonging to the same isotropic subspace are local Clifford-equivalent.

5.1 Qbit Stabilizer Codes

In the non-binary case, $w(M)$ provided a faithful representation of an isotropic vector space M. For two-level systems, things are more complicated because the binary composition law (Eq. (39)) introduces phase factors even when two *commuting* Weyl operators are composed. This will cause $w(M)$ to be closed under composition only modulo phases. However, once a basis has been choosen within M, these phases can be fixed by the following construction. Let $\{m_i\}_i$ be a basis of an isotropic space M. Choose $\dim M$ numbers $\chi(m_i) \in \{+1, -1\}$. Every element $m \in M$ has a unique decomposition

$$m = \sum c_i m_i. \tag{68}$$

The operator

$$S(m) := \prod c_i \chi(m_i) w(m_i) \tag{69}$$

is well-defined, because the $w(m_i)$ commute (for M is isotropic). Thus the stabilizer group associated to the set $\{M, \{m_i\}_i, \chi\}$ can be defined as

$$S(M, \{m_i\}, \chi) := \{S(m) | m \in M\} \tag{70}$$

and the corresponding stabilizer code $\rho(M, \{m_i\}, \chi)$ is the the set of common eigenvectors of the operators $S(M, \{m_i\}, \chi)$ to the eigenvalue 1.

For the sake of simplicity, we define $S(\mathcal{M})$ to be $S(M, \{m_i\}, \mathbb{1})$, where the vectors m_i are the columns of the generator matrix $\mathcal{M}$. Thus $\rho(\mathcal{M})$ is well-defined in the binary case whereelse $\rho(M)$ is not.

For subsequent use, define the function $s(m)$ implicitely by the relation

$$S(m) = s(m)\chi(m)w(m). \tag{71}$$

6 The Characteristic Function

6.1 The Integrated Representation

The Schrödinger representatin of the Heisenberg group induces a representation of the convolution algebra $L_1(H^n)$ as in Eq. (20)

$$L_1(H^n) \ni f \mapsto w(f) := \sum_{p,q,t} f(p,q,t) w(p,q,t). \tag{74}$$

Following Ref. [13], we call $w(f)$ the *Integrated representation*.

The Integrated representation is not faithful. Indeed, only one Fourier component of $f(p,q,t)$ with respect to t contributes to the operator $w(f)$.

Proof. [13] We write $\mathcal{F}_3$ for the Fourier transformation operator with respect to the third argument of a function. Further, let χ be the character used in the definition of the Schrödinger representation, that is, let χ be such that

$$w(p,q,t) = w(p,q)\langle\chi|t\rangle.$$

Defining $\hat{f} = \mathcal{F}_3 f$ and inserting the identity

$$\begin{aligned} f(p,q,t) &= (\mathcal{F}_3^{-1}\hat{f})(p,q,t) \\ &= \frac{1}{\sqrt{d}} \sum_{\zeta} \hat{f}(p,q,\zeta)\langle t|\zeta\rangle \end{aligned}$$

into the definition of the integrated representation, we see that

$$\begin{aligned} w(f) &= \sum_{p,q,t} \frac{1}{\sqrt{d}} \sum_{\zeta} \hat{f}(p,q,\zeta)\langle t|\zeta\rangle w(p,q)\langle\chi|t\rangle \\ &= \sum_{p,q}\sum_{\zeta} \hat{f}(p,q,\zeta) d^{-1/2} \sum_{t} \langle\zeta|t\rangle\langle\chi|t\rangle \\ &= \sum_{p,q}\sum_{\zeta} \hat{f}(p,q,\zeta) d^{1/2} \delta_{\zeta,\chi^*} \\ &= \sqrt{d}\sum_{p,q} \hat{f}(p,q,\chi^*), \end{aligned}$$

which proves the assertion. □

Given a function F on $\mathbb{F}^{2n}$, we can lift it to a function on the Heisenberg group by setting

$$(l \circ F)(p,q,t) := \phi(p,q)\chi^*(t)d^{-1/2}. \tag{75}$$

The integrated representation now naturally extends to phase space functions on $\mathbb{F}^{2n}$ as

$$\begin{aligned} w(F) &:= w(l \circ \phi) \\ &= \sum_{p,q} F(p,q) w(p,q) \end{aligned} \tag{76}$$

where the last identity can easily be checked.

Recall, that in Eq. (20) we have seeen that the Integrated representation is compatible with convolution in the sense that

$$w(f * g) = w(f)w(g) \tag{77}$$

for $f, g \in L_1(H^n)$. It is now natural to ask how the lifting procedure introduced in the last paragraph fits into this framework. To this end, let F, G be phase space functions. Then

$$\begin{aligned}
& (lF) * (lG)(p,q,t) && (78)\\
= \quad & \frac{1}{d} \sum_{p',q',t'} F(p',q')\chi^*(t')G(p-p',q-q')\chi^*(t-t'-2^{-1}(-2^{-1}(p'q-q'p)) \\
= \quad & \frac{1}{d} \sum_{t'} \chi^*(t'-t')\chi^*(t) \sum_{p',q'} F(p',q')G(p-p',q-q')\chi^*(-2^{-1}(p'q-q'p)) \\
= \quad & \chi^*(t) \sum_{p',q'} F(p',q')G(p-p',q-q')\chi^*(2^{-1}(pq'-qp')) \\
=: \quad & l(F \natural G),
\end{aligned}$$

where we have defined the *twisted convolution* [13]

$$(F \natural G)(p,q) = \sum_{p',q'} F(p',q')G(p-p',q-q')\chi^*(2^{-1}(pq'-qp')). \tag{79}$$

Comparison with Eq. (77) shows that

$$w(F \natural G) = w(F)w(G) \tag{80}$$

for phase space functions F and G.

The following diagram symbolizes these relations.

$$\begin{tikzcd}
\langle F, G\rangle \arrow[r, "\natural"] \arrow[d, "l"'] & F \natural G \arrow[d, "l"] \\
\langle lF, lG\rangle \arrow[r, "*"] \arrow[d, "w"'] & lF * lG \arrow[d, "w"] \\
\langle w(F), w(G)\rangle \arrow[r, "\cdot"] & w(F)w(G)
\end{tikzcd}$$

6.2 Inverting the Integrated Representation: The Characteristic Function

The Integrated Representation associates an operator to a complex function on the vector space $\mathbb{F}^{2n}$. This mapping is one-to-one and can easily be inverted. Making use of the fact that

$$\operatorname{tr}(w(p,q)) = d^n \delta_{p,0}\delta_{q,0} \tag{81}$$

and the group law (27) one finds immidiately that the Weyl operators form an orthonormal basis with respect to the Hilbert-Schmidt inner product $\frac{1}{d^n}\operatorname{tr}(\cdot,\cdot)$. We identify the phase space function in Eq. (76) as the expansion coefficients with respect to this basis (modulo normalization). The relation

$$F(p,q) = \frac{1}{d^n}\operatorname{tr}(w(p,q)^\dagger w(F)) \tag{82}$$

follows.

The phase space function F is called the *characteristic function* of the operator $w(F)$. Because the Weyl operators form an orthonormal basis, any operator has a characteristic function which we will denote by

$$\Xi(A)(p,q) = \Xi_A(p,q) = \frac{1}{d^n}\operatorname{tr}(w(p,q)^\dagger A) \tag{83}$$

for a general operator A.

$$\begin{tikzcd}
\langle F,G\rangle \arrow[r, "\natural"] \arrow[d, shift right, "w"'] & F\natural G \arrow[d, shift left, "w"] \\
\langle w(F),w(G)\rangle \arrow[u, shift right, "c"'] \arrow[r, "\cdot"] & w(F)w(G) \arrow[u, shift left, "\Xi"]
\end{tikzcd}$$

We list some properties of the characteristic function.

1. *(Symplectic Covariance)* Using the results from Section 4.5 one immediately gets

$$\begin{aligned}
\Xi_{\mu(S)A\,\mu(S)^\dagger}(a) &= \frac{1}{d^n}\operatorname{tr}\left(w(a)^\dagger\mu(S)A\,\mu(S)^\dagger\right)\\
&= \frac{1}{d^n}\operatorname{tr}\left(\mu(S)^\dagger w(a)^\dagger\mu(S)A\right)\\
&= \frac{1}{d^n}\operatorname{tr}\left(w(S^{-1}a)^\dagger A\right)c_{S^{-1}}(a)\\
&= \Xi_A(S^{-1}a)c_{S^{-1}}(a),
\end{aligned}$$

where $c_{S^{-1}}(a)$ equals 1 in the case of non-binary system and is else given by Eq. (55). It is hence justified to call the characteristic function *symplectically covariant*.

2. *(Translations)* With the help of Eq. (29), we see that

$$\begin{aligned}
\Xi_{w(b)Aw(b)^\dagger}(a) &= \frac{1}{d^n}\operatorname{tr}\left(w(a)^\dagger w(b)Aw(b)^\dagger\right)\\
&= \frac{1}{d^n}\operatorname{tr}\left(w(b)^\dagger w(a)^\dagger w(b)A\right)\\
&= \frac{1}{d^n}\chi([a,b])^*\operatorname{tr}\left(w(a)^\dagger A\right)\\
&= \chi([a,b])^*\,\Xi_A(a).
\end{aligned}$$

Thus conjugation by Weyl operators corresponds to multiplying the characteristic function by a *character*.

3. *(Adjoint Operators)*

$$\begin{aligned}\Xi_{A^\dagger}(a) &= \frac{1}{d^n}\,\mathrm{tr}(w(a)^\dagger A^\dagger) \\ &= \frac{1}{d^n}\,\mathrm{tr}(Aw(a))^* \\ &= \frac{1}{d^n}\,\mathrm{tr}(w(-a)^\dagger A)^* \\ &= \Xi_A(-a)^*.\end{aligned}$$

Observe, that the matrix elements of A fullfil the same relation.

4. *(Trace)*

$$\begin{aligned}\mathrm{tr}(A) &= \mathrm{tr}\left(\sum_a \Xi_A(a)w(a)\right) \\ &= \sum_a \Xi_A(a)\,\mathrm{tr}\,w(a) \\ &= d^n\Xi_A(0)\end{aligned}$$

5. *(Hilbert-Schmidt scalar product)*

$$\begin{aligned}\frac{1}{d^n}\,\mathrm{tr}(A^\dagger B) &= \left(\Xi_{A^\dagger}\natural\,\Xi_B\right)(0) \\ &= \sum_a \Xi_{A^\dagger}(a)\Xi_B(0-a)\chi^*([a,0]) \\ &= \sum_a \Xi_A^*(-a)\Xi_B(-a) \\ &= \sum_a \Xi_A^*(a)\Xi_B(a) \\ &=: \Xi_A.\Xi_B\end{aligned}$$

where in the last line, we have defined a *scalar product* for complex phase space functions

$$\Xi_A.\Xi_B = \sum_a \Xi_A^*(a)\Xi_B(a). \tag{84}$$

6. *(State Vectors)* Let $|\psi\rangle$ be a state vector in $\mathcal{H}$ with coefficients $\langle x|\psi\rangle = \psi(x)$.

Then

$$\begin{aligned}
\Xi(|\psi\rangle\langle\psi|)(p,q) &= \frac{1}{d^n}\,\mathrm{tr}(w(-p,-q)|\psi\rangle\langle\psi|) \qquad (85)\\
&= \frac{1}{d^n}\,\mathrm{tr}(w(-p,-q)|\psi\rangle\langle\psi|)\\
&= \frac{1}{d^n}\langle\psi|w(-p,-q)|\psi\rangle\\
&= \frac{1}{d^n}\sum_{x\in\mathbb{F}^n}\psi(x)^*\chi(-2^{-1}pq)\chi(px)\psi(x-q)\\
&= \frac{1}{d^n}\sum_{y|x=y+2^{-1}q}\chi(-2^{-1}pq+p(y+2^{-1}q))\\
&\quad\ \psi(y+2^{-1}q)^*\psi(y+(2^{-1}-1)q)\\
&= \frac{1}{d^n}\sum_{y}\chi(py)\psi(y+2^{-1}q)^*\psi(y-2^{-1}q)
\end{aligned}$$

where we have used the fact that

$$(2^{-1}-1)(-2) = -1+2 = 1. \qquad (86)$$

and hence $2^{-1}-1=(-2)^{-1}$.

6.3 Computer Implementation

```
In[56]:= << head.m

         << qmatrixHead.m

         << heisenberg.m
In[57]:= qInit[1,3]
```

Define some operator.

```
In[58]:= w1 = W[{1,1}] + 0.75 W[{0,1}]
          (        0.          0.    0.25 + 0.866025 i )
Out[58]=  (0.25 - 0.866025 i   0.          0.          )
          (        0.         1.75         0.          )
         {ket[q1],bra[q1]}
```

characteristic[] computes its characteristic function.

```
In[59]:= (c1 = characteristic[w1]) //MatrixForm
          (0  0.75  0 )
Out[59]=  (0   1.   0 )
          (0   0    0 )
```

Take any second operator, for example a projection operator.

```
In[60]:= ψ = matrix[{1,0,0},{ket[q1]}]
          (1. )
Out[60]=  (0. )
          (0. )
         {ket[q1]}
In[61]:= w2 = ψ ** hc[ψ]
```

```
          ⎛1.  0.  0. ⎞
Out[61]=  ⎜0.  0.  0. ⎟
          ⎝0.  0.  0. ⎠
          {ket[q1],bra[q1]}

In[62]:=  (c2 = characteristicSave[w2])//MatrixForm
              1
          ⎛   ─      0  0 ⎞
Out[62]=  ⎜   3           ⎟
          ⎜0.333333  0  0 ⎟
          ⎝0.333333  0  0 ⎠
```

The *twisted convolution* of the two characteristic functions can be computed. It should be compatible with operator composition.

```
In[63]:=  twist[c1,c2] == characteristic[w1 ** w2]
Out[63]=  True
```

7 The Wigner-Transformation

7.1 Definition

We define the Wigner function of an hermitian operator A to be the symplectic Fourier transform of its characteristic function:

$$W := \tilde{\mathcal{F}} \circ \Xi. \tag{87}$$

Conversely, by inverting Eq. (87), one can associate an operator to a phase space function:

$$\Omega := W^{-1} = \Xi^{-1} \circ \tilde{\mathcal{F}}^{-1} = w \circ \tilde{\mathcal{F}}. \tag{88}$$

In the continuous case, the preceding relation is known as the *Weyl correspondance* [13].

$$\begin{tikzcd}
\tilde{F} \arrow[rr, shift left, "w"] & & w(\tilde{F}) \arrow[ll, shift left, "\Xi"] \arrow[dl, shift right, "W"'] \\
& F \arrow[ul, leftrightarrow, "\tilde{\mathcal{F}}"] \arrow[ur, shift right, "\Omega"'] &
\end{tikzcd}$$

Let us explore the consequences of the definitions. Consider the case $\mathcal{H} = \mathbb{C}^{nd}, d = p^r, V = \mathbb{F}_d^{2n}$. For the Wigner function we have for all $a \in V$

$$\begin{aligned}
W_A(a) &= W(A)(a) \qquad (89)\\
&= \tilde{\mathcal{F}}\,\Xi_A(a)\\
&= \frac{1}{d^{2n}} \sum_{b \in V} \chi([a,b])^* \operatorname{tr}(w(b)^\dagger A)\\
&= \frac{1}{d^n} \operatorname{tr}\left((\frac{1}{d^n} \sum_{b \in V} \chi([a,b])^* w(b)^\dagger)\, A \right).
\end{aligned}$$

The above function leads naturally to the definition of the *phase space point operators* (see Ref. [9])

$$A(a) := \frac{1}{d^n} \sum_{b \in V} \chi([a,b])^* w(b)^\dagger. \tag{90}$$

We establish some properties of the phase space point operators.

1. Phase space point operators are hermitian.

$$\begin{aligned}
A^\dagger(a) &= \frac{1}{d^n} \sum_b \chi([a,b]) w(b)\\
&= \frac{1}{d^n} \sum_b \chi([a,-b])^* w(-b)\\
&= \frac{1}{d^n} \sum_b \chi([a,b])^* w(b)\\
&= A(a),
\end{aligned}$$

where the line next to the last one is justified since the sum ranges over a vector space.

2. Phase space point operators have unit trace.

$$\begin{aligned}
\operatorname{tr} A(a) &= \frac{1}{d^n} \operatorname{tr}\left(\sum_b \chi([a,b])^* w(b)\right) \\
&= \frac{1}{d^n} \sum_b \chi([a,b])^* \operatorname{tr} w(b) \\
&= \frac{1}{d^n} d^n \\
&= 1
\end{aligned}$$

3. Phase space point operators form an orthonormal basis with respect to the Hilbert-Schmidt inner product.

$$\begin{aligned}
\frac{1}{d^n} \operatorname{tr}(A^\dagger(a)A(b)) &= \frac{1}{d^n} \operatorname{tr}(A(a)A(b)) \\
&= \frac{1}{d^{3n}} \sum_{c,d} \chi([a,c])^* \chi([b,d])^* \operatorname{tr}(w(c)w(d)) \\
&= \frac{1}{d^{2n}} \sum_{c,d} \chi([a,c])^* \chi([b,d])^* \delta_{c,-d} \\
&= \frac{1}{d^{2n}} \sum_{c} \chi([a,c])^* \chi([b,c]) \\
&= \frac{1}{d^{2n}} d^{2n} \delta_{a,b} \\
&= \delta_{a,b}
\end{aligned}$$

4. The sum over all phase space point operators is a multiple of the unity.

$$\begin{aligned}
\sum_a A(a) &= \frac{1}{d^n} \sum_a \sum_b \chi([a,b]) w(b) \\
&= \frac{1}{d^n} \sum_b \left(\sum_a \chi([a,b])\right) w(b) \\
&= \frac{1}{d^n} \sum_b d^{2n} \delta_{b,0} w(b) \\
&= d^n w(0) \\
&= d^n \mathbb{1}.
\end{aligned}$$

7.2 Properties

From the properties of the phase space point operators, we can derive immediately an interpretation of the Wigner function of an operator: it gives the expansion coefficients of that operator in terms of the orthogonal basis of phase space point operators. Because the latter are hermitian, the Wigner function of a hermitian operator is real.

Further properties:

1. *(Symplectic Covariance)* Using the symplectic covariance of the symplectic Fourier transformation (24) and of the characteristic function (84), we get for the case of non-binary systems

$$\begin{aligned} W_{\mu(S)B\mu(S)^\dagger}(a) &= (\tilde{\mathcal{F}}\Xi_{\mu(S)B\mu(S)^\dagger})(a) \\ &= (\tilde{\mathcal{F}}\Xi_B)(S^{-1}a). \\ &= W_B(S^{-1}a). \end{aligned} \tag{91}$$

   In the qbit case, the phases $c_{\mu(S)}$ are in general non-trivial. Here, the Wigner function looses its covariance under Clifford operations.

   If, in the qbit case, the phases $c_{\mu(S)}$ are non-trivial, the Wigner function looses its covariance under Clifford operations.

2. *(Translational Covariance)* The Wigner function is also covariant under phase space shifts:

$$\begin{aligned} W_{w(b)Bw(b)^\dagger}(a) &= \Big(\tilde{\mathcal{F}}(\chi([\cdot,b])^*\,\Xi_B(\cdot))\Big)\,(a) \\ &= \Big(\tilde{\mathcal{F}}\,\Xi_B\Big)\,(a-b), \\ &= W_B(a-b), \end{aligned} \tag{92}$$

   where we have made use of Eq. (25).

3. *(Trace)*

$$\begin{aligned} \mathrm{tr}(B) &= \mathrm{tr}\left(\sum_a W_B(a)A(a)\right) \\ &= \sum_a W_B(a)\,\mathrm{tr}(A) \\ &= \sum_a W_B(a) \end{aligned} \tag{93}$$

4. *(Hilbert-Schmidt scalar product)* Let B and C be hermitian.

$$\begin{aligned} \frac{1}{d^n}\,\mathrm{tr}(BC) &= \frac{1}{d^n}\,\mathrm{tr}\sum_b W_B(b)A(b)\sum_c W_C(c)A(c) \\ &= \sum_{b,c} W_B(b)W_C(c)\frac{1}{d^n}\,\mathrm{tr}(A(b)A(c)) \\ &= \sum_{b,c} W_B(b)W_C(c)\delta_{b,c} \\ &= \sum_b W_B(b)W_C(b) \\ &=: W_B.W_C. \end{aligned} \tag{94}$$

   The last line uses the phase space scalar product defined in Eq. (84). Note the difference in normalization as compared to the standard physicists' convention for computing expectation values.

We can now analyze to covariance properties of the Wigner function. To this end, consider an affine transformation on V:

$$v \mapsto Av + a \tag{95}$$

for some $A \in GL(V)$ and $a \in V$. We denote the set of elements of $\mathrm{Aff}(V)$ whose 'linear part' A is symplectic by $\mathrm{SpAff}(V)$. SpAff can be checked to be a subgroup of Aff, or, if one wishes, to be a *semi-direct product* of $\mathrm{Sp}(V)$ and V. We define a mapping from $\mathrm{SpAff}(V)$ to $U(\mathcal{H})$ by

$$A \cdot + a \mapsto w(a)\mu(A). \tag{96}$$

No confusion should arise by denoting the above map by μ as well. Note, that this designation is compatible with the special case $a = 0$. Now,

$$\begin{aligned}(A \cdot + a) \circ (B \cdot + b) &= A(B \cdot + b) + a \\ &= AB \cdot + (Ab + a)\end{aligned} \tag{97}$$

while

$$\begin{aligned}(w(a)\mu(A))\,(w(b)\mu(B)) &= w(a)\mu(A)w(b)\mu(B) \\ &= w(a)\mu(A)w(b)\mu(A)^\dagger \mu(A)\mu(B) \\ &= w(a)w(Ab)\mu(A)\mu(B) \\ &\propto w(Ab + a)\mu(AB)\end{aligned} \tag{98}$$

and therefore μ is a projective representation of $\mathrm{SpAff}(V)$. The group generated by the image of μ is sometimes referred to as the *Jacobi group* [21]. Combining the symplectic and the translational covariance of the Wigner function, we see that if

$$B' := \mu(A \cdot + a)B\,\mu(A \cdot + a)^\dagger \tag{99}$$

then

$$\begin{aligned}&W_{B'}(v) = W_B(A^{-1}v - A^{-1}a). \\ \Leftrightarrow\quad &W_{B'}(A\,v + a) = W_B(v).\end{aligned} \tag{100}$$

It is in this sense that the Wigner function is covariant under the action of the affine group of V.

7.3 Wigner Functions of Stabilizer Codes

Recall from Section 5 that a projection operator onto a stabilizer code associated with the isotropic space M and the character ζ can be obtained by the sum

$$\rho(M, \chi) = \frac{1}{d^k} \sum_{m \in M} \zeta^*(m)w(m). \tag{101}$$

Because $v \mapsto \chi([v, \cdot])$ is an isomorphism into the character group of $\mathbb{F}$, there always is a $v \in V$ such that

$$\zeta(\cdot) = \chi([v, \cdot]) \tag{102}$$

for any given character ζ. Now, obviously,

$$\chi([v,m]) = \chi([v',m]) \tag{103}$$

for all $m \in M$ if and only if $v' - v$ lies in the symplectic complement $M^\perp$ of M. Hence, there is a one-one correspondence between characters of M and

$$V/M^\perp. \tag{104}$$

Because $M^\perp$ is a vector space, the quotient above is an *affine space*. In the special case that M is maximally isotropic, $M^\perp = M$ and

$$V/M^\perp = V/M. \tag{105}$$

We see that instead of using the data $\{M, \zeta\}$, we can specify a stabilizer code by $\{M, v\}$, where v is an element of $V/M^\perp$. In that sense, stabilizer codes can be thought of as affine spaces with directional vector space M and base point v. The Wigner function representation of stabilizer states turns out to be compatible with that point of view. Indeed, we see that

$$\begin{aligned} \Xi_{\rho(M,v)}(a) &= \frac{1}{d^{n+k}} \sum_{m\in M} \chi([m,v])^* \operatorname{tr}(w(-a)w(m)) \qquad (106) \\ &= \frac{1}{d^k}\chi([a,v])^* \delta_M(a), \end{aligned}$$

where δ_M is the *indicator function* of M defined to be

$$\delta_M(v) = \begin{cases} 1 & v \in M \\ 0 & \text{else} \end{cases} . \tag{107}$$

Further,

$$\begin{aligned} (\tilde{\mathcal{F}}\,\delta_M)(a) &= \frac{1}{d^n} \sum_{m\in M} \chi([a,m])^* \qquad (108) \\ &= \frac{1}{d^n}|M|\delta_{M^\perp}(a) \\ &= \delta_{M^\perp}(a). \end{aligned}$$

Hence, making use of the results of Section 3.4.1,

$$W_{\rho(M,v)} = \frac{1}{d^k}\,\delta_{M^\perp+v} \tag{109}$$

and in the special case of stabilizer *states*,

$$W_{\rho(M,v)} = \frac{1}{d^n}\,\delta_{M+v}. \tag{110}$$

7.4 Marginal Probabilities

We shortly comment on how the above results on stabilizer codes can be used to describe the computation of *marginal probabilities* in phase space. For a more detailed presentation of the topic and how it relates to *quantum state tomography*, see Ref. [9].

In the case $n = 1$ of a single system, the Wigner function of a stabilizer state is the indicator function of a one dimensional affine space, that is, it is a line in phase space. Now consider the Wigner function W_σ of some density matrix σ and let λ be some line in phase space. Using Eq. (94) and Eq. (110), it is clear that

$$\sum_{a \in \lambda} W_\sigma(a) = \mathrm{tr}(\sigma \rho(\lambda)) \tag{111}$$

where $\rho(\lambda)$ is the stabilizer state associated to (the affine space) λ in the sense of the last section.

As a particular example, look at the lines parallel to the momentum axis, displaced from the origin by the offset q

$$\lambda_q := \left\{ \begin{pmatrix} p \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ q \end{pmatrix} | p \in \mathbb{F} \right\}. \tag{112}$$

It is easy to see that

$$\rho(\lambda_q) = |q\rangle\langle q| \tag{113}$$

and thus, the sum of the values of a Wigner function W_σ over the points of the line λ_q is the expectation value of $|q\rangle\langle q|$ with respect to the state σ. The same procedure can be repeated for any set of parallel lines in phase space – forming a perfect analogy to the computation of *marginal probabilities* of a classical probability distribution on phase space.

7.5 Computer Implementation

```
In[64]:= <<head.m

         <<qmatrixHead.m

         <<heisenberg.m

         <<someStates.m
In[65]:= qInit[1,3]
```

Let us look at a computational basis state (or 'position' eigenstate, if one wishes) in dimension three.

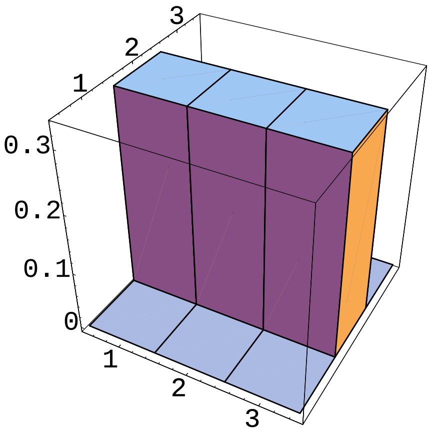
```
In[66]:= ψ = posEigenstate[1,1];

In[67]:= Chop@posEigenstate[1,1] //toAbstract
Out[67]= 1. |0 >
```

`wigner[]` computes the Wigner function of a given state vector or operator.

```
In[68]:= wigner[ψ ∗ ∗hc[ψ]] //MatrixForm
         ⎛0.333333  0  0⎞
Out[68]= ⎜0.333333  0  0⎟
         ⎝0.333333  0  0⎠
```

However, most of the times we are interested in a visual representation. The function **`Visualize[]`** is a powerful wrapper for several visualization methods. We'll comment on it soon.

```
In[69]:= Visualize[ψ]
```



```
Out[69]= -Graphics3D-
```

The function `A[]` returns a phase space point operator. The first argument specifies the system it acts on, the second argument the phase space point it belongs to.

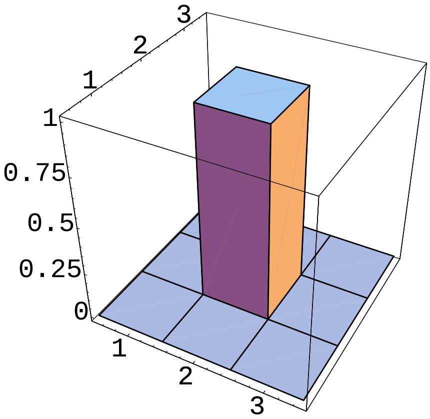
```
In[70]:= A[1,0,0]
          ⎛1.  0.  0. ⎞
Out[70]=  ⎜0.  0.  1. ⎟
          ⎝0.  1.  0. ⎠
         {ket[q1],bra[q1]}
```

The following definition is taken from `heisenberg.m`. It shows how to use the Fourier transformation function on operators.

```
In[71]:= A[i_,ξ_,x_] := A[i,ξ,x] = SFT[W[i,#1,#2]&][ξ,x];
```

A phase space point operator's Wigner function is sharply concentrated in both position and momentum space.

```
In[72]:= Visualize[A[0,0]]
```



```
Out[72]= -Graphics3D-
```

However it does not represent a physical state because it is not a positive operator.

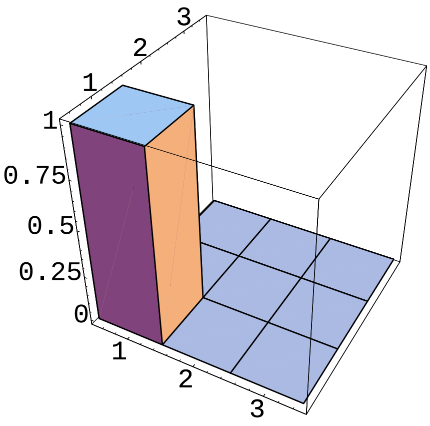
```
In[73]:= eigenvalues@A[1,0,0]
Out[73]= {-1.,1.,1.}
```

The wrapper **`Visualize[]`** comes with several options.

```
In[74]:= Options[Visualize]
Out[74]= {Style → BarChart, Centered → True, SymbolMethod → wigner, ImageSize →
200}
```

If we turn of the centering option, then the origin of the phase space will be placed at the lower left corner.

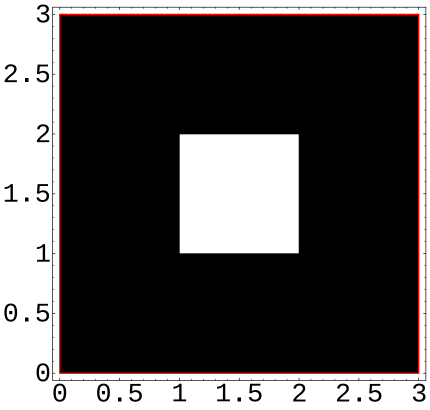
```
In[75]:= Visualize[A[0,0], Centered → False]
```



```
Out[75]= -Graphics3D-
```

For more complex situations, the bar graphs are hard to interpret. A 'flat' representation turns out to be more advantageous.

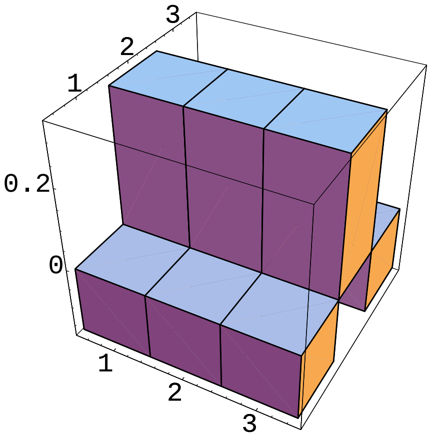
```
In[76]:= Visualize[A[0,0], Style → Density]
```



```
Out[76]= -DensityGraphics-
```

Visualize[] is not limited to Wigner functions. Any function that turns an operator into a 2-D matrix can be specified as an argument to the **SymbolMethod** option.

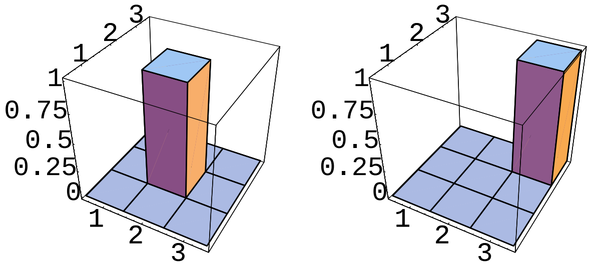
```
In[77]:= Visualize[A[1,0], SymbolMethod → (Chop@Re[characteristic[#]]&)]
```



```
Out[77]= -Graphics3D-
```

If one wants to look at many transforms simultaneously, then **DrawArray[]** offers some space savings.

```
In[78]:= DrawArray[A[0,0], W[{1,1}] ** A[0,0] ** hc[W[{1,1}]]]
```

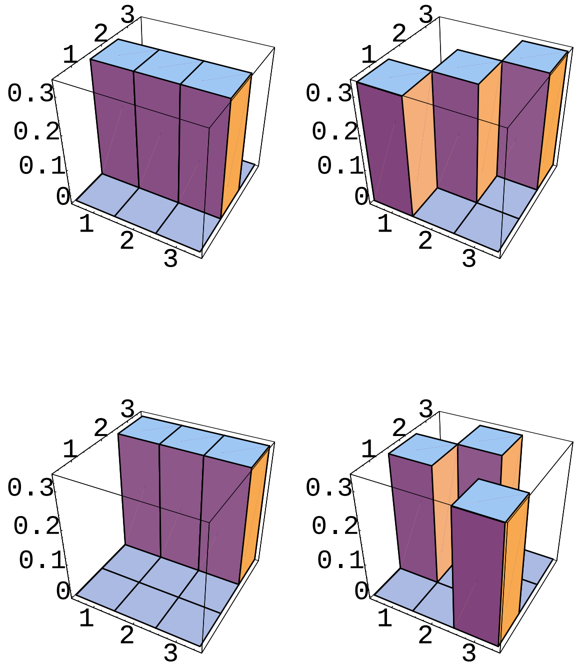


Let us check the covariance properties under the action of the Jacobi group.

```
In[79]:= (S = {{1,1},{1,0}}) //MatrixForm
```

Out[79]= $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

```
In[80]:= DrawArray[ψ, μ[S] ** ψ, W[{0,1}] ** ψ, W[{0,1}] ** μ[S] ** ψ, 2]
```



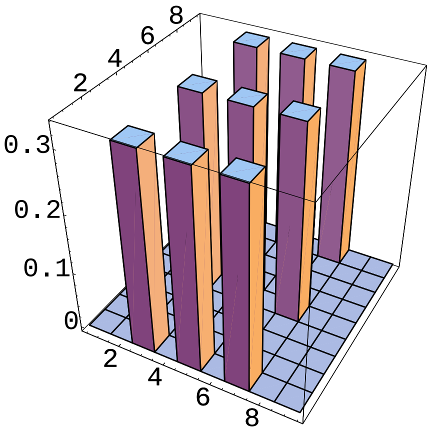
```
In[81]:= qInit[2,3]
```

Here is an example of a two-particle system.

```
In[82]:= Psi = posEigenstate[1,1]**posEigenstate[2,1]+posEigenstate[1,2]*
*posEigenstate[2,2] + posEigenstate[1,3] * *posEigenstate[2,3];
```

```
In[83]:= Chop@Psi //toAbstract
Out[83]= 1. |00 > +1. |11 > +1. |22 >
```

```
In[84]:= WignerDraw[Psi]
```

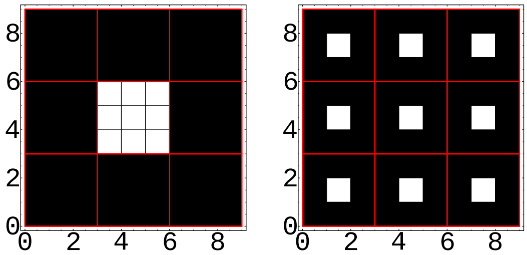


```
Out[84]= -Graphics3D-
```

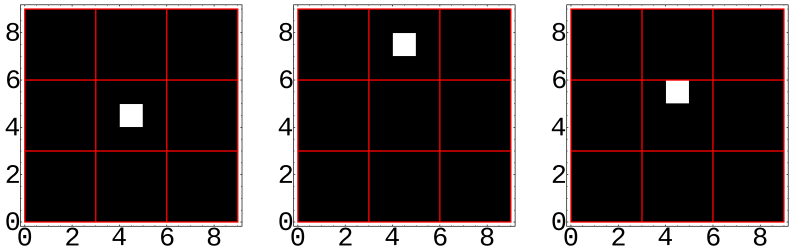
The 4-D phase space is flattened out using a ’first-system major, second system minor’ approach as will be exemplified below.

```
In[85]:= SetOptions[Visualize, Style → Density];
```

```
In[86]:= DrawArray[A[1,0,0]**W[2,0,0],W[1,0,0]**A[2,0,0]]
```



```
In[87]:= DrawArray[A[1,0,0]**A[2,0,0],A[1,0,1]**A[2,0,0],A[1,0,0]**A[2,0,1]]
```



Consider, for example, the (vertical) position axis. It has nine points where three consecutive points correspond to a fixed value of the position coordinates of the first system.

7.6 The Case of Extension Fields

Let us take a look at the one-dimensional Heisenberg group on an extension field $\mathbb{F} = \mathbb{F}_{p^r}$. According to Section 3.1 it is possible to find two bases $\{e_i\}, \{e^j\}$ in $\mathbb{F}$ which are dual to each other in the sense that

$$\mathrm{Tr}(e_i e^j) = \delta_i^j. \tag{114}$$

Adopting Einstein’s summation convention, we can write elements p, q of $\mathbb{F}$ in terms of these bases as

$$p = p_i e^i \tag{115}$$

$$q = q^i e_i \tag{116}$$

where the p_i and q^i are elements of the base field $\mathbb{F}_p$. Further, we know that the character χ used in the definition of the Heisenberg group is of the form

$$\chi(\cdot) = \omega^{\mathrm{Tr}\, a\cdot} \tag{117}$$

for some $a \in \mathbb{F}$. Because the trace $\mathbb{F}_{p^r} \to \mathbb{F}_p$ is never faithful, the Weyl representation Eq. (31) cannot be faithful in the case of a Heisenberg group over an extension field. It is thus natural to define the *reduced Heisenberg group* $h(\mathbb{F})$ as $\mathbb{F} \times \mathbb{F} \times \mathbb{F}_p$ with composition law

$$(p,q,t)(p',q',t') = (p+p', q+q', t+t'+2^{-1}\operatorname{Tr} a\left[\left(\begin{array}{c} p \\ q \end{array}\right), \left(\begin{array}{c} p' \\ q' \end{array}\right)\right]). \tag{118}$$

The function

$$\begin{array}{rcl} H(\mathbb{F}) & \to & h(\mathbb{F}) \\ (p,q,t) & \mapsto & (p,q,\operatorname{Tr} at) \end{array} \tag{119}$$

can be checked to be a group homomorphism. Further, it is clear that the Weyl representation is faithful on $h(\mathbb{F})$.

The Weyl representation of $H(\mathbb{F}_{p^r})$ is defined on

$$\mathcal{H} = \mathbb{C}^{p^r} \cong (\mathbb{C}^p)^r \tag{120}$$

with basis $\{|i\rangle\}_{i=1\cdots p^r}$. We can introduce a tensor structure on $\mathcal{H}$ by setting

$$T : |q_1, \cdots, q_r\rangle \mapsto |q^i e_i\rangle. \tag{121}$$

The shift and clock operators are compatible with that structure in the sense that

$$\begin{aligned} x(\sum_i q^i e_i) &= \prod_i x(q^i e_i) \\ &= \bigotimes_i x^{(i)}(q^i) \end{aligned} \tag{122}$$

$$\begin{aligned} z(\sum_i p^i e^i) &= \prod_i z(p_i e^i) \\ &= \bigotimes_i z^{(i)}(p_i) \end{aligned} \tag{123}$$

where we have implicitly defined the operators

$$x^{(i)}(q) := x(qe_i) \tag{124}$$

$$z^{(i)}(p) := z(pe^i) \tag{125}$$

and the tensor notation is justified because the newly defined operators act only on the ith subsystem in the sense of Eq. (121) as can easily be seen.

Let us for the moment assume that $a = 1$. By the linearity of the trace it holds that

$$\begin{aligned} \operatorname{Tr} pq &= \operatorname{Tr}\left((p_i e^i)(q^j e_j)\right) \\ &= p_i q^j \operatorname{Tr}(e^i e_j) \\ &= p_i q^j \delta^i_j \\ &= p_i q^i \end{aligned} \tag{126}$$

and hence

$$\begin{aligned}\chi(pq) &= \omega^{\operatorname{Tr} pq} \\ &= \omega^{\sum_i p_i q^i} \\ &= \prod_i \chi_{\mathbb{F}_p}(p_i q^i).\end{aligned} \tag{127}$$

Note that we do not apply the summation convention if the index variable is bound by some symbol, as for example by the product $\prod_i$ in the last line.

Combining the results from the last two paragraphs, we see that

$$\begin{aligned}w(p,q,t) &= \chi(-2^{-1}pq)z(p)x(q) \\ &= \prod_i \chi(-2^{-1}p_i q^i) \bigotimes_i z^{(i)}(p_i) \bigotimes_i x^{(i)}(q^i) \\ &= \bigotimes_i w^{(i)}(p_i, q^i)\end{aligned} \tag{128}$$

and hence the Weyl representation *factors* with respect to the tensor structure (121).

Going on, we compute

$$\begin{aligned}A(p,q) &= \sum_{\xi,\zeta\in\mathbb{F}} \chi\left(\left[\begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} \xi \\ \zeta \end{pmatrix}\right]\right) w(p,q) \\ &= \sum_{\xi,\zeta} \chi(p\zeta)\chi(q\xi)^* \bigotimes_i w^{(i)}(p_i, q^i) \\ &= \sum_{\xi,\zeta} \prod_i \chi(p_i\zeta^i)\chi(q^i\xi_i)^* \bigotimes_i w^{(i)}(p_i, q^i) \\ &= \bigotimes_i \sum_{\xi_i,\zeta^i\in\mathbb{F}_p} \chi(p_i\zeta^i)\chi(q^i\xi_i)^* w^{(i)}(p_i, q^i) \\ &= \bigotimes_i A^{(i)}(p_i, q^i)\end{aligned} \tag{129}$$

and thus the phase space point operators factor as well.

So with the character χ chosen the way we did (in particular $a = 1$), the Weyl operators w and the phase space point operators A of $\mathbb{F}_{p^r}$ are identical to the ones of $(\mathbb{F}_p)^r$ and, in particular, inherit all transformation properties from the multi-dimensional case.

Let us formalize this observation. Consider the symplectic vector space $V = \mathbb{F}^2$ over the extension field $\mathbb{F} = \mathbb{F}_{p^r}$ with a symplectic basis $\{e_p, e_q\}$. Further, choose two field bases $\{f_i\}, \{f^i\}$ which are dual to each other. Every vector v of V can be written as

$$v = v_i f^i e_p + v^i f_i e_q \tag{130}$$

and is thus connected to a set of $2r$ coordinates $\{v_i, v^i\}$ in the base field $\mathbb{F}_p$. Therefore the map

$$\iota : v \mapsto \begin{pmatrix} v_1 \\ \vdots \\ v_r \\ v^1 \\ \vdots \\ v^r \end{pmatrix} \tag{131}$$

is well-defined and maps V to the $\mathbb{F}_p$-vector space W of $2r$-dimensional column vectors. The map ι is compatible with addition and $\mathbb{F}_p$-scalar multiplication. The vector space W inherits a symplectic form via

$$[\iota\, a, \iota\, b]_W := \mathrm{tr}[a, b]_V. \tag{132}$$

The following statements relate the structures of V and W.

1. ι maps subspaces of V to subspaces of W. Its inverse, ι^{-1}, need not have this property.
2. ι maps isotropic subsets of V to isotropic subsets of W. Again, the converse statement does not hold in general.
3. Let $S_V \in \mathrm{Sp}(V)$ be a symplectic linear mapping in V. Then $\iota\, S_V \iota^{-1}$ is an element of $\mathrm{Sp}(W)$. On the other hand, for $S_W \in \mathrm{Sp}(W)$, the mapping $\iota\, S_W \iota^{-1}$ can fail to be linear or isotropic.

Proof.

1. Let M_V be a subspace of V and denote $\iota\, M$ by M_W. Let $\iota\, a, \iota\, b \in M_W$, $\lambda \in \mathbb{F}_p$. Then

   $$\lambda\iota\, a + \iota\, b \quad = \quad \iota\,(\lambda a + b) \in M_W$$

   because M_W is linear. A counterexample for the converse statement can easily be constructed.
2. Let $M_V \subset V$ be isotropic. For $\iota\, a, \iota\, b \in \iota\, M_V$ we have

   $$[\iota\, a, \iota\, b]_W = \mathrm{tr}[a, b]_V$$

   which is zero if $[a, b]_V$ is.
3. The last statement is a consequence of the previous ones.

□

From a pragmatic standpoint the following question arises: given an p^r dimensional Hilbert space, is it more fruitful to associate it with a 2-dimensional phase space over $\mathbb{F}_{p^r}$ or with a $2r$-dimensional one over $\mathbb{F}_p$? From the considerations above, the latter choice seems to be more natural since all relevant structures (subspaces, isotropic spaces, symplectic mappings) can be mapped from $\mathbb{F}_{p^r}^2$ to $\mathbb{F}_p^{2r}$, but not vice versa. However, certain constructions in quantum state tomography and in the theory of mutually unbiased bases [9] rely on the geometry of a 2-dimensional vector space which is of course more manifestly present in $\mathbb{F}_{p^r}^2$.

Note that in the section, we have addressed two questions posed by Gibbons, Hoffman and Wootters in [9], namely the question of whether factoring phase space point operators exits in any prime-power dimension and which symmetrie groups they are subject to.

8 An Application: Automorphisms of SIC-POVMs

A detailed introduction to the problem of SIC-POVMs can be found in the Appendix. The particular problem we like to address here is the following. In Ref. [32] Renes et al. described a numerical method for finding fiducial states for SIC-POVMs which are covariant under the Weyl representation. Zauner's conjecture implies that these fiducial states are eigenvectors of a Clifford operation. How can we efficiently compute the Clifford symmetries of the fiducial states, given the numerical data?

The answer turns out to be easy if one uses the covariance properties of the Wigner function. Indeed, if $|\psi\rangle$ is some state vector and $Z = \mu(A \cdot + a)$ any Clifford operation such that $Z|\psi\rangle = |\psi\rangle$, then the Wigner function of $|\psi\rangle$ must be invariant under the affine transformation $A \cdot + a$. So the analysis of Clifford symmetries of a quantum state reduces to the study of classical symmetries of the related phase space distribution. In the next paragraphs we will derive an algorithm that automatically detects a subset of these symmetries.

Before proceeding, let us briefly turn to the concept of a *histogram*. Given a function $f : A \to B$ defined on a finite set A, the histogram $\mathrm{hist}_f : B \to \mathbb{N}$ is

$$\mathrm{hist}_f(b) := |f^{-1}(b)| \tag{133}$$

that is, the number of times f takes on the value b.

Now consider a density matrix ρ which fulfills the equation $Z\rho Z^\dagger = \rho$ for some

$$Z = \mu(A \cdot + a).$$

The following algorithm will recover the affine transformation $A \cdot + a$ given ρ, if the criteria

- A has no eigenvectors and
- there exists at least one $r \in \mathbb{R}$ such that $|\,\mathrm{hist}_W(r)| = 1$

are met.

1. Compute the Wigner function W_ρ of ρ.
2. Compute the *histogram* of the Winger function.
3. There is exactly one value r such that $\mathrm{hist}_W(r) = 1$ (from the assumptions, there is at least one such value – the uniqueness will be shown later). Let v_0 be the phase space point where W takes on that unique value.
4. Let $\{e_i\}_i$ be a basis in V, let

   $$v_i := v_0 + e_i. \tag{134}$$

   Let $T_i := \{w \in V | W(w) = W(v_i)\}$ (T stands for *target* – the reason for this designation will become apparent soon).

5. Now, choose a vector t_i from each set T_i and assemble the vectors $t_i - v_0$ as the columns of a matrix S. Then

$$S \cdot + (\mathbb{1} - S)v_0 \tag{135}$$

is a candidate for a symmetry of ρ. The original transformation $A \cdot +a$ will be among the ones constructed in the described way.

Proof. *(of the functioning of the algorithm)* Let $f : v \mapsto Av + a$ be the affine transformation such that $\mu(f)$ leaves ρ invariant. From the covariance properties of the Wigner function we know that $Z\rho Z^\dagger = \rho$ if and only if

$$W_\rho(f(v)) = W_\rho(v)$$

for all $v \in V$. In other words, W must be constant on the orbits $\{O_i\}_i$ of f acting on V. Therefore,

$$\mathrm{hist}(r) = \sum_{\{i \,|\, W(O_i)=r\}} |O_i|.$$

We have assumed that A has no eigenvectors and hence the equation

$$\begin{aligned} & f(v) = v \\ \Leftrightarrow \quad & Av + a = v \\ \Leftrightarrow \quad & Av - v = -a \\ \Leftrightarrow \quad & -(A - \mathbb{1})v = a \end{aligned}$$

has exactly one solution, namely

$$v = v_0 := -(A - \mathbb{1})^{-1} a.$$

So $\{v_0\}$ is the only orbit of f with just a single element and we have proven the claim made in step 3.

Consider the definitions from step 4 and 5. Certainly, $f(v_i) \in T_i$ and therefore, among the matrices S constructed in step 5, there will be one with its ith column equal to $f(v_i) - v_0$, for all i. But

$$\begin{aligned} Se_i &= f(v_i) - v_0 \\ &= A(v_0 + e_i) + a - v_0 \\ &= Av_0 + Ae_i - (A - \mathbb{1})v_0 - v_0 \\ &= Ae_i + Av_0 - Av_0 + v_0 - v_0 \\ &= Ae_i \end{aligned}$$

and thus there is a choice of $t_i \in T_i$, for all i, such that $S = A$. In that case

$$S \cdot + (\mathbb{1} - S)v_0 = A \cdot +a$$

which concludes the proof. □

8.1 Computer Implementation

The algorithm described in the last section was designed to analyze numerical data and therefore this time the computer implementation is not just an accompanying example but the sole reason for the algorithm to have been developed.

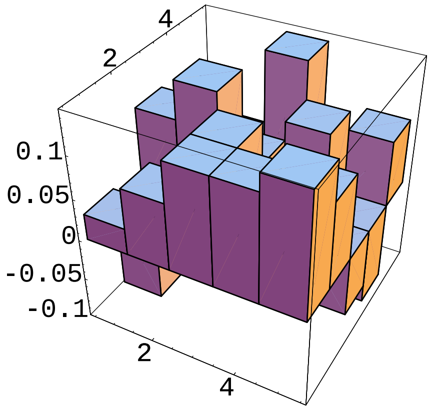
```
In[88]:= <<head.m

         <<qmatrixHead.m

         <<sicNumerics.m

         <<findAutomorphisms.m
```

The package **`sicNumerics.m`** provides the function **`sic[]`** which returns a **`qmatrix`** representation of the numerical fiducial states found by Renes et al. for any dimension up to 45.

```
In[89]:= qInit[1,5]

In[90]:= sic[5]
          ⎛ 0.163095 - 0.35541 ⅈ   ⎞
          ⎜0.304839 + 0.0113255 ⅈ  ⎟
Out[90]=  ⎜ 0.278427 + 0.383676 ⅈ  ⎟
          ⎜ 0.647962 - 0.282966 ⅈ  ⎟
          ⎝ 0.154455 - 0.074289 ⅈ  ⎠
          {ket[q1]}
```

On first sight, the Wigner function does not look like it conveys much information.

```
In[91]:= Visualize[sic[5]]
```



```
Out[91]= -Graphics3D-
```

The histogram seems to be more promising:

```
In[92]:= numHistogram[wigner[sic[5]]] //MatrixForm
```

```
            ⎛1  -0.0732051⎞
            ⎜3  -0.0943128⎟
            ⎜3   -0.04984 ⎟
            ⎜3  0.0267202 ⎟
Out[92]=    ⎜3  0.0306711 ⎟
            ⎜3  0.0778175 ⎟
            ⎜3  0.0993055 ⎟
            ⎜3   0.124063 ⎟
            ⎝3   0.143311 ⎠
```

We can immediately guess that **`sic[5]`** is invariant under a Clifford operation of order three with one fixed point.

The function **`findAutomorphisms[]`** reports the linear part of the affine transformation.

```
In[93]:= autos = findAutomorphisms[sic[5]];

In[94]:= MatrixForm /@ autos
Out[94]= {( 0     {1}₅ ), ( {4}₅  {4}₅ )}
          ( {4}₅  {4}₅ )  ( {1}₅   0   )

In[95]:= (S = autos[[1]]) //MatrixForm
Out[95]= ( 0     {1}₅ )
         ( {4}₅  {4}₅ )

In[96]:= S.S //MatrixForm
Out[96]= ( {4}₅  {4}₅ )
         ( {1}₅   0   )

In[97]:= S.S.S //MatrixForm
Out[97]= ( {1}₅   0   )
         (  0    {1}₅ )
```

This is indeed an order three matrix.

The function **`findOrigin[]`** checks if a Wigner function has one value that occurs only once and reports the phase space point where that value is taken on.

```
In[98]:= v₀ = findOrigin[wigner[sic[5]]]
Out[98]= {{2}₅, 0}
```

The next line shows how it looks like if **`findOrigin`** fails to locate a unique point

```
In[99]:= findOrigin[wigner[W[{0,0}]]]

findOrigin :: AmbiguousOrigin : Can't locate origin : {{25, 1/5}}
```

We have found an element of the Clifford group which should admit **`sic[5]`** as an eigenvector...

```
In[100]:= a = (IdentityMatrix[2] - A).v₀
Out[100]= {{2}₅, {2}₅}

In[101]:= (W[a] ** μ[S] ** sic[5]) ~prop~ (sic[5])
Out[101]= True
```

...and indeed it does. The binary relation **`~prop~`** tests vectors or operators for proportionality:

```
In[102]:= X[1,1]~prop~ - X[1,1]
Out[102]= True
```

The matrix we just found complies with Zauner's conjecture. Can we discover anything surprising?

```
In[103]:= qInit[1,7]

In[104]:= MatrixForm /@ (autos = findAutomorphisms[sic[7]])

testAutomorphism :: unexpectedDet : {{0,{6}7},{{6}7,{2}7}} has determinant {6}7

testAutomorphism :: unexpectedDet : {{{2}7,{2}7},{{2}7,{5}7}}hasdeterminant{6}7

testAutomorphism :: unexpectedDet : {{{5}7,{6}7},{{6}7,0}} has determinant {6}7
Out[104]=  {  (   0     {6}7 ) , ( {1}7   {5}7 ) , ( {2}7   {2}7 ) ,
              ( {6}7   {2}7 )   ( {5}7   {5}7 )   ( {2}7   {5}7 )
              ( {5}7   {2}7 ) , ( {5}7   {6}7 ) }
              ( {2}7   {1}7 )   ( {6}7    0   )
```

The function **findAutomorphisms[]** performs some 'sanity checking' on its findings and warns that some symmetries it found correspond to linear transformations with determinant 6=-1 (mod 7). They are *anti-symplectic* rather then symplectic matrices.

```
In[105]:= A = autos[[1]];

In[106]:= A.A //MatrixForm
Out[106]= ( {1}7   {5}7 )
          ( {5}7   {5}7 )

In[107]:= MatrixPower[A,3] //MatrixForm
Out[107]= ( {2}7   {2}7 )
          ( {2}7   {5}7 )

In[108]:= MatrixPower[A,6] //MatrixForm
Out[108]= ( {1}7    0   )
          (  0     {1}7 )
```

The automorphism group is cyclic of order six. We conclude that the usual order-three symmetry group that seems to be present in all dimensions has an anti-symplectic 'root' in dimension 7. It is not hard to see that the metaplectic representation on a two-dimensional vector space can be extended to cover anti-symplectic transformations, if one allows for anti-*unitary* operators.

Using the described method, we have verified the compatibility of Renes' numerical fiducial states with Zauner's conjecture for all prime dimensions between 5 and 43.

After this work had been conducted, the compliance of Renes's fiducial states with Zauner's conjecture has been verified by Appleby [34] using different techniques.

Part II

Equivalence Relations Among Stabilizer Codes

9 Introduction

In quantum information theory it is natural to regard two multi-particle states as *equivalent* if they can be mapped onto each other by a local unitary operation. However, the task of deciding whether or not two given quantum states are equivalent in that sense is far from easy. For the special case of stabilizer states, there is a second notion of locality which is formulated in terms of their description as subspaces of a phase space $\mathbb{F}_d^{2n}$. Two stabilizer states are called *local Clifford* (LC) equivalent if they are related by the action of a local Clifford operation. Clearly (see Sections 4.5 and 5), this is the case if and only if their associated isotropic spaces can be converted into each other by a local symplectic mapping. A question that has attracted some attention in the literature is whether the two described definitions of locality agree: does local unitary (LU) equivalence imply LC equivalence? The second half of this thesis is devoted to finding a partial solution to this problem for the special case of binary states. The problem has some history which can be found in Ref. [27, 22, 23, 24, 25].

The purpose of this first section is to develop some notions and tools for discussing locality relations between stabilizer states. We start with an analysis of the space of hermitian operators and their transformation properties under conjugation by local unitary mappings. Some of the ideas and definitions in the following section are taken from Ref. [28, 27] Since we will be concerned only with binary systems, $\mathbb{F}$ means $\mathbb{F}_2$ for the rest of the thesis.

The four-dimensional real vector space H of hermitian operators on $\mathbb{C}^2$ is spanned by the Weyl operators

$$\begin{aligned} \{w(0,0), w(0,1), w(1,1), w(1,0)\} &= \{\sigma_0, \cdots, \sigma_3\} \qquad (136) \\ &= \{\mathbb{1}, X, Y, Z\} \qquad (137) \end{aligned}$$

The Hilbert-Schmidt inner product

$$(\rho, \sigma) = \frac{1}{2^n} \operatorname{tr}(\rho\sigma) \qquad (138)$$

turns H into an orthogonal vector space. To emphasize the role of H as an orthogonal vector space, we adopt a bra-ket-type notation for its elements by setting

$$\sigma_i \mapsto |i\rangle\rangle \qquad (139)$$

for $i \in \{0, \cdots, 3\}$. As H possess an inner product, dual vectors are well-defined and denoted as 'bra's:

$$\langle\langle\rho| := (\rho, \cdot). \qquad (140)$$

Additionally, it will prove useful to talk about vectors of H in terms of their coordinates with respect to the orthonormal basis (139). For a vector $|\rho\rangle\rangle$ we define

$$\rho^i := \langle\langle i|\rho\rangle\rangle = (\sigma_i, \rho). \qquad (141)$$

Clearly,

$$|\rho\rangle\rangle = \sum_i \rho^i |i\rangle\rangle. \qquad (142)$$

The function

$$i \mapsto \rho^i \qquad (143)$$

is nothing else but the *characteristic function* of $|\rho\rangle\!\rangle$. We write the coordinates of bras with respect to the dual basis $\{\langle\!\langle i|\}_i$ using lower indices:

$$\langle\!\langle \rho| = \sum_i \rho_i \langle\!\langle i|. \tag{144}$$

However, it is easy to see that they coincide

$$\rho_i = \rho^i. \tag{145}$$

Conjugation by a unitary operator U induces a unimodular orthogonal mapping $R(U)$ in H via the relation

$$U\sigma_i U^\dagger \quad = \quad \sum_j R^i{}_j \sigma_j. \tag{146}$$

What is more, *all* orthogonal matrices $R \in SO(3)$ can be obtained this way. See [29] for detailed formulas. Because σ_0 is fixed under conjugation, R takes on the form

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & r^1_1 & r^1_2 & r^1_3 \\ 0 & r^2_1 & r^2_2 & r^2_3 \\ 0 & r^3_1 & r^3_2 & r^3_3 \end{pmatrix} \tag{147}$$

where $r = (r^i{}_j)$ is a three-by-three orthogonal mapping. We have three ways of looking at the transformation:

$$\begin{aligned} \rho' &= U\rho U^\dagger \\ |\rho'\rangle\!\rangle &= R(U)|\rho\rangle\!\rangle \\ \rho^{i'} &= \rho^i R^{i'}{}_i \end{aligned} \tag{148}$$

Here, we have adopted the bad habit of general relativitists to mark the transformed version of a vector by priming its indices. Also, Einstein's summation convention applies.

The generalization to tensor products $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ is straightforward.

The set

$$\{|m\rangle\!\rangle := w(m)|m \in \mathbb{F}^{2n}\} \tag{149}$$

forms a basis in the space of hermitian operators on $\mathcal{H}$. The characteristic function becomes

$$\begin{aligned} |\rho\rangle\!\rangle &= \sum_{m\in\mathbb{F}^{2n}} \rho^m |m\rangle\!\rangle \\ &= \sum_{i_1,\cdots,i_n} \rho^{i_1\cdots i_n} |i_1\rangle\!\rangle \otimes \cdots \otimes |i_n\rangle\!\rangle. \end{aligned} \tag{150}$$

The latter notation is more convenient when talking about transformation properties and should cause no confusion. Under conjugation with a local unitary mapping

$$U = U_1 \otimes \cdots \otimes U_n \tag{151}$$

$|\rho\rangle\rangle$ transforms as

$$\rho^{i'_1\cdots i'_n} = \rho^{i_1\cdots i_n} (R_1)^{i'_1}{}_{i_1} \cdots (R_n)^{i'_n}{}_{i_n}. \tag{152}$$

For a phase space vector $m \in \mathbb{F}^{2n}$, the *support of* m – $\operatorname{supp} m$ – is the set of systems where m is non-zero. We also need a term for the phase space points where a characteristic function is non-zero. However, in order to avoid confusion, we refrain from using the word *support* for this set too. Instead, we speak of the *domain* of a phase space function. The domain of a vector $\operatorname{dom}|\rho\rangle\rangle$ of H is defined via its characteristic function:

$$\operatorname{dom}|\rho\rangle\rangle := \operatorname{dom}\rho^{\cdot} := \{m|\rho^m \neq 0\}. \tag{153}$$

If B is a subset of $\mathbb{F}^{2n}$, then $\operatorname{supp} B$ is the set $\{\operatorname{supp} b|b \in B\}$, as one would expect.

Two more definitions are in place. Consider a set of systems $\omega \subset \{1,\cdots,n\}$. By $\langle i_1,\cdots,i_{|\omega|}\rangle_\omega$ we denote the phase space vector that takes on the values i_1 to $i_{|\omega|}$ on the systems in ω and zero elsewhere. Conversely, $\pi_\omega(m)$ is the restriction of $m \in \mathbb{F}^{2n}$ to ω. $\pi_i(m)$ is the value of m on the ith system.

9.1 Stabilizer Codes

Fix an isotropic subspace M of V and a basis $\{m_i\}_i$ of M. Using the definition of $s(\cdot)$ from Section 5, we define

$$w_M(m) = s(m)w(m). \tag{154}$$

It is now easily checked that

$$w_M(m_1 + m_2) = w_M(m_1)w_M(m_2) \tag{155}$$

for $m_1, m_2 \in M$ and thus the representation $m \mapsto w_M(m)$ is faithful. The set $\{w_M(m)|m \in M\}$ is an orthonormal basis in the space of all hermitian operators whose domain is contained in M. If $|\rho\rangle\rangle$ is such an operator, its expansion reads

$$|\rho\rangle\rangle = \sum_{m\in M} \rho_M^m w_M(m) \tag{156}$$

where the function $m \mapsto \rho_M^{\cdot}$ is called the M*-characteristic function* of $|\rho\rangle\rangle$. It holds that

$$\rho_M^m = \rho^m s(m). \tag{157}$$

Of course, the representation $w_M(\cdot)$ depends on the choice of a basis $\{m_i\}$ of M. However, because that choice is completely arbitrary, we drop any reference to the basis in our notation. Once a representation $w_M(\cdot)$ is fixed, no phase ambiguity occurs in the correspondence of $w_M(m)$ to m, so we don't necessarily distinguish between phase space vectors and Weyl operators. For example, the symbol $XXYY\mathbb{1}$ might be an element of either $\mathbb{F}^{2n}$ or of H depending on the context.

For any d-dimensional isotropic subspace M of $\mathbb{F}^{2n}$, we define

$$\begin{aligned} |M\rangle\rangle &:= \frac{1}{2^d}\sum_{m\in M} w_M(m) && (158)\\ &= \frac{1}{2^d}\sum_{m\in M} s(m)|m\rangle\rangle. && (159)\end{aligned}$$

That is $|M\rangle\rangle$ is the projection operator onto the stabilizer code defined by M (see Section 5).

9.2 Invariant Subspaces

The fact that (147) does not mix non-trivial Weyl operators with the identity causes some subspaces of H to be invariant under the action of the local unitary group.

Definition 3 (Invariant subspaces) *Let ω be a subset of $\{1, \cdots, n\}$.*

1. *T_ω is the set of phase space vectors with support on ω. I.e.*

$$T_\omega := \{m \in \mathbb{F}^{2n} |\, \mathrm{supp}(m) = \omega\}$$

2. *$\mathcal{T}_\omega$ is the subspace of H spanned by the operators*

$$\{|m\rangle\rangle | m \in T_\omega\}.$$

3. *We define*

$$\hat{\mathcal{T}}_\omega = \sum_{m \in T_\omega} |m\rangle\rangle\langle\langle m|.$$

This is the projection operator onto $\mathcal{T}_\omega$.

Proof. *(of the claim made in point 3)* The range of $\hat{\mathcal{T}}_\omega$ is clearly $\mathcal{T}_\omega$. Further, $\hat{\mathcal{T}}_\omega$ is idempotent

$$\begin{aligned}
\hat{\mathcal{T}}_\omega \hat{\mathcal{T}}_\omega &= \sum_{m \in T_\omega} |m\rangle\rangle\langle\langle m| \sum_{m' \in T_\omega} |m'\rangle\rangle\langle\langle m'| \\
&= \sum_{m,m'} |m\rangle\rangle\langle\langle m|m'\rangle\rangle\langle\langle m| \\
&= \sum_{m} |m\rangle\rangle\langle\langle m| \\
&= \hat{\mathcal{T}}_\omega
\end{aligned}$$

and self-adjoint

$$\begin{aligned}
\langle\langle \rho | \hat{\mathcal{T}}_\omega \sigma \rangle\rangle &= \sum_m \langle\langle \rho | \Big(|m\rangle\rangle \langle\langle m|\sigma\rangle\rangle \Big) \\
&= \sum_m \langle\langle \rho|m\rangle\rangle\langle\langle m|\sigma\rangle\rangle \\
&= \sum_m \langle\langle \sigma|m\rangle\rangle\langle\langle m|\rho\rangle\rangle \\
&= \langle\langle \sigma | \hat{\mathcal{T}}_\omega \rho \rangle\rangle \\
&= \langle\langle \hat{\mathcal{T}}_\omega \rho | \sigma \rangle\rangle.
\end{aligned}$$

□

Lemma 4 [28] *The following holds.*

1. *$\mathcal{T}_\omega$ is preserved under the action of local unitaries.*

2. *$\hat{\mathcal{T}}_\omega$ commutes with local unitaries.*

3. *Let $|\rho\rangle\rangle$ be some element of H whose domain is contained in an isotropic space M. The effect of $\hat{\mathcal{T}}$ on the M-characteristic function is*

$$\left(\hat{\mathcal{T}}_\omega|\rho\rangle\rangle\right)_M^m = \rho_M^m \chi_{T_\omega}(m)$$

where χ_{T_ω} is the indicator function on T_ω:

$$\chi_{T_\omega}(m) := \begin{cases} 1 & m \in T_\omega \\ 0 & else \end{cases} .$$

Proof. The first assertion is proven in [28]. The second one follows immediately. Lastly,

$$\begin{aligned} \left(\hat{\mathcal{T}}_\omega|\rho\rangle\rangle\right)_M^m &= s(m)\langle\langle m|\hat{\mathcal{T}}_\omega|\rho\rangle\rangle \\ &= s(m)\langle\langle \rho|\hat{\mathcal{T}}_\omega|m\rangle\rangle, \end{aligned}$$

but

$$\hat{\mathcal{T}}_\omega|m\rangle\rangle = \begin{cases} |m\rangle\rangle & m \in T_\omega \\ 0 & else \end{cases} .$$

□

9.3 Composition

The standard operator product gives H the structure of an algebra. If $|\rho\rangle\rangle$ and $|\sigma\rangle\rangle$ are elements of H, we denote the their operator product as

$$|\rho\rangle\rangle \star |\sigma\rangle\rangle. \tag{160}$$

If two hermitian operators $|\rho\rangle\rangle$ and $|\sigma\rangle\rangle$ have support on a common isotropic space M, the M-characteristic function of their operator product is particularly simple.

Lemma 5 *Let $|\rho\rangle\rangle$ and $|\sigma\rangle\rangle$ be vectors on H. Let $\operatorname{dom}|\rho\rangle\rangle$ and $\operatorname{dom}|\sigma\rangle\rangle$ be subsets of a common isotropic space M. Then*

$$(|\rho\rangle\rangle \star |\sigma\rangle\rangle)_M^m = \sum_{\substack{m_1 \in \operatorname{dom}|\rho\rangle\rangle \\ m_2 \in \operatorname{dom}|\sigma\rangle\rangle \\ m_1 + m_2 = m}} \rho_1^m \sigma_2^m.$$

Proof.

$$\begin{aligned} |\rho\rangle\rangle \star |\sigma\rangle\rangle &= \left(\sum_{m1 \in \operatorname{dom}|\rho\rangle\rangle} \rho_M^{m_1} w_M(m_1)\right) \star \left(\sum_{m2 \in \operatorname{dom}|\sigma\rangle\rangle} \sigma_M^{m_2} w_M(m_2)\right) \\ &= \sum_{m1 \in \operatorname{dom}|\rho\rangle\rangle} \sum_{m2 \in \operatorname{dom}|\sigma\rangle\rangle} \rho_M^{m_1} \sigma_M^{m_2} w_M(m_1 + m_2). \end{aligned}$$

□

9.4 Traces

Having both kets and bras, we can construct operators on H. Indeed, it is easy to pinpoint a basis of the set of all operators on H:

$$\{|m\rangle\rangle\langle\langle n| \quad |m,n \in \mathbb{F}^{2n}\}. \tag{161}$$

Thus a basis expansion of an arbitrary operator A reads

$$A = \sum_{m,n\in\mathbb{F}^{2n}} A^{m}{}_{n}|m\rangle\rangle\langle\langle n| \tag{162}$$

For a subset ω of $\{1,\cdots,n\}$, we define the partial trace over ω in the same way it is commonly used in Hilbert spaces:

$$\mathrm{Tr}_\omega\, A := \sum_{m\in\mathbb{F}_2^{2|\omega|}} {}_\omega\langle\langle m|A|m\rangle\rangle_\omega. \tag{163}$$

In terms of the characteristic function, the partial trace is a *contraction*. For example, by tracing over the first k systems, we get

$$(\mathrm{Tr}_\omega\, A)^{i_{k+1}\cdots i_n}{}_{j_{k+1}\cdots j_n} = A^{l_1\cdots l_k i_{k+1}\cdots i_n}{}_{l_1\cdots l_k j_{k+1}\cdots j_n}. \tag{164}$$

The partial trace is compatible with LU-transforms in the sense that

$$\mathrm{Tr}_\omega\left(RAR^T\right) = R_{\bar\omega}\left(\mathrm{Tr}_\omega\, A\right) R_{\bar\omega}^T \tag{165}$$

as can be seen using (164).

The norm of $|\rho\rangle\rangle$ fulfills

$$\begin{aligned} |||\rho\rangle\rangle|| &:= \langle\langle\rho|\rho\rangle\rangle \\ &= \mathrm{Tr}\,|\rho\rangle\langle\rho| \\ &= \rho^{i_1\cdots i_n}\rho_{i_1\cdots in} \end{aligned} \tag{166}$$

9.5 Clifford Operations

A Clifford operation is a unitary operator which maps Weyl operators onto Weyl operators under conjugation. For a single system $n=1$, a Clifford operation thus corresponds to a *permutation* of the basis vectors $\{|X\rangle\rangle, |Y\rangle\rangle, |Z\rangle\rangle\}$ modulo phases. We see that a unitary mapping is a Clifford operation if and only if the matrix $r^i{}_j\,(U)$, as defined in (147), contains in each column exactly one entry different from zero. To satisfy orthogonality, this entry must be one of $\{-1,+1\}$. Such a matrix is called *monic* [27]. One can weaken the notion of a Clifford operation to describe unitaries that map, for example, only one of the three Weyl operators to another Weyl operator. This motivates the following.

Definition 6 (i-monoticity)

1. *An orthogonal three-by-three matrix r is called* i-monic *if it contains at least i columns with exactly one non-zero entry each.*

2. *If the jth column of a matrix r is monic, we say that r is σ_j*-monic.

3. *A unitary operation on one system is i-monic if it induces a i-monic matrix r via (147).*

4. *A local unitary mapping is i-monic if all its factors are.*

For example, an operation is X-monic if it maps the operator X to another Weyl operator under conjugation.

Lemma 7 (i-monic matrices)

1. *Any orthogonal 2-monic matrix is 3-monic.*

2. *Any orthogonal 1-monic matrix is LC-equivalent to*

$$\begin{pmatrix} cos\phi & -sin\phi & 0 \\ sin\phi & cos\phi & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

   The above matrix is induced by the Hilbert space operator

$$\begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}.$$

3. *Multiplication by 3-monic matrices preserves monoticity.*

Proof. To prove the first claim, use the standard vector product to compute the third column out of the two monic ones.

As for the second claim, let r be a 1-monic matrix. There exists a column, the kth say, which is monic. Let l denote the position of the non-zero entry of that column, so $|r^k{}_l| = 1$. There is a representation π of the symmetric group S_3 in terms of monic $SO(3)$-matrices [27] generated by

$$\begin{aligned} (12) \quad &\mapsto \quad \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \\ (23) \quad &\mapsto \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}. \end{aligned}$$

Modulo signs, this is the standard representation of the symmetric group by permutation matrices. Now let $\pi_{(3k)}$ and $\pi_{(3l)}$ by the images of the two-cycles $(3k)$ and $(3l)$ under π. Let

$$\tilde{r} := \pi_{(3k)} r \pi_{(3l)}. \tag{167}$$

It is easy to see that

$$\left|\tilde{r}^3_3\right| = |r^k{}_l| = 1 \tag{168}$$

which implies that both the third row and the third column of r must be monic due to orthogonality. Thus $\tilde{r}$ has the form

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}. \tag{169}$$

We can assume that the sign of $\hat{r}_3^3$ is positive, for else we multiply by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in SO(3). \tag{170}$$

Then the upper left block matrix must be an element of $SO(2)$ and any such matrix is of the form (2), as is well-known.

The generating unitary matrix can be found in Chapter 4.2 of [26].

Lastly, note that – modulo phases – left (right) multiplication with a 3-monic matrix only permutes columns (rows) of r and thus does not change monoticity. □

10 Blocks

Consider an isotropic space M. Using Lemma 4 it is not hard to see that

$$\begin{aligned} \operatorname{supp}\operatorname{dom}|M\rangle\rangle &= \{\omega | \exists m \in M, \operatorname{supp}(m) = \omega\} \\ &= \operatorname{supp} M \end{aligned}$$

is an LU-invariant. It is known [30] that these invariants are not powerful enough to discriminate LC-equivalence classes. Now, look at a subset B of M and define

$$|B\rangle\rangle = \sum_{b \in B} w_M(b).$$

Obviously, $\operatorname{supp}\operatorname{dom}|\rho\rangle\rangle = \operatorname{supp} B$ is an LU-invariant as well. But in general we can make little use of this information. Indeed, if R is a local unitary operator such that $R|M\rangle\rangle$ is another stabilizer code $|M'\rangle\rangle$, then there is no obvious interpretation of $\operatorname{dom} R|B\rangle\rangle$ in terms of elements of M' (remember that $|B\rangle\rangle$ does have such an interpretation with respect to M). However, there exists subsets of M such that $\operatorname{dom} R|B\rangle\rangle$ is a subset of M'. We call those sets the *blocks* of M. It turns out that the supports of the blocks of an isotropic space convey much information about the space itself. In the sections to come, we will define and explore the block structure of isotropic spaces.

Definition 8 (Blocks) *Let M be an isotropic space. The* blocks *of M are subsets of M defined recursively by the following rules.*

0. *M is a block.*
1. *If B is a block and ω is a subset of $\{1, \cdots, n\}$ then*

$$T_\omega \cap B$$

is a block, denoted by $r_1^\omega(B)$.

2. *If B_1 and B_2 are blocks then*
$$B_1 + B_2 := \{m_1 + m_2 | m_1 \in B_1, m_2 \in B_2\}$$
is a block, denoted as $r_2(B_1, B_2)$.

3. *If B_1 and B_2 are blocks then*
$$B_1 \cup B_2$$
is a block, denoted as $r_3(B_1, B_2)$.

4. *If B is a block then*
$$B \quad \setminus \quad T_\omega$$
is a block for every $\omega \subset \{1, \cdots, n\}$, denoted as $r_4^\omega(B)$.

In other words, a block is the result of any recursive applications of the functions r_i on M. For example, the set

$$B := \{m_1 + m_2 | m_i \in M, m_1 + m_2 \neq 0\} \tag{171}$$

can be written as

$$B = r(M) := r_4^{\{\emptyset\}}(r_2(M, M)) \tag{172}$$

and is thus manifestly a block.

Definition 9 (Block rules) *If B is a block of M and r is a composition of the functions $\{r_i\}_{i=1\cdots 4}$ (as in (172)) such that*

$$r(M) = B$$

then we say that r is the rule of *B.*

From the definition of a block, it is clear that such a (possibly non-unique) rule always exists.

Here is why blocks are important.

Theorem 10 (A family of LU-invariants) *Let $M \subset \mathbb{F}^{2n}$ be an isotropic space. Let r be the rule for some block of M. Then the function*

$$M \mapsto \operatorname{supp} r(M)$$

is an LU-invariant.

The rest of this section is devoted to the proof of the theorem.

Definition 11 (Block vectors) *Let M be an isotropic space. A vector $|\rho\rangle\rangle$ is called a* block vector *if*

1. *the domain of $|\rho\rangle\rangle$ is a block of M and*

2. *the M-characteristic function of $|\rho\rangle\rangle$ is non-negative.*

In the following paragraphs, we'll often speak of two block vectors at a time and assume implicitly that their respective domains are blocks of the *same* isotropic space. This should always be clear from the context.

We now prove that there exists a quantum analogue of blocks.

Lemma 12 (Operations on block vectors) *Let $|\rho\rangle\rangle$ and $|\sigma\rangle\rangle$ be block vectors. Let ω be a subset of $\{1, \cdots, n\}$.*

0. *Let M be a isotropic space. Then $|M\rangle\rangle$ is a block vector where* $\operatorname{dom}|M\rangle\rangle = M$.

1. *Let $|\rho\rangle\rangle$ be a block vector. Then*

$$\hat{r}_1^{\omega}(|\rho\rangle\rangle) := \hat{\mathcal{T}}_{\omega}|\rho\rangle\rangle$$

is a block vector where

$$\begin{aligned}\operatorname{dom}\hat{\mathcal{T}}_{\omega}B &= T_{\omega} \cap \operatorname{dom}|\rho\rangle\rangle \\ &= r_1^{\omega}(\operatorname{dom}|\rho\rangle\rangle).\end{aligned}$$

2. *Let $|\rho\rangle\rangle$ and $|\sigma\rangle\rangle$ be block vectors. Then*

$$\hat{r}_2(|\rho\rangle\rangle, |\sigma\rangle\rangle) := |\rho\rangle\rangle \star |\sigma\rangle\rangle$$

is a block vector where

$$\begin{aligned}\operatorname{dom}(|\rho\rangle\rangle \star |\sigma\rangle\rangle) &= (\operatorname{dom}|\rho\rangle\rangle) + (\operatorname{dom}|\sigma\rangle\rangle) \\ &= r_2(\operatorname{dom}|\rho\rangle\rangle, \operatorname{dom}|\sigma\rangle\rangle).\end{aligned}$$

3. *Let $|\rho\rangle\rangle$ and $|\sigma\rangle\rangle$ be block vectors. Then*

$$\hat{r}_3(|\rho\rangle\rangle, |\sigma\rangle\rangle) := |\rho\rangle\rangle + |\sigma\rangle\rangle$$

is a block vector where

$$\begin{aligned}\operatorname{dom}(|\rho\rangle\rangle + |\sigma\rangle\rangle) &= \operatorname{dom}|\rho\rangle\rangle \cup \operatorname{dom}|\sigma\rangle\rangle \\ &= r_3(\operatorname{dom}|\rho\rangle\rangle, \operatorname{dom}|\sigma\rangle\rangle).\end{aligned}$$

4. *Let $|\rho\rangle\rangle$ be a block vector. Then*

$$\hat{r}_4(|\rho\rangle\rangle) := \left(\mathbb{1} - \hat{\mathcal{T}}_{\omega}\right)|\rho\rangle\rangle$$

is a block vector where

$$\operatorname{dom}|\rho\rangle\rangle \setminus T_{\omega} = r_4^{\omega}(\operatorname{dom}|\rho\rangle\rangle).$$

Further, let B be a block of M, and let be r a rule such that $r(M) = B$. Let $\hat{r}$ be the operator obtained from r by replacing each rule r_i by $\hat{r}_i$. Then

$$\operatorname{dom}\hat{r}(|M\rangle\rangle) = r(M).$$

Proof. Let us look at the points in turn.

0. $\operatorname{dom}|M\rangle\!\rangle = M$ which is a block of M by Definition 8.0. Further, the M-characteristic function of $|M\rangle\!\rangle$ is non-negative (and even constant):

$$\begin{aligned}\langle\!\langle m|s(m)|M\rangle\!\rangle &= \langle\!\langle m|s(m)\sum_{m'} s(m')|m'\rangle\!\rangle \\ &= s(m)s(m')\sum_{m'}\langle\!\langle m|m'\rangle\!\rangle \\ &= s(m)^2 \\ &= 1\end{aligned}$$

1. By Lemma 4 the M-characteristic function of $\hat{\mathcal{T}}_\omega|\rho\rangle\!\rangle$ is pointwise non-negative and its domain is $\operatorname{dom}|\rho\rangle\!\rangle \cap T_\omega$. The latter set is a block of M because $\operatorname{dom}|\rho\rangle\!\rangle$ is and thus the rule from Definition 8.1 is applicable.

2. Consider the formula in Lemma 5. If for a given m, there exist $m_1 \in \operatorname{dom}|\rho\rangle\!\rangle$ and $m_2 \in \operatorname{dom}|\sigma\rangle\!\rangle$ such that $m_1+m_2 = m$ then $(|\rho\rangle\!\rangle+|\sigma\rangle\!\rangle)_M^m$ is strictly positive because all summands in the above mentioned formula are strictly positive. Thus $|\rho\rangle\!\rangle + |\sigma\rangle\!\rangle$ has the claimed domain and its M-characteristic function is non-negative. The claim is proven by the use of Definition 8.2.

The remaining points 3. and 4. can be verified analogously.

To prove the last statement, one only needs to compare the formulas for the domains of the block vectors with the corresponding expressions in Definition 8. □

Definition 13 (Rule Operators) *If B is a block of M and*

$$B = r(M)$$

for some rule r, we define

$$|B\rangle\!\rangle := \hat{r}|M\rangle\!\rangle,$$

and call $\hat{r}$ the rule operator *corresponding to r.*

The following simple observation is crucial.

Lemma 14 *Rule operators commute with local unitaries:*

$$\hat{r}R|M\rangle\!\rangle = R\hat{r}|M\rangle\!\rangle,$$

for each local unitary operator R.

Proof. The fact that the projections $\hat{\mathcal{T}}_\omega$ commute with LU operators has been shown in Lemma 4. Now recall that LU operators act on H *by conjugation* (see (146)). Thus the application of LU operators commutes with composition, addition and subtraction of vectors of H. But these are the operations which the $\hat{r}_i$ are built of. □

We can now proof the central theorem of this section.

Proof. *(of Theorem 10).* Let M be an isotropic space and let r be the rule for some block of M. Let $\omega \subset \{1, \cdots, n\}$.

$$\begin{aligned} \omega \in \operatorname{supp} r(M) &\Leftrightarrow \omega \in \operatorname{supp} \hat{r}|M\rangle\rangle \\ &\Leftrightarrow \{m \in \operatorname{dom} \hat{r}|M\rangle\rangle \,|\, \operatorname{supp}(m) = \omega\} \neq \{\emptyset\} \\ &\Leftrightarrow \hat{\mathcal{T}}_\omega \hat{r}|M\rangle\rangle \neq 0. \end{aligned}$$

The last line is LU-invariant by Lemma 4 and Lemma 14. □

There is a particular type of blocks that will prove useful in the sequel.

Definition 15 *We define the rule*

$$\begin{aligned} d(B) &:= (B + B) \setminus T_{\{\emptyset\}} \\ &= \{b_1 + b_2 | b_1, b_2 \in B \wedge b_1 + b_2 \neq 0\}. \end{aligned}$$

11 A Restriction on LU Operators

Not every local unitary operator can map a stabilizer code to another one. We will now explore the restrictions imposed on LU operators by the requirement that they do possess this capability.

Lemma 16 *Let M be an isotropic space, let B be a block of M. Let R be a local unitary mapping such that $R|M\rangle\rangle$ is again a stabilizer code $|M'\rangle\rangle$.*

If $B = \{m\}$ is of order 1 then R is 1-monic on $\operatorname{supp} m$.

Proof. Let r be the rule corresponding to B. The main task is to show that $B' := r(M')$ has again order one. Using Definition 15 it is easy to see that

$$d(B) = \{\emptyset\}.$$

That is, $\operatorname{supp} d(B) = \operatorname{supp} d(B') = \{\emptyset\}$. But $\operatorname{supp} d(A) = \{\emptyset\}$ for some block A only if $|A| = 1$ because if A had two distinct elements m_1 and m_2, then $0 \neq m_1 + m_2 \in d(A)$ by Definition 15.

Now, consider $|B\rangle\rangle$ and $|B'\rangle\rangle = R|B\rangle\rangle$. We know that the respective domain of each of these operators is just one phase space point. Thus they are proportional to the Weyl operators $|m\rangle\rangle$ and $|m'\rangle\rangle$ respectively. But because both Weyl operators and R are local by definition,

$$R_i|\pi_i(m)\rangle\rangle = |\pi_i(m')\rangle\rangle$$

for all $i \in \operatorname{supp} m$. It follows that R_i is $\pi_i(m)$-monic. □

The above result can be slightly generalized.

Lemma 17 *Let M be an isotropic space, let B be a block of M. Let R be a local unitary mapping such that $R|M\rangle\rangle$ is again a stabilizer code $|M'\rangle\rangle$.*

If for some system i it holds that $|\pi_i(B)| = 1$ and $\pi_i(B) \neq \{\mathbb{1}\}$, then R_i is 1-monic.

Proof. As in the last proof, we see that $|\pi_i(B')|$ must be one. Indeed, no element ω of $B+B$ contains the system i and hence the same holds for the elements of $B'+B'$. Again, if there were two vectors m_1 and m_2 in B' that differed on i, then $i \in \operatorname{supp}(m_1+m_2)$ which is a contradiction.

Now, let $\{W\} = \pi_i(B)$. It is easy to see that

$$\begin{aligned} |B\rangle\!\rangle &= |W\rangle\!\rangle_i \otimes |V\rangle\!\rangle \\ |B'\rangle\!\rangle &= |W'\rangle\!\rangle_i \otimes |V'\rangle\!\rangle \end{aligned}$$

for some vectors $|V\rangle\!\rangle, |V'\rangle\!\rangle$. R_i maps $|W\rangle\!\rangle$ to $\pm|W'\rangle\!\rangle$ and is thus W-monic. □

Next, we will consider a type of blocks which imposes an even stronger restriction on R.

Definition 18 (See [27]). *A block B is said to be of* Rains' type *if*

1. *B is of order three,*
2. *all elements have support on the same set of systems ω,*
3. *for any system $i \in \omega$, $|\pi_i(B)| = 3$, that is, all elements of B are pairwise different on any system,*
4. *$|\omega| > 2$.*

It is easy to see that any block of Rains' type is LC-equivalent to

$$\left\{X^{|\omega|}, Y^{|\omega|}, Z^{|\omega|}\right\}. \tag{173}$$

Lemma 19 *Let M be an isotropic space, let B be a block of M. Let R be a local unitary mapping such that $R|M\rangle\!\rangle$ is again a stabilizer code $|M'\rangle\!\rangle$.*

If $B = r(M)$ is of Rains' type then $B' := r(M')$ is again of Rains' type.

Proof. There is no loss of generality in assuming that B is of the form (173).

Using Definition 15 one finds by direct calculation that

$$d(B) = B \tag{174}$$

and hence

$$\operatorname{supp} d(B) = \operatorname{supp} d(B') = \omega. \tag{175}$$

We can now show that any two distinct elements m_1, m_2 of B' differ on all systems of ω. Indeed, let us assume to the contrary, that there exists a system $i \in \omega$ such that m_1 equals m_2 on i. Then $i \notin \operatorname{supp}(m_1+m_2)$ and thus

$$\operatorname{supp}(m_1+m_2) \neq \omega.$$

From Definition 15 we know that

$$m_1 + m_2 \in d(B')$$

and thus

$$\operatorname{supp}(m_1+m_2) \in \operatorname{supp} d(B')$$

which contradicts (175).

We go on to show that $|B'| = 3$ by ruling out all other cases.

1. Assume $|B'| > 3$. Then on any system i at least two elements of B' must be equal (for there are only three different values to choose from). But this is impossible from the last paragraph.

2. If on the other hand $|B'| = 0$ or $|B'| = 1$. Then $d(B') = \{\emptyset\}$ again contradicting (175).

3. Lastly, if $|B'| = 2$ then B' is LC-equivalent to

   $$\{X^{|\omega|}, Z^{|\omega|}\}$$

   and we see that

   $$d(B') \sim_{LC} \{Y^{|\omega|}\}.$$

   Thus

   $$d^2(B') = \{\emptyset\} \tag{176}$$

   (again by Definition 15). But (174) shows that

   $$d^2(B) = d(B) = B$$

   implying that

   $$\omega = \operatorname{supp} d^2(B) = \operatorname{supp} d^2(B')$$

   which contradicts (176).

B' is therefore a block of order three and any two vectors in B' differ on all systems. But any such block is LC-equivalent to (173). □

Lemma 20 *Let M be an isotropic space, let B be a block of M. Let R be a local unitary mapping such that $R|M\rangle\rangle$ is again a stabilizer code $|M'\rangle\rangle$.*

If $B = r(M)$ is of Rains' type then R is 3-monic on ω.

Proof. By Lemma 19 we know that there exists an LC-mapping L such that $LB' = B$. Because of Lemma 6, $\mu(L)R$ is 3-monic if and only if R is and hence there is no loss of generality in assuming that R is such that $B = B'$. Further, we assume that B is of the form (173).

The rest of the proof is due to Rains (Theorem 13 in [27]). We repeat it here for the sake of completeness, in order to translate it into our language and to make some slight generalizations.

Let

$$\begin{aligned} |\rho\rangle\rangle &:= |B\rangle\rangle \\ |\rho'\rangle\rangle &:= R|B\rangle\rangle \end{aligned}$$

Recall that any vector $|\sigma\rangle\rangle$ with domain B has the form

$$\begin{aligned} |\sigma\rangle\rangle \quad = \quad & \sigma^{X\cdots X}|X\rangle\rangle_1 \otimes \cdots \otimes |X\rangle\rangle_{|\omega|} + \\ & \sigma^{Y\cdots Y}|Y\rangle\rangle_1 \otimes \cdots \otimes |Y\rangle\rangle_{|\omega|} + \\ & \sigma^{Z\cdots Z}|Z\rangle\rangle_1 \otimes \cdots \otimes |Z\rangle\rangle_{|\omega|}. \end{aligned}$$

Now let $\beta = \{1,2\}, \gamma = \{3, \cdots, |\omega|\}$ and consider the operator

$$\begin{aligned}
\rho'^{X\cdots X}|X\rangle\!\rangle_{22}\langle\!\langle X| &= {}_1\langle\!\langle X| \left[\mathrm{Tr}_\gamma |\rho'\rangle\!\rangle\langle\!\langle\rho'|\right] |X\rangle\!\rangle_1 \\
&= {}_1\langle\!\langle X| \left[\mathrm{Tr}_\gamma R|\rho\rangle\!\rangle\langle\!\langle\rho|R^T\right] |X\rangle\!\rangle_1 \\
&= {}_1\langle\!\langle X| \left[\mathrm{Tr}_\gamma R_\beta|\rho\rangle\!\rangle\langle\!\langle\rho|R_\beta^T\right] |X\rangle\!\rangle_1 \\
&= R_2 \left({}_1\langle\!\langle X| \left[R_1 \,\mathrm{Tr}_\gamma |\rho\rangle\!\rangle\langle\!\langle\rho|R_1^T\right] |X\rangle\!\rangle_1\right) R_2^T.
\end{aligned}$$

From the first line it is clear that the rank of the operator is 1. Thus

$$\begin{aligned}
1 &= \mathrm{rank}\, R_2 \left({}_1\langle\!\langle X| \left[R_1 \,\mathrm{Tr}_\gamma |\rho\rangle\!\rangle\langle\!\langle\rho|R_1^T\right] |X\rangle\!\rangle_1\right) R_2^T \\
&= \mathrm{rank}\, {}_1\langle\!\langle X| \left[R_1 \,\mathrm{Tr}_\gamma |\rho\rangle\!\rangle\langle\!\langle\rho|R_1^T\right] |X\rangle\!\rangle_1.
\end{aligned}$$

But

$$\begin{aligned}
\mathrm{Tr}_\gamma |\rho\rangle\!\rangle\langle\!\langle\rho| = \;& \rho^{X\cdots X}|XX\rangle\!\rangle\langle\!\langle XX| + \\
& \rho^{Y\cdots Y}|YY\rangle\!\rangle\langle\!\langle YY| + \\
& \rho^{Z\cdots Z}|ZZ\rangle\!\rangle\langle\!\langle ZZ|
\end{aligned}$$

and thus

$$\begin{aligned}
{}_1\langle\!\langle X| \left[R_1 \,\mathrm{Tr}_\beta |\rho\rangle\!\rangle\langle\!\langle\rho|R_1^T\right] |X\rangle\!\rangle_1 = \;& (R_1)^X{}_X \;\rho^{X\cdots X}|X\rangle\!\rangle\langle\!\langle X| + \\
& (R_1)^X{}_Y \;\rho^{Y\cdots Y}|Y\rangle\!\rangle\langle\!\langle Y| + \\
& (R_1)^X{}_Z \;\rho^{Z\cdots Z}|Z\rangle\!\rangle\langle\!\langle Z|
\end{aligned}$$

which has rank 1 if and only if $(R_1)^X{}_\cdot$ is monic. The same argument can be repeated with ${}_1\langle\!\langle X| \cdot |X\rangle\!\rangle_1$ replaced by the corresponding expressions involving Y and Z and hence R_1 must be 3-monic. The same holds for all systems. □

Part of the definition of a block of Rains' type was that $|\omega| > 2$. This is no restriction of generality as the following lemma shows.

Lemma 21 *Let M be an isotropic space. If $|M\rangle\!\rangle$ is fully entangled, then there is no subset in M which fulfills Rains' condition except that $|\omega| = 2$.*

Proof. Let $M \subset \mathbb{F}^{2n}$ be an isotropic space and let $B \subset M$ be a subset as stated in the lemma. In compliance with (173), we assume that B has the form

$$\{\langle XX\rangle_\omega, \langle YY\rangle_\omega, \langle ZZ\rangle_\omega\}. \tag{177}$$

Two phase space vectors commute if and only if they are non-zero and different on an even number of systems. Thus any vector which commutes with the elements in B must be XX, YY, ZZ or $\mathbb{1}\mathbb{1}$ on ω. Therefore, M is spanned by B and the set of vectors which equal $\mathbb{1}\mathbb{1}$ on ω. Denote the latter set by A. Then

$$M = A \oplus B$$

and hence

$$|M\rangle\!\rangle = |A\rangle\!\rangle \otimes |B\rangle\!\rangle.$$

The expression is well-defined because both A and $B \cup \{0\}$ are isotropic spaces. We conclude that $|M\rangle\!\rangle$ is not fully entangled. □

Definition 22 (Simple blocks) *B is a* simple block *if $|\operatorname{supp} B| = 1$, that is, if all its elements have the same support.*

We now state the central theorem of this section. Here, and in the sequel, we'll always assume that for any isotropic space M, $\dim M > 2$, to rule out some special cases.

Theorem 23 (Restriction on LU mappings) *Let M be an isotropic space. If R is a local unitary operator such that $R|M\rangle\rangle$ is again a stabilizer code $|M'\rangle\rangle$, then R is 1-monic.*

Proof. Fix a system i. We will prove the following assertion by induction on $|\omega|$:

If M contains a simple block B where $\operatorname{supp}(B) = \omega$ and $i \in \omega$ then R_i is 1-monic.

If $|\omega| = 1$ then B is one of X, Y or Z on the ith system. R_i is then 1-monic by Lemma 16. Now suppose $|\omega| > 1$. Let's treat three different cases in turn:

1. $|\pi_i(B)| = 1$. Then R_i is $\pi_i(B)$-monic by (17) and we are done.
2. $|\pi_i(B)| = 2$. There exist two elements $m_1, m_2 \in B$ such that $\pi_i(m_1) \neq \pi_i(m_2)$ and hence
$$i \in \omega' := \operatorname{supp}(m_1 + m_2). \tag{178}$$
Clearly then,
$$A := (B + B) \cap \mathcal{T}_{\omega'} \tag{179}$$
is a simple block of M. Further, $\pi_i(A) = \pi_i(m_1 + m_2)$, thus $|\pi_i(A)| = 1$ and we have reduced this case to the previous one.
3. $|\pi_i(B) = 3|$. We know there exist elements m_1, m_2, m_3 of B such that
$$\begin{aligned} \pi_i(m_1) &= X \\ \pi_i(m_2) &= Y \\ \pi_i(m_3) &= Z. \end{aligned}$$
We again distinguish two cases.
   (a) Suppose among those three vectors there exists a pair $\langle m_k, m_l \rangle$ such that $\omega' := \operatorname{supp}(m_k + m_l)$ is a proper subset of ω. Define A as in (179). A is a simple block, $i \in \operatorname{supp}(A)$ and further $|\operatorname{supp} A| = |\omega'| < |\omega|$ and thus the existence of A is sufficient to conclude that R_i is 1-monic by the induction hypothesis.
   (b) If the condition for the last case can not be fulfilled then any two vectors of $\{m_1, m_2, m_3\}$ differ on all systems. Thus $\{m_1, m_2, m_3\}$ is LC-equivalent to (173) and there is no loss of generality in assuming that
$$\begin{aligned} m_1 &= X^{|\omega|} \\ m_2 &= Y^{|\omega|} \\ m_3 &= Z^{|\omega|}. \end{aligned}$$
   If $|B| = 3$ then R_ω is 3-monic by Lemmas 20 and 21 and nothing remains to be shown. So assume that $|B| > 3$. There exists a vector $m_4 \in B$

distinct from m_1, m_2, m_3. Let's for now assume that $\pi_i(m_4) = X$ (all other cases can be treated in an analogue way). There must exist a proper subset ω' of ω such that $\pi_{\omega'}(m_4)$ equals either $Y^{|\omega'|}$ or $Z^{|\omega'|}$ for else m_4 would equal m_1. Define A as in (179) and proceed by induction as in 3a.

Finally, note that for any system i there exists a simple block B such that $i \in \operatorname{supp} B$. Take any element m of M such that $i \in \operatorname{supp} m$. Then

$$T_{\operatorname{supp} m} M$$

is such a simple block. □

We have seen that the presence of blocks of order one and of Rains' type are sufficient to ensure that only 1-monic unitaries can map stabilizer codes to stabilizer codes. It is natural to suspect that blocks of higher orders impose even stronger restrictions on the unitaries and that – except for the well-known Bell state case – only Clifford operations can map stabilizer codes to stabilizer codes. However, this is not so as the following example shows.

12 An Example: GHZ-State on Four Systems

We consider the GHZ-State on four systems:

$$|GHZ\rangle = |0000\rangle + |1111\rangle. \tag{180}$$

It is a stabilizer state corresponding to the isotropic space M spanned by the columns of the matrix

$$\begin{pmatrix} z & . & . & x \\ z & z & . & x \\ . & z & z & x \\ . & . & z & x \end{pmatrix}. \tag{181}$$

We have replaced '0' by a dot in order to underline the support of the vectors. The entire isotropic space is

$$\begin{pmatrix} . & . & . & . & x & x & x & x & z & z & z & z & y & y & y & y \\ . & . & z & z & x & x & y & y & . & . & z & z & x & x & y & y \\ . & z & . & z & x & y & x & y & . & z & . & z & x & y & x & y \\ . & z & z & . & x & y & y & x & z & . & . & z & y & x & x & y \end{pmatrix}. \tag{182}$$

We clearly see that the blocks of order one guarantee the z-monoticity. But we have no tool at hand that would tell us whether or not the block

$$\begin{pmatrix} x & x & x & x & y & z & y & y & y \\ x & x & y & y & y & z & y & x & x \\ x & y & y & x & x & z & y & y & x \\ x & y & x & y & x & z & y & x & y \end{pmatrix} \tag{183}$$

can be mapped to the block of another stabilizer state by a non-Clifford operation. However, the structure of the Hilbert space vector $|GHZ\rangle$ is much easier. Indeed,

$$\begin{aligned} & \begin{pmatrix} e^{-i\phi_1/2} & 0 \\ 0 & e^{i\phi_2/2} \end{pmatrix} \cdots \begin{pmatrix} e^{-i\phi_4/2} & 0 \\ 0 & e^{i\phi_4/2} \end{pmatrix} |GHZ\rangle \\ \propto \quad & e^{-i(\phi_1+\cdots+\phi_4)}|0000\rangle + |1111\rangle \end{aligned} \tag{184}$$

which equals $|GHZ\rangle$ if and only if the phases ϕ_i sum to unity. So we have found a $(n-1)$-parameter family of non-Clifford automorphisms of the GHZ-state and thus of (183). It is not hard to see that all local unitary automorphisms of the GHZ state are contained in this group.

The result can easily be generalized to any GHZ-state on an even number of systems.

13 LU=LC for Blocks

In Lemma 6 we have shown that any 1-monic LU operator R is LC-equivalent to an operator $\tilde{R} = \mu(L_2)R\mu(L_1)$ which fixes Z. Therefore, $R|M\rangle\rangle$ is another stabilizer code $|M'\rangle\rangle$ if and only if

$$\tilde{R}|L_1 M\rangle\rangle = |L_2^{-1} M'\rangle\rangle. \tag{185}$$

Clearly, M and M' are LC-equivalent if and only if $L_1 M$ and $L_2^{-1} M'$ are. This motivates the following definition.

Definition 24 (Reductions)

1. *The* reduced local unitary group RLU *is defined to be*

   $$\{R \in LU | R_i |Z\rangle\rangle = |Z\rangle\rangle\}.$$

   That is, each factor of an operator in RLU keeps Z fixed. RLC is defined similarly.

2. *For a phase space vector $m \in \mathbb{F}^{2n}$, we define its* reduced support *to be the set of systems where m is X or Y:*

   $$\operatorname{supp}_R m := \{i | \pi(m) \in \{X, Y\}\}.$$

3. *Let $\beta_{\mathbb{1}}$ and β_Z be subsets of $\{1, \cdots, n\}$.*

   (a) $S_{\beta_{\mathbb{1}},\beta_Z}$ is the set of phase space vectors which are equal to $\mathbb{1}$ on $\beta_{\mathbb{1}}$ and equal to Z on β_Z.

   (b) $\hat{\mathcal{S}}_{\beta_{\mathbb{1}},\beta_Z}$ is the projection operator onto the space spanned by

   $$\{|m\rangle\rangle | m \in \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z}\}.$$

Having these terms at hand, we can formulate a corollary of the discussion at the beginning of the section.

Lemma 25 *$LU(M) = LC(M)$ for all isotropic spaces M if and only if $RLU(M) = RLC(M)$ for all such M.*

Proof. See discussion above. □

In the light of the last lemma, we will restrict our attention to the action of the reduced groups in the sequel. In order to suit this new situation, we now re-define the notion of a *block*. It is our hope that the confusion that arises due to giving a new meaning to an existing term is less than the confusion which the introduction of yet a new type of blocks would cause.

Definition 26 *Let M be an isotropic space. A subset B of M is a block of M if*

1. *B is a block in the sense of Definition 8*
2. *If B is a block, then*
$$\mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap B =: r_s^{(\beta_{\mathbb{1}},\beta_Z)}(B)$$
is a block for all subsets $\beta_{\mathbb{1}}, \beta_Z$ of $\{1, \cdots, n\}$.

The rule operator associated to r_s is

$$\hat{r}_s^{(\beta_{\mathbb{1}},\beta_Z)}|\rho\rangle\rangle = \hat{\mathcal{S}}_{\beta_{\mathbb{1}},\beta_Z}|\rho\rangle\rangle.$$

Lemma 27 *The function*
$$B \mapsto \operatorname{supp}(B)$$
is an RLU-invariant for all blocks B.

Proof. We omit the proof, which can be conducted along the same lines as the one in Section 10. □

A vector $m \in \mathbb{F}^{2n}$ which has trivial reduced support $\operatorname{supp}_R m = \{\emptyset\}$ is invariant under the action of the reduced groups. Further, consider two vectors m_1, m_2 with have the same reduced support. Their sum is an invariant vector because $\operatorname{supp}_R(m_1 + m_2) = \{\emptyset\}$. A re-occurring scheme in the next paragraphs will be to describe as many aspects of a block as possible in terms of invariant vectors.

Lemma 28 (Generated Subspaces) *Let B be a block of an isotropic space M. Then*

$$\langle B\rangle := \{\text{all linear combinations of elements of B}\}$$

is a block of M.

Proof.

$$\begin{aligned}\langle B\rangle &= (B \cup 0)^{+n} \\ &= (B \cup T_{\{\emptyset\}}(M))^{+n}.\end{aligned}$$

□

Definition 29 *A block B is called* primary *if*

$$B = \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap M.$$

If $\mathcal{B} \subset B$ generates a primary block B in the sense that

$$\mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap \langle\mathcal{B}\rangle = B$$

then $\mathcal{B}$ is called a basis *of B.*

Lemma 30 (Properties of Primary Blocks) *Let M be an isotropic space, let B be a block of M. Let $R \in RLU$ such that $R|M\rangle\rangle$ is again a stabilizer code $|M'\rangle\rangle$.*

If

$$B = \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap M.$$

is primary, then

1. $$|B'| = |B|.$$

2. $$\mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap \langle B \rangle \quad = \quad B$$

Proof.

1. Lemma 4 can easily be adopted to the new definition of a block. We then see that

$$2^d \left(\hat{\mathcal{S}}_{\beta_{\mathbb{1}},\beta_Z} |M\rangle\rangle \right)^m \quad = \quad \begin{cases} \pm 1 & m \in \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap M \\ 0 & else \end{cases}$$

   and thus

$$\begin{aligned} ||2^d \hat{\mathcal{S}}_{\beta_{\mathbb{1}},\beta_Z} |M\rangle\rangle|| &= |\mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap M| \\ &= |B| \end{aligned}$$

   by (166). The last statement is clearly LU-invariant.

2. Let $b \in B$. Clearly, $b \in \langle B \rangle$ and hence $b \in \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap \langle B \rangle$. Conversely, if $b \in \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap \langle B \rangle$ then $b \in M$ in particular and $b \in \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z}$, therefore $b \in B$.

□

The preceding lemma shows that each primary block has a basis.

Theorem 31 *Let M be an isotropic space, let B be a reduced block of M. Let $R \in RLU$ such that $R|M\rangle\rangle$ is again a stabilizer code $|M'\rangle\rangle$.*

If

$$B = \mathcal{S}_{\beta_{\mathbb{1}},\beta_Z} \cap M.$$

is primary, then B' is RLC-equivalent to B.

Proof. Let $\mathcal{B} = \{m_1, \cdots, m_d\}$ be a basis of B. The following set is another basis in B:

$$\mathcal{N} := \{m_1, \underbrace{m_2 + m_1}_{=:n_2}, \underbrace{m_3 + m_1}_{=:n_3}, \cdots, \underbrace{m_d + m_1}_{=:n_d}\}$$

The vector m_1 is the only element in $\mathcal{N}$ that has a non-trivial reduced support. In contrast, the vectors $\{n_i\}_{n=2\cdots d}$ are invariant and thus contained in M'. Because $\operatorname{supp}_R B$ is an RLU-invariant, there must exist at least one element n_1 in M' such that

$$\operatorname{supp}_R n_1 = \operatorname{supp}_R B.$$

Besides its support, we don't know anything about n_1 and the key observation is that we need not to. Indeed, irrespective of the details of n_1, it holds that

$$\{n_1, n_2, \cdots, n_d\} =: \mathcal{B}' \subset M'$$

is RLC-equivalent to

$$\{m_1, n_2, \cdots, n_d\} = \mathcal{B} \subset M.$$

This is because n_1 and m_1 are RLC-equivalent (any pair of vectors with same reduced support is) and the $n_i, i > 2$ are RLC-invariant. But then

$$\mathcal{S}_{\beta_1,\beta_Z} \cap \langle \mathcal{B} \rangle \sim_{LC} \mathcal{S}_{\beta_1,\beta_Z} \cap \langle \mathcal{B}' \rangle$$

The right-hand side is a subset of

$$\mathcal{S}_{\beta_1,\beta_Z} \cap M' = B'.$$

Hence B' contains a subset which is RLC-equivalent to B. But because of Lemma 30.1 this subset must be all of B'. □

14 The Next Step

Until now we have tried to tackle the LU-equivalence problem by dividing the isotropic spaces into 'building blocks' and solving the problem for these smaller constituents. This programme has been completed, because any isotropic space is the disjoint union of its primary blocks. We now need to put the pieces back together.

Indeed, consider two blocks B_1 and B_2 of M. We know there exist LC operators L_1 and L_2 such that $RB_i = L_i B_i$ for any LU operator R. But it is a priori not clear that there exists an L that *simultaneously* maps B_1 to B_1' and B_2 to B_2'.

Unfortunately, a solution to this problem is currently not in sight. We will briefly describe why this task poses a serious challenge and what further questions need to be addressed. Consider two blocks B_1 and B_2 with respective reduced supports ω_1, ω_2 and their images B_1' and B_2' under some RLU-operation. The result of the last section allows us to assume that $B_1' = B_1$ without loosing generality. By the remark following Lemma 27, it holds that $B_1 + B_2$ is a block with reduced support $\omega_1 \Delta \omega_2$. Here, $a \Delta b$ denotes the *symmetric complement* of the sets a and b. Therefore, $\pi_{\omega_1 \cap \omega_2}(B_1 + B_2)$ is invariant. The latter invariant describes in a sense the *correlations* between B_1 and B_2. The proof of Theorem 31 can now be generalized to yield that these correlations already determine B_2' on the systems $\omega_1 \cap \omega_2$. More concretely, in the above setting we automatically have $\pi_{\omega_1}(B_2') = \pi_{\omega_1}(B_2)$. Furthermore, it is not hard to see that by the use of RLU operations that act only on the complement $\bar{\omega}_1$ of ω_1 it is possible to achieve $\pi_{\bar{\omega}_1}(B_2') = \pi_{\bar{\omega}_1}(B_2)$. Summarizing, we have

$$
\begin{aligned}
B_1' &= B_1 && (186)\\
\pi_{\omega_1}(B_2') &= \pi_{\omega_1}(B_2) && (187)\\
\pi_{\bar{\omega}_1}(B_2') &= \pi_{\bar{\omega}_1}(B_2). && (188)
\end{aligned}
$$

Note that the last two conditions are not sufficient to conclude that $B_2' = B_2$ holds, opposed to what a naive intuition might suggest.

For the case of a code spanned by only two blocks, it is still feasible to prove that LU equivalence implies LC equivalence. However, already starting with three blocks, only partial correlations in the sense of Eq. (187), (188) can be shown to hold. The next step in the analysis of the LU-equivalence vs. LC-equivalence problem must clearly be to gain a greater understanding of the implications of these partial correlations.

15 Conclusions

In this work a coherent picture of phase space methods in quantum information has been drawn. A description of *characteristic functions*, *Wigner functions* and *stabilizer codes* in an algebraic language has been given. We have analyzed the automorphism group of the Weyl operators and used theses results to describe the covariance properties of Wigner functions. The case of phase spaces over extension fields has received a detailed treatment. We applied the findings to the analysis of Clifford symmetries of a set of numerically given quantum states that generate SIC POVMs. Many of the introduced concepts have been implemented in a collection of packages for a computer algebra system. Lastly, we have set up a framework for discussing the problem of local unitary vs. local Clifford equivalence of stabilizer codes and derived some partial results on that open problem.

16 Acknowledgments

The author would like to thank Jens Eisert for his continuous support which vastly exceeded the norm.

I am grateful to Dirk Schlingemann for fruitful discussions on discrete Weyl systems, and to Marten van den Nest and Marc Hein for conversations on the elusive LU vs. LC problem. Thanks to K. Hellwig for still giving lectures on Quantum Information and to Timo Felbinger for his constant supply of TeX advises. Further, the pleasant support of the Studienstiftung des Deutschen Volkes is kindly acknowledged.

17 Zusammenfassung

Diese Arbeit befasst sich mit endlichen Phasenräumen und drarauf basierenden Methoden in der Quanteninformationstheorie. Die Konzepte der *charakteristischen Funktion*, der *Wignerfunktion* und von *Stabilisatorkodes* werden in einer einheitlichen, algebraischen Sprache präsentiert. Desweiteren analysieren wir die Automorphismengruppen von Weyloperatoren und verwenden diese Resultate um die Kovarianzeigenschaften von Wignerfunktionen zu beschreiben. Der Spezialfall von Phasenräumen über algebraischen Erweiterungskörpern wird im detailiert behandelt. Diese Erkenntnisse werden weiter verwendet um die Clifford-Symmetrien von numerisch gegebenen Quantenzuständen zu analysieren, die SIC POVMs erzeugen. Viele der eingeführten Konzepte wurden in einer Sammlung von Paketen für ein Computeralgebra-System implementiert. In einem zweiten Teil wird ein mathematischer Rahmen zur Diskussion des Problems von lokaler unitärer Äquivalenz im Gegensatz zu lokaler Clifford Äquivalenz von Stabilisatorkodes geschaffen. Wir geben einige Teilantworten zu diesem offenen Problem.

Diese Arbeit wurde von dem Autor selbständig und ohne Zuhilfenahme anderer als der angegebenen Quellen verfasst.

18 Appendix I: SIC POVMs and Zauner's Conjecture

The following is a summary of the SIC POVM problem written by the author for the *Open Problems in Quantum Information* collection maintained at [31].

18.1 Problem

We will give three variants of the problem, each being stronger than its predecessor. The terminology of problems 1 and 2 is taken mainly from [32]. For problem 3 see [33] and [34].

18.1.1 Problem 1 (SIC-POVMs)

A set of d^2 normed vectors $\{|\phi_i\rangle\}_i$ in a Hilbert space of dimension d constitutes a set of *equiangular lines* if their mutual inner products

$$|\langle\phi_i|\phi_j\rangle|^2$$

are independent of the choice of $i \neq j$. It can be shown [32] that

- the associated projection operators sum to a multiple of unity and thus induce a POVM (up to normalization) and that
- these operators are linearly independent and hence any quantum state can be reconstructed from the measurement statistics $p_i := \operatorname{tr}(|\phi_i\rangle\langle\phi_i|\rho)$ of the POVM.

A POVM that arises in this way is called *symmetric informationally complete*, or a *SIC-POVM* for short.

The most general form of the problem is: decide if SIC-POVMs exists in any dimension d.

18.1.2 Problem 2 (Covariant SIC-POVMs)

A vector $|\phi\rangle$ is called a *fiducial vector* with respect to the Heisenberg group if the set

$$\big\{w(p,q)\,|\phi\rangle\langle\phi|\,w(p,q)^\dagger\big\}_{p,q=0..d-1} \tag{189}$$

induces a SIC-POVM. Such a SIC-POVM is said to be *group covariant*. The definition makes sense for any group of order at least d^2. However, we will focus on the Heisenberg group in what follows.

The problem: decide if group covariant SIC-POVMs exist in any dimension d.

18.1.3 Problem 3 (Zauner's Conjecture)

The normalizer of the Heisenberg group within the unitaries $U(d)$ is called the *Clifford group*. There exists an element z of the Clifford group which is defined via its action on the Weyl operators as

$$z\,w(p,q)z^\dagger \quad = \quad w(q-p,-p). \tag{190}$$

Zauner's conjecture, as formulated in [34], runs: in any dimension d, a fiducial vector can be found among the eigenvectors of z.

18.2 Background

Besides their mathematical appeal, SIC-POVMs have obvious applications to quantum state tomography. The symmetry condition assures that the possible measurement outcomes are in some sense maximally complementary.

18.3 History and Partial Results

- In the context of quantum information, the problem seems to have been tackled first by Gerhard Zauner in his doctorial thesis [33] in 1999. To our knowledge, the results were neither published nor translated into English, which caused some confusion in the English literature, as to what Zauner had actually conjectured[4]. Zauner analyzed the spectrum of z. He listed analytical expressions for fiducial vectors in dimension 2, 3, 4, 5 and numerical expressions for $d = 6, 7$. He noted that for dimension 8 an analytic SIC-POVM is known, which is covariant under the action of the threefold tensor product of the two dimensional Heisenberg group.

- Wide interest in the problem arose with the 2003 paper by Renes et. al. [32]. Building on concepts from *frame theory*, the authors reduced the task of numerically finding fiducial vectors to a non-convex global optimization problem. Using this method, they presented numerical fiducial vectors for all dimensions up to 45 and counted the number of distinct covariant SIC-POVMs up to dimension 7. The question of whether those vectors were eigenstates of a Clifford operation was left open (but see below). Further, four groups other than the Heisenberg group were numerically found to induce SIC-POVMs in the sense of (189).

  The authors showed that a SIC-POVM corresponds to a *spherical 2-design*[5]. The same assertion was proven by Klappenecker and Rötteler in [35] and was apparently known to Zauner (see Remark 3 in [35]).

- In [36] Grassl used a computer algebra system capable of symbolic calculations to prove Zauner's conjecture for $d = 6$. He remarked that elements of the Clifford group map fiducial vectors onto fiducial vectors. Building on that observation, he could account for all 96 covariant SIC-POVMs that were reported to exist for $d = 6$ in [32].

- Appleby in [34] gave a detailed description of the Clifford group and extended it by allowing for anti-unitary operators. He verified that the numeric solutions of [32] were compatible with Zauner's conjecture and analyzed their stability groups inside the Clifford group[6]. Appleby goes on to present analytical expressions for fiducial vectors in dimension 7 and 19 and specifies an infinite sequence of dimensions for which he conjectures that solutions can be found more easily.

- Inspired by a construction that links finite geometries to MUBs, there have been some speculations by Wootters about whether SIC-POVMs can be linked to finite

[4] Refer e.g. to the first vs. the second version of [34] on the arXiv server.

[5] A finite set X of unit vectors is a *t-design* if the average of any *t*-th order polynomial over X is the same as the average of that polynomial over the entire unit sphere.

[6] The same results were derived in Section 8.

affine planes [37]. The same line of thought was pursued by Bengtsson and Ericsson in [38]. However, the existence of such a construction remains an open problem. The results by Grassl are of some relevance here, as it is known that affine planes of order 6 do not exist.

References

[1] D. Jungnickel, *Finite fields.* (BI-Wiss.-Verl., Mannheim, 1993).

[2] B. Huppert, *Endliche Gruppen.* (Springer, Berlin, 1967).

[3] E. Wigner, *On the Quantum Correction For Thermodynamic Equilibrium*. Phys. Rev. **40**, 749 (1932).

[4] W.K. Wootters, *A Wigner-Function Formulation of Finite-State Quantum-Mechanics*, Annals of Physics **167**, 1 (1987).

[5] U. Leonhardt, *Quantum-State Tomography and Discrete Wigner Function*. Phys. Rev. Let. **74**, 4101 (1995).

[6] P. Bianucci, C. Miquel, J.P. Paz, and M. Saraceno, *Discrete Wigner functiosn and the phase space representation of quantum computers.* quant-ph/0106091.

[7] J.P. Paz, *Discrete Wigner functions and the phase space representation of quantum teleportation*. quant-ph/0204150.

[8] N. Mukunda, S. Chaturvedi, and R. Simon, *Wigner distributions for non Abelian finite groups of odd order*. quant-ph/0305127.

[9] K.S. Gibbons, M.J. Hoffman, and W.K. Wootters, *Discrete phase space based on finite fields.* Phys. Rev. A **70**, 062101 (2004), quant-ph/040115.

[10] A. Vourdas, *Quantum systems with finite Hilbert space.* Rep. Prog. Phys. **67**, 267 (2004).

[11] A.S. Holevo, *Probabilistic and statistical aspects of quantum theory.* (North-Holland Publ. Co., Amsterdam, 1982).

[12] M. Neuhauser, *An Explicit Construction of the Metaplectic Representation over a Finite Field.* Journal of Lie Theory **12**, 15 (2002).

[13] G.B. Folland, *Harmonic analysis in phase space.* (Princeton Univ. Pr., Princeton, 1989).

[14] W. Rudin, *Fourier analysis on groups.* (Wiley-Interscience, New York, 1990).

[15] B. Simon, *Representations of fintie and compact groups.* (American Mathematical Society, Providence, Rhode Island, 1996).

[16] T. Felbinger, *qmatrix: A Package for Quantum Information Theory*, http://library.wolfram.com/infocenter/MathSource/1893.

[17] M. Hein, J. Eisert, and H.J. Briegel, *Multi-party entanglement in graph states*, Phys. Rev. A **69**, 06231 (2002), quant-ph/0206171.

[18] D. Schlingemann, *Quantum error-correcting codes associated with graphs*, quant-ph/0012111, D. Schlingemann, *Stabilizer codes can be realized as graph codes*, quant-ph/0111080.

[19] D. Schlingemann, *Cluster states, algorithms and graphs*, quant-ph/0305170.

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

[21] R. Berndt, R. Schmidt, *Elements of the representation theory of the Jacobi Group.* (Birkhäuser, Basel, 1998).

[22] M. Van den Nest, J. Dehaene, and B. De Moor, *Local invariants of stabilizer codes.* quant-ph/0404106.

[23] M. Van den Nest, J. Dehaene, and B. De Moor, *The invariants of the local Clifford group.* Phys. Rev. A **71**, 022310 (2005), quant-ph/0410035

[24] M. Van den Nest, J. Dehaene, and B. De Moor, *Finite set of invariants to characterize local Clifford equivalence of stabilizer states.* quant-ph/0410165.

[25] M. Van den Nest, J. Dehaene, and B. De Moor, *On local unitary versus local Clifford equivalence of stabilizer states.* quant-ph/0411115.

[26] M. A. Nielsen, I.L. Chuang, *Quantum computation and quantum information.* (Cambridge University Press, Cambridge, 2000).

[27] E. M. Rains, *Quantum Codes of Minimal Distance Two.* quant-ph/9704043 (1997).

[28] H. Aschauer, J. Calsamiglia, M. Hein, and H. J. Briegel, *Local invariants for multi-partite entangled states allowing for a simple entanglement criterion.* Quant. Inf. Comp. 4, 383 (2004), quant-ph/0306048.

[29] J. Schwinger, *Unitary Operator Bases.* Proc. NAS 46, 570 (1960).

[30] A. Bouchet, *Recognizing locally equivalent graphs.* Discrete Math. **114**, 75 (1993).

[31] O. Krüger, R.F. Werner (editors), *Open Problems in Quantum Information*, quant-ph/0504166, http://www.imaph.tu-bs.de/qi/problems/.

[32] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric Informationally Complete Quantum Measurements*, J. Math. Phys. 45, 2171 (2004) and quant-ph/0310075 (2003).

[33] G. Zauner, *Quantendesigns – Grundzüge einer nichtkommutativen Designtheory*, Doctorial thesis, University of Vienna, 1999 (available online at http://www.mat.univice.ac.at/˜neun/papers/physpapers.html).

[34] D. M. Appleby, *SIC-POVMs and the Extended Clifford Group*, quant-ph/0412001 (2004).

[35] A. Klappenecker, and M. Rötteler, *Mutually Unbiased Bases are Complex Projective 2-Designs*, quant-ph/0502031 (2005).

[36] M. Grassl, *On SIC-POVMs and MUBs in dimension 6*, quant-ph/0406175 (2004).

[37] W. K. Wootters, *Quantum measurements and finite geometry*, quant-ph/0406032 (2004).

[38] I. Bengtsson, and Åsa Ericsson, *Mutually Unbiased Bases and The Complementarity Polytope*, quant-ph/0410120 (2004).