IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Galois quantum systems

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2005 J. Phys. A: Math. Gen. 38 8453

(http://iopscience.iop.org/0305-4470/38/39/011)

View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 171.66.16.94
The article was downloaded on 03/06/2010 at 03:58

Please note that terms and conditions apply.

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **38** (2005) 8453–8471 doi:10.1088/0305-4470/38/39/011

Galois quantum systems

A Vourdas

Department of Computing, University of Bradford, Bradford BD7 1DP, UK

Received 25 February 2005
Published 14 September 2005
Online at stacks.iop.org/JPhysA/38/8453

Abstract

A finite quantum system in which the position and momentum take values in the Galois field GF(p^ℓ) is constructed from a smaller quantum system in which the position and momentum take values in $\mathcal{Z}_p$, using field extension. The Galois trace is used in the definition of the Fourier transform. The Heisenberg–Weyl group of displacements and the Sp(2, GF(p^ℓ)) group of symplectic transformations are studied. A class of transformations inspired by the Frobenius maps in Galois fields is introduced. The relationship of this 'Galois quantum system' with its subsystems in which the position and momentum take values in subfields of GF(p^ℓ) is discussed.

PACS numbers: 03.67.−a, 03.65.Ca
Mathematics Subject Classification: 81S30, 11T06

1. Introduction

Quantum systems with d-dimensional Hilbert space have been studied originally by Weyl and Schwinger [1], and later by many authors [2–9] (for a review see [10]). A formalism analogous to the harmonic oscillator is developed, with position and momentum taking values in $\mathcal{Z}_d$ (the integers modulo d). There are however difficulties when we pursue this analogy with harmonic oscillator. The harmonic oscillator has the plane $R \times R$ as phase space and we can define the group Sp(2, R) of symplectic transformations, which are useful in many contexts (e.g., Radon transforms, quantum tomography, etc). A finite quantum system has the toroidal lattice $\mathcal{Z}_d \times \mathcal{Z}_d$ as phase space, which (in general) is a collection of points with no geometrical structure and we cannot define symplectic transformations. Consequently, the properties of such systems are much weaker in comparison to the harmonic oscillator. The root of these difficulties is that $\mathcal{Z}_d$ is a ring (there are no inverses).

However when the dimension of the system is the power of a prime number p (i.e., $d = p^\ell$), the position and momentum take values in the Galois field GF(p^ℓ). We call them Galois quantum systems. We have explained in [7, 10] that in this case the phase space is a finite geometry [11] and has very powerful geometrical properties (e.g., there are well-defined translations and rotations and they form groups). Consequently, we are able to define a group

 © 2005 IOP Publishing Ltd Printed in the UK

of symplectic transformations and use them to prove strong properties analogous those of a harmonic oscillator.

In Galois fields, we start from a field $\mathcal{Z}_p$ (the integers modulo a prime p) and we use the concept of field extension to get bigger fields GF(p^ℓ). In our case, we start with p-dimensional Hilbert spaces $\mathcal{H}$ and we use tensor products $\mathcal{H} \otimes \cdots \otimes \mathcal{H}$ to construct bigger systems with dimension p^ℓ. At this stage, the technical details are crucial for the properties of the system that we will construct. We use the Galois trace in the definition of the Fourier transform and consequently our system is different from a trivial tensor product of ℓ component systems. There is a lot of extra structure which we explain throughout the paper. Work in a similar direction has recently been presented in [12, 13].

Another desirable property in finite quantum systems is to find mutually unbiased bases (orthonormal bases $|a_i\rangle$ and $|b_j\rangle$ such that $|\langle a_i|b_j\rangle|^2 = d^{-1}$). It is known that the number of such bases cannot exceed $d + 1$; and it is also known that for systems where d is the power of a prime, the number of such bases is indeed $d + 1$. Mutually unbiased bases are important in quantum communications, and for this reason they have recently been studied extensively [14–21]. Related to this is also the so-called 'mean king's problem' [22]. In summary, the problem of mutually unbiased bases also leads, through another root, to quantum systems with dimension which is the power of a prime. We do not study this problem here, but we mention it as one of the motivations for the study of these systems.

Another motivation is the extensive use of Galois fields in classical coding (e.g., in classical cyclic codes). These techniques could be transferred in quantum information processing if Galois fields are incorporated in quantum systems (e.g., work on the quantum version of cyclic codes has been presented in [23]). Other work with Galois fields in the context of quantum coding has been reported in [24–26]. Further understanding of quantum systems in which the variables take values in Galois fields will be a valuable toolbox which can be used to bridge the gap between classical and quantum information processing.

From a mathematical point of view this work transfers the concept of field extension in the context of Hilbert spaces. It starts from systems described by Hilbert spaces with a prime dimension and produces bigger Hilbert spaces with a power of a prime dimension. There are connections with the subject of applied harmonic analysis which studies various transforms (Fourier, Gabor, wavelet, etc) on functions $f(t)$ where the variable t takes values in some set S. We are interested in the case where the set S is a Galois field; and in this paper using a field extension we go to a bigger Galois field and study the corresponding bigger Hilbert space and the transformations in it.

In section 2, we briefly review the theory of finite quantum systems and introduce the notation. In section 3, we adapt some known concepts from Galois theory, into our own context, for later use. For example, we introduce the matrix g which is used in calculations of the Galois trace; and we study additive characters and their properties, which are used later in Fourier transforms.

Galois quantum systems are discussed in section 4. We introduce the Fourier transform F using the Galois trace and explain that it is different from the tensor product $\mathcal{F} \otimes \cdots \otimes \mathcal{F}$ of independent Fourier transforms on the ℓ component systems. We also discuss the displacement operators and their properties, and the displaced parity operators and their properties. In section 5, we discuss symplectic transformations and show explicitly that they are different from independent symplectic transformations on the ℓ component systems.

An important aspect of Galois fields is the Frobenius maps among Galois conjugates. In section 6, we introduce 'Frobenius subspaces' comprised by states labelled with Galois conjugates, and study transformations which leave them invariant. Another related aspect of Galois fields is the study of their subfields. The implications of this in our context is that

there are Galois subsystems in which the position and momentum take values in a subfield. We study them in section 7 and clarify the relation between transformations within the 'big' Galois quantum system and the corresponding ones in the subsystems.

We conclude in section 8 with a discussion of our results.

2. Finite quantum systems

We consider a quantum system with a d-dimensional Hilbert space $\mathcal{H}$. In this space, we consider an orthonormal basis of 'position states' which we denote as $|\mathcal{X}; m\rangle$. Here, $\mathcal{X}$ is not a variable, but it simply indicates position states. m belongs to $\mathcal{Z}_d$.

The finite Fourier transform plays an important role in the formalism and is defined as

$$\mathcal{F} = d^{-1/2}\sum_{m=0}^{d-1}\sum_{n=0}^{d-1}\omega(mn)|\mathcal{X}; m\rangle\langle\mathcal{X}; n|; \qquad \omega(\alpha) \equiv \omega^{\alpha} = \exp\left[\mathrm{i}\frac{2\pi\alpha}{d}\right]. \tag{1}$$

An identity which is easily proved and which is very useful later is

$$\frac{1}{d}\sum_{n}\omega[n(m-\ell)] = \delta(m,\ell) \tag{2}$$

where $\delta(n, m)$ is the Kronecker delta which is equal to 1 when $n = m(\mathrm{mod}(d))$. Using it we prove that

$$\mathcal{F}\mathcal{F}^{\dagger} = \mathcal{F}^{\dagger}\mathcal{F} = \mathbf{1}; \qquad \mathcal{F}^4 = \mathbf{1}. \tag{3}$$

Using the Fourier transform we define another orthonormal basis, the 'momentum states', as

$$|\mathcal{P}; m\rangle = \mathcal{F}|\mathcal{X}; m\rangle = d^{-1/2}\sum_{n}\omega(mn)|\mathcal{X}; n\rangle. \tag{4}$$

We also define the 'position and momentum operators' $\hat{x}$ and $\hat{p}$ as

$$\hat{x} = \sum_{n=0}^{d-1} n|\mathcal{X}; n\rangle\langle\mathcal{X}; n|; \qquad \hat{p} = \sum_{n=0}^{d-1} n|\mathcal{P}; n\rangle\langle\mathcal{P}; n|; \qquad \hat{p} = \mathcal{F}\hat{x}\mathcal{F}^{\dagger}. \tag{5}$$

We note that n are integers modulo d and consequently $\hat{x}$ and $\hat{p}$ are defined modulo $d\mathbf{1}$. However, below we will use exponentials of these operators and they are single valued.

In our finite quantum system both the position and momentum are integers modulo d. Therefore, the position–momentum phase space is the toroidal lattice $\mathcal{Z}_d \times \mathcal{Z}_d$. In this phase space, we define the displacement operators

$$\begin{aligned}\mathcal{Z} &= \omega^{\hat{x}} = \sum_{n=0}^{d-1}\omega(n)|\mathcal{X}; n\rangle\langle\mathcal{X}; n| \\ \mathcal{X} &= \omega^{-\hat{p}} = \sum_{n=0}^{d-1}\omega(-n)|\mathcal{P}; n\rangle\langle\mathcal{P}; n|.\end{aligned} \tag{6}$$

They are unitary operators and perform displacements along the $\mathcal{P}$ and $\mathcal{X}$ axes in the phase space. Indeed, we can show that

$$\mathcal{Z}^{\alpha}|\mathcal{P}; m\rangle = |\mathcal{P}; m+\alpha\rangle; \qquad \mathcal{Z}^{\alpha}|\mathcal{X}; m\rangle = \omega(\alpha m)|\mathcal{X}; m\rangle \tag{7}$$

$$\mathcal{X}^{\beta}|\mathcal{P}; m\rangle = \omega(-m\beta)|\mathcal{P}; m\rangle; \qquad \mathcal{X}^{\beta}|\mathcal{X}; m\rangle = |\mathcal{X}; m+\beta\rangle. \tag{8}$$

The displacement operators obey the relations

$$\mathcal{X}^d = \mathcal{Z}^d = \mathbf{1}; \qquad \mathcal{X}^{\beta}\mathcal{Z}^{\alpha} = \mathcal{Z}^{\alpha}\mathcal{X}^{\beta}\omega(-\alpha\beta) \tag{9}$$

where α, β are integers in $\mathcal{Z}_d$.

The general displacement operators are defined as

$$\mathcal{D}(\alpha,\beta)=\mathcal{Z}^{\alpha}\mathcal{X}^{\beta}\omega(-2^{-1}\alpha\beta);\qquad [\mathcal{D}(\alpha,\beta)]^{\dagger}=\mathcal{D}(-\alpha,-\beta). \tag{10}$$

The $\mathcal{D}(\alpha,\beta)$ are unitary operators and are associated with the Heisenberg–Weyl group in the context of finite quantum systems. Using equation (9), we can prove the multiplication rule

$$\mathcal{D}(\alpha_1,\beta_1)\mathcal{D}(\alpha_2,\beta_2)=\mathcal{D}(\alpha_1+\alpha_2,\beta_1+\beta_2)\omega[2^{-1}(\alpha_1\beta_2-\alpha_2\beta_1)]. \tag{11}$$

3. Galois fields

In this section, we adapt some concepts from Galois theory in a language which is suitable for later use. For example, we introduce the matrix g which is used in the calculation of the Galois trace.

The $\mathcal{Z}_d$ is in general a ring. When d is a power of a prime p ($d=p^{\ell}$), it is a Galois field which we denote as GF(p^{ℓ}). Its elements can be written as polynomials of an indeterminate ϵ with coefficients in $\mathcal{Z}_p$:

$$\alpha=\alpha_0+\alpha_1\epsilon+\cdots+\alpha_{\ell-1}\epsilon^{\ell-1};\qquad \alpha_0,\alpha_1,\ldots,\alpha_{\ell-1}\in\mathcal{Z}_p. \tag{12}$$

These polynomials are defined modulo an irreducible polynomial of degree ℓ:

$$P(\epsilon)\equiv c_0+c_1\epsilon+\cdots+c_{\ell-1}\epsilon^{\ell-1}+\epsilon^{\ell};\qquad c_0,c_1,\ldots,c_{\ell-1}\in\mathcal{Z}_p. \tag{13}$$

Different irreducible polynomials of the same degree ℓ lead to isomorphic finite fields, and in this sense there is only one finite field which we denote as GF(p^{ℓ}). We note that results of practical calculations do depend on the choice of the irreducible polynomial, but different choices lead to isomorphic results.

The Frobenius map $\sigma(\alpha)=\alpha^{p}$ defines an automorphism in GF(p^{ℓ}). Its powers

$$\sigma(\alpha)=\alpha^{p};\qquad \sigma^{2}(\alpha)=\alpha^{p^{2}};\qquad \ldots\qquad ;\sigma^{\ell}(\alpha)=\alpha^{p^{\ell}}=\alpha \tag{14}$$

leave all elements of the base field $\mathcal{Z}_p$ fixed; and form a cyclic group of order ℓ. The powers $\alpha^{p},\ldots,\alpha^{p^{\ell-1}}$ are Galois conjugates of α. The elements of the base field $\mathcal{Z}_p$ are Galois self-conjugates.

The product

$$f(y)\equiv(y-\alpha)(y-\alpha^{p})\cdots\left(y-\alpha^{p^{\ell-1}}\right) \tag{15}$$

which contains all conjugates to a given number α is an irreducible polynomial of degree ℓ in $\mathcal{Z}_p[y]$ (the polynomials with coefficients in $\mathcal{Z}_p$). For $\alpha=\epsilon$, we get the irreducible polynomial $P(y)$ of equation (13).

The $y^{p^{\ell}}-y$ is precisely the product of all the distinct irreducible polynomials in $\mathcal{Z}_p[y]$ of degree d where d is a divisor of ℓ:

$$y^{p^{\ell}}-y=\prod f_i(y). \tag{16}$$

3.1. Trace

The trace of α is defined as the sum of all its conjugates:

$$\mathrm{Tr}(\alpha)=\alpha+\alpha^{p}+\cdots+\alpha^{p^{\ell-1}};\qquad \mathrm{Tr}(\alpha)\in\mathcal{Z}_p. \tag{17}$$

All conjugates have the same trace. The following properties will be useful later:

$$\begin{aligned} &\mathrm{Tr}(\alpha+\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)\\ &\mu\in\mathcal{Z}_p \quad\rightarrow\quad \mathrm{Tr}(\mu\alpha)=\mu\,\mathrm{Tr}(\alpha)\\ &\mu\in\mathcal{Z}_p \quad\rightarrow\quad \mathrm{Tr}(\mu)=\mu\ell(\mathrm{mod}\ p). \end{aligned} \tag{18}$$

The last equation implies that if ℓ is an integer multiple of p, then $\mathrm{Tr}(\mu)=0$ for $\mu\in\mathcal{Z}_p$.

We next define

$$\begin{aligned} &\mathcal{E}_\lambda\equiv\mathrm{Tr}\,\epsilon^\lambda; \qquad \mathcal{E}_\lambda\in\mathcal{Z}_p\\ &\mathcal{E}_0=\mathrm{Tr}(1)=\ell(\mathrm{mod}\ p); \qquad \mathcal{E}_1=-c_{\ell-1}. \end{aligned} \tag{19}$$

For $\alpha,\beta\in\mathrm{GF}(p^\ell)$

$$\alpha=\sum_{\lambda=0}^{\ell-1}\alpha_\lambda\epsilon^\lambda; \qquad \beta=\sum_{\kappa=0}^{\ell-1}\beta_\kappa\epsilon^\kappa, \tag{20}$$

the trace can be written as

$$\begin{aligned} &\mathrm{Tr}(\alpha)=\sum_{\lambda=0}^{\ell-1}\alpha_\lambda\mathcal{E}_\lambda\\ &\mathrm{Tr}(\alpha\beta)=\sum_{\lambda,\kappa}g_{\lambda\kappa}\alpha_\lambda\beta_\kappa; \qquad g_{\lambda\kappa}\equiv\mathcal{E}_{\lambda+\kappa}; \qquad \det(g)\neq 0. \end{aligned} \tag{21}$$

We note that the $\ell\times\ell$ matrix $(g_{\lambda\kappa})$ has elements in $\mathcal{Z}_p$ and non-zero determinant. Indeed, if the determinant of g is zero, then there exist non-zero β such that $\mathrm{Tr}(\alpha\beta)=0$ for all α. But then for an arbitrary $\gamma\in\mathrm{GF}(p^\ell)$, we can choose $\alpha=\gamma\beta^{-1}$ and prove that $\mathrm{Tr}(\gamma)=0$. This argument shows that the determinant of g is non-zero. Consequently, the inverse matrix of g exists and we denote it as G.

The $\mathrm{GF}(p^\ell)$ can be regarded as an ℓ-dimensional vector space with $1,\epsilon,\epsilon^2,\ldots,\epsilon^{\ell-1}$ as a basis. Then the general number α of equation (12) corresponds to the vector $(\alpha_0,\ldots,\alpha_{\ell-1})$. Of course we can change this basis into any other basis, and for later use we introduce the dual basis $E_0,E_1,\ldots,E_{\ell-1}$, as follows:

$$E_\kappa=\sum_\lambda G_{\kappa\lambda}\epsilon^\lambda; \qquad G_{\kappa\lambda}\equiv(g^{-1})_{\kappa\lambda}; \qquad G_{\kappa\lambda}\in\mathcal{Z}_p. \tag{22}$$

We note that

$$\mathrm{Tr}(\epsilon^\kappa E_\lambda)=\delta_{\kappa\lambda}. \tag{23}$$

A number $\alpha\in\mathrm{GF}(p^\ell)$ can be expressed as

$$\begin{aligned} &\alpha=\sum_{\lambda=0}^{\ell-1}\alpha_\lambda\epsilon^\lambda=\sum_{\lambda=0}^{\ell-1}A_\lambda E_\lambda; \qquad \alpha_\lambda=\sum_\kappa G_{\lambda\kappa}A_\kappa\\ &\alpha_\lambda=\mathrm{Tr}[\alpha E_\lambda]; \qquad A_\lambda=\mathrm{Tr}[\alpha\epsilon^\lambda]. \end{aligned} \tag{24}$$

3.2. Characters

Additive characters in $\mathrm{GF}(p^\ell)$ are generalizations of the exponential function. They are complex-valued functions $\chi(\alpha)$ which satisfy the relation

$$\chi(\alpha)\chi(\beta)=\chi(\alpha+\beta); \qquad \alpha,\beta\in\mathrm{GF}(p^\ell). \tag{25}$$

Below we will use the function

$$\chi(\alpha) = \omega[\mathrm{Tr}(\alpha)]; \qquad \omega = \exp\left(\mathrm{i}\frac{2\pi}{p}\right) \tag{26}$$

which indeed obeys the relation of equation (25). We next show that this function also obeys the important relation

$$\frac{1}{p^\ell}\sum_n \omega\left[\mathrm{Tr}(nm - nr)\right] = \delta(m, r); \qquad n, m, r \in \mathrm{GF}(p^\ell). \tag{27}$$

This is analogous to equation (2). In order to prove it we use the relation $\mathrm{Tr}[n(m-r)] = \sum g_{ij} n_i (m_j - r_j)$ and equation (2) in conjuction with the fact that the determinant of g is non-zero.

A more general result which is easily proved using equation (42) is

$$\frac{1}{p^\ell}\sum_n \omega\left[\mathrm{Tr}\left(nm - n^{p^\lambda} r\right)\right] = \delta\left(m, r^{p^{\ell-\lambda}}\right) = \delta\left(m^{p^\lambda}, r\right). \tag{28}$$

4. Galois quantum systems

We consider a p-dimensional Hilbert space $\mathcal{H}$ (where p is an odd prime) which has the mathematical structure described in section 2. We also consider the tensor product of ℓ such spaces $H = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$. We use calligraphic letters for operators and states on the various p-dimensional Hilbert spaces $\mathcal{H}$ and ordinary letters for operators and states on the p^ℓ-dimensional Hilbert space H.

The position states in H can be written as

$$|X; m\rangle \equiv |\mathcal{X}; m_0\rangle \otimes \cdots \otimes |\mathcal{X}; m_{\ell-1}\rangle; \qquad m = \sum_i m_i \epsilon^i. \tag{29}$$

Using the character of equation (26), we introduce the finite Fourier transform as

$$\begin{aligned} F &= (p^\ell)^{-1/2} \sum_{m,n} \omega[\mathrm{Tr}(mn)] |X; m\rangle\langle X; n| \\ &= (p^\ell)^{-1/2} \sum_{m_i, n_j} \omega\left[\sum_{i,j} g_{ij} m_i n_j\right] |\mathcal{X}; m_0\rangle\langle\mathcal{X}; n_0| \otimes \cdots \otimes |\mathcal{X}; m_{\ell-1}\rangle\langle\mathcal{X}; n_{\ell-1}| \end{aligned} \tag{30}$$

$$\omega = \exp\left(\mathrm{i}\frac{2\pi}{p}\right).$$

We stress that in general $g_{ij} \neq \delta_{ij}$ and therefore F is *different* from the operator $\mathcal{F} \otimes \cdots \otimes \mathcal{F}$; where $\mathcal{F}$ are the Fourier operators of equation (1) acting on the various p-dimensional Hilbert spaces $\mathcal{H}$.

Using equation (28), we prove that the Fourier operator F obeys the relation

$$FF^\dagger = F^\dagger F = \mathbf{1}; \qquad F^4 = \mathbf{1}. \tag{31}$$

We introduce the momentum states as follows:

$$|P; m\rangle = F|X; m\rangle = (p^\ell)^{-1/2} \sum_n \omega[\mathrm{Tr}(mn)]|X; n\rangle; \qquad m, n \in \mathrm{GF}(p^\ell). \tag{32}$$

They form an orthonormal basis in H. It is easily seen that

$$|P; m\rangle = |\mathcal{P}; M_0\rangle \otimes \cdots \otimes |\mathcal{P}; M_{\ell-1}\rangle; \qquad m = \sum_i m_i \epsilon^i = \sum_i M_i E_i. \tag{33}$$

Position and momentum operators can be defined as in equation (5):

$$\begin{aligned}\hat{x} &= \sum_m m|X;m\rangle\langle X;m| = \sum_i \epsilon^i[\mathbf{1}\otimes\cdots\otimes x_{(i)}\otimes\cdots\otimes\mathbf{1}]\\ \hat{p} &= \sum_m m|P;m\rangle\langle P;m| = \sum_i E_i[\mathbf{1}\otimes\cdots\otimes p_{(i)}\otimes\cdots\otimes\mathbf{1}].\end{aligned} \tag{34}$$

Their eigenvalues are elements of GF(p^ℓ) and therefore obey the relation $m^{p^\ell} = m$. According to the Cayley–Hamilton theorem their characteristic equation is

$$\hat{x}^{p^\ell} = \hat{x}; \qquad \hat{p}^{p^\ell} = \hat{p}. \tag{35}$$

Motivated by the concept of trace in Galois fields, we can define the Galois trace of operators (like $\hat{x}$, $\hat{p}$) whose eigenvalues are in GF(p^ℓ) as

$$\mathrm{Tr}_{\mathcal{G}}(\alpha\hat{x}) = \alpha\hat{x} + (\alpha\hat{x})^p + \cdots + (\alpha\hat{x})^{p^{\ell-1}}; \qquad \alpha \in \mathrm{GF}(p^\ell). \tag{36}$$

The Galois trace of an operator (which we denote with $\mathrm{Tr}_{\mathcal{G}}$) is another operator with eigenvalues in $\mathcal{Z}_p$; and it is a different concept from the ordinary trace which is a number. For $\mu \in \mathcal{Z}_p$, it is easily seen that $\mathrm{Tr}_{\mathcal{G}}(\mu\hat{x}) = \mu\,\mathrm{Tr}_{\mathcal{G}}\hat{x}$.

4.1. Displacements and the Heisenberg–Weyl group

We next define the displacement operators

$$\begin{aligned}Z^\alpha &\equiv \omega[\mathrm{Tr}_{\mathcal{G}}(\alpha\hat{x})] = \sum_n \omega[\mathrm{Tr}(\alpha n)]|X;n\rangle\langle X;n|\\ X^\beta &\equiv \omega[-\mathrm{Tr}_{\mathcal{G}}(\alpha\hat{p})] = \sum_n \omega[-\mathrm{Tr}(\beta n)]|P;n\rangle\langle P;n|.\end{aligned} \tag{37}$$

We have used here the characters of equation (26) and this ensures that

$$Z^{\alpha_1}Z^{\alpha_2} = Z^{\alpha_1+\alpha_2}; \qquad X^{\beta_1}X^{\beta_2} = X^{\beta_1+\beta_2}. \tag{38}$$

It is worth pointing out that according to the above definition Z is the diagonal $p^\ell \times p^\ell$ matrix $(\omega[\mathrm{Tr}(n)])$. We can easily calculate powers of this matrix if they belong to the base field $\mathcal{Z}_p$. For $\alpha \in \mathcal{Z}_p$, we use the fact that $\alpha\,\mathrm{Tr}(n) = \mathrm{Tr}(\alpha n)$ and get equation (37). For $\alpha \in \mathrm{GF}(p^\ell)\alpha\,\mathrm{Tr}(n) = \mathrm{Tr}(\alpha n)$ is in general not valid, but at the same time the meaning of the complex matrix Z to a power which belongs to a Galois field is unclear and needs to be defined. In this case, equation (37) is a *definition* for Z^α based on the character of equation (26), which is a complex-valued function with the property of equation (25) and this ensures the property of equation (38).

The Z^α, X^β are unitary operators and using equation (37) we prove that

$$Z^\alpha|P;m\rangle = |P;m+\alpha\rangle; \qquad Z^\alpha|X;m\rangle = \omega[\mathrm{Tr}(\alpha m)]|X;m\rangle \tag{39}$$

$$X^\beta|P;m\rangle = \omega[-\mathrm{Tr}(m\beta)]|P;m\rangle; \qquad X^\beta|X;m\rangle = |X;m+\beta\rangle. \tag{40}$$

Using these relations we show that

$$X^\beta Z^\alpha = Z^\alpha X^\beta \omega[-\mathrm{Tr}(\alpha\beta)]. \tag{41}$$

The general displacement operators in the GF(p^ℓ) $\times$ GF(p^ℓ) phase space are defined as

$$\begin{aligned}&D(\alpha,\beta) = Z^\alpha X^\beta \omega[-2^{-1}\,\mathrm{Tr}(\alpha\beta)]; \qquad [D(\alpha,\beta)]^\dagger = D(-\alpha,-\beta)\\ &D(\alpha,\beta)D(\gamma,\delta) = \omega[2^{-1}\,\mathrm{Tr}(\alpha\delta-\beta\gamma)]D(\alpha+\gamma,\beta+\delta).\end{aligned} \tag{42}$$

In order to see the relation between the displacement operators acting on H and the displacement operators $\mathcal{D}$ of equation (10) acting on the various p-dimensional Hilbert spaces $\mathcal{H}$, we show that

$$D(\alpha,\beta)=\mathcal{D}(A_0,\beta_0)\otimes\cdots\otimes\mathcal{D}(A_{\ell-1},\beta_{\ell-1})$$
$$\alpha=\sum_i\alpha_i\epsilon^i=\sum_i A_iE_i;\qquad \beta=\sum_i\beta_i\epsilon^i. \tag{43}$$

Using equation (42), we can show that if γ belongs to the base field $\mathcal{Z}_p$ then

$$[D(\alpha,\beta)]^\gamma=D(\alpha\gamma,\beta\gamma). \tag{44}$$

More generally for $\gamma\in\mathrm{GF}(p^\ell)$ we define the power of $D(\alpha,\beta)$ through the above equation. Alternative derivations of equation (44) can also be given, e.g., through explicit calculation of $\{Z^\alpha X^\beta\omega[-2^{-1}\,\mathrm{Tr}(\alpha\beta)]\}^\gamma$. They will be proofs for $\gamma\in\mathcal{Z}(p)$, but for $\gamma\in\mathrm{GF}(p^\ell)$ they will involve complex numbers to powers in $\mathrm{GF}(p^\ell)$ which need to be defined, using the character of equation (26). So in any case, equation (44) is really a definition for $\gamma\in\mathrm{GF}(p^\ell)$.

We note that the displacement operators considered earlier in equation (6) are $d\times d$ matrices, and they have d distinct eigenvalues to each of which corresponds one eigenvector (there is no degeneracy). Here the displacement operators of equation (37) are $p^\ell\times p^\ell$ matrices, and they have only p distinct eigenvalues (there is large degeneracy).

We next show the 'marginal properties':

$$\frac{1}{p^\ell}\sum_{\alpha\in\mathrm{GF}(p^\ell)}D(\alpha,\beta)=|X;2^{-1}\beta\rangle\langle X;-2^{-1}\beta|$$
$$\frac{1}{p^\ell}\sum_{\beta\in\mathrm{GF}(p^\ell)}D(\alpha,\beta)=|P;2^{-1}\alpha\rangle\langle P;-2^{-1}\alpha| \tag{45}$$
$$\frac{1}{p^\ell}\sum_{\alpha,\beta\in\mathrm{GF}(p^\ell)}D(\alpha,\beta)=P(0,0).$$

In order to prove them we use the fact that analogous relations are valid for all finite systems with odd dimension [7, 10], the fact that when α,β take all values in $\mathrm{GF}(p^\ell)$ then A_i,β_i take all values in $\mathcal{Z}_p$ and equation (43). Using them we can show related properties for the Weyl functions [7, 10].

4.2. Displaced parity operators

We define the parity operator around the origin as $P(0,0)=F^2$. Clearly it obeys the relation $[P(0,0)]^2=\mathbf{1}$. Acting with it on position and momentum states, we get

$$P(0,0)|X;m\rangle=|X;-m\rangle;\qquad P(0,0)|P;m\rangle=|P;-m\rangle. \tag{46}$$

These equations show that

$$P(0,0)=\mathcal{P}(0,0)\otimes\cdots\otimes\mathcal{P}(0,0) \tag{47}$$

where $\mathcal{P}(0,0)=\mathcal{F}^2$ are the parity operators on the various $\mathcal{H}$ Hilbert spaces. We have explained that F is different from the operator $\mathcal{F}\otimes\cdots\otimes\mathcal{F}$, but we see here that $F^2=\mathcal{F}^2\otimes\cdots\otimes\mathcal{F}^2$.

The displaced parity operator (parity operator around the point (α,β) in phase space) is defined as

$$P(\alpha,\beta)=D(\alpha,\beta)P(0,0)[D(\alpha,\beta)]^\dagger=D(2\alpha,2\beta)P(0,0)=P(0,0)[D(2\alpha,2\beta)]^\dagger. \tag{48}$$

It obeys the relation $[P(\alpha,\beta)]^2 = \mathbf{1}$. Combining equation (48) with equation (43) we show that

$$\begin{aligned} &P(\alpha,\beta) = \mathcal{P}(A_0,\beta_0)\otimes\cdots\otimes\mathcal{P}(A_{\ell-1},\beta_{\ell-1}) \\ &\alpha = \sum_i \alpha_i \epsilon^i = \sum_i A_i E_i; \qquad \beta = \sum_i \beta_i \epsilon^i. \end{aligned} \tag{49}$$

In a similar way we can show the following relations for the displaced parity operator:

$$\begin{aligned} &\frac{1}{p^\ell}\sum_{\beta\in \mathrm{GF}(p^\ell)} P(\alpha,\beta) = |P;\alpha\rangle\langle P;\alpha| \\ &\frac{1}{p^\ell}\sum_{\alpha\in \mathrm{GF}(p^\ell)} P(\alpha,\beta) = |X;\beta\rangle\langle X;\beta| \\ &\frac{1}{p^\ell}\sum_{\alpha,\beta\in \mathrm{GF}(p^\ell)} P(\alpha,\beta) = \mathbf{1}. \end{aligned} \tag{50}$$

Using them we can show related properties for the Wigner functions [7, 10].

We next use equations (45), (48) to show that the displaced parity operators are related to the displacement operators through a two-dimensional Fourier transform

$$P(\alpha,\beta) = \sum_{\gamma,\delta} D(\gamma,\delta)\omega[\mathrm{Tr}(\alpha\delta-\beta\gamma)]. \tag{51}$$

5. The Sp(2, GF(p^ℓ)) group of symplectic transformations

In the $\mathrm{GF}(p^\ell)\times\mathrm{GF}(p^\ell)$ phase space, we consider the unitary transformations

$$\begin{aligned} &(Z')^\alpha = S(\kappa,\lambda,\mu)Z^\alpha S^\dagger(\kappa,\lambda,\mu) = D(\lambda\alpha,\kappa\alpha) \\ &(X')^\beta = S(\kappa,\lambda,\mu)X^\beta S^\dagger(\kappa,\lambda,\mu) = D(\nu\beta,\mu\beta) \\ &\kappa\nu-\lambda\mu = 1; \quad \kappa,\lambda,\mu,\nu\in\mathrm{GF}(p^\ell). \end{aligned} \tag{52}$$

These transformations preserve equation (41):

$$(X')^\beta(Z')^\alpha = (Z')^\alpha(X')^\beta\omega[-\mathrm{Tr}(\alpha\beta)]; \qquad \alpha,\beta\in\mathrm{GF}(p^\ell). \tag{53}$$

They contain four variables but because of the constraint there are three independent variables. Since the variables belong to a field, for a given triplet κ,λ,μ (with $\kappa\neq 0$), there exist $\nu = \kappa^{-1}(\lambda\mu+1)$ which satisfies the constraint. We can easily show that these transformations form a group, which we call $\mathrm{Sp}(2,\mathrm{GF}(p^\ell))$. In the language of finite geometry (which is the phase space of these systems), we perform rotations.

In [10], we have given an analytical expression for the symplectic operators S in equation (58), for the case of systems with a dimension which is a prime number. The same formulae with an extra trace in the exponentials are also valid here. To summarize the result, we introduce the following special cases of symplectic operators:

$$\begin{aligned} &S(\xi_3,0,0) = \sum_m |X;\xi_3 m\rangle\langle X;m| = \sum_n \left|P;\xi_3^{-1}m\right\rangle\langle P;m| \\ &S(1,\xi_2,0) = \sum_m \omega[\mathrm{Tr}(2^{-1}\xi_2 m^2)]|X;m\rangle\langle X;m| \\ &S(1,0,\xi_1) = \sum_m \omega[\mathrm{Tr}(-2^{-1}\xi_1 m^2)]|P;m\rangle\langle P;m| \end{aligned} \tag{54}$$

where $m \in \mathrm{GF}(p^\ell)$. The general symplectic operator $S(\kappa, \lambda, \mu)$ is given by

$$\begin{aligned} &S(\kappa, \lambda, \mu) = S(1, 0, \xi_1)S(1, \xi_2, 0)S(\xi_3, 0, 0) \\ &\xi_1 = \mu\kappa(1 + \lambda\mu)^{-1} \qquad \xi_2 = \lambda\kappa^{-1}(1 + \lambda\mu) \qquad \xi_3 = \kappa(1 + \lambda\mu)^{-1}. \end{aligned} \tag{55}$$

For later use we point out that the operators $S(\xi_3, 0, 0)$ for all values of ξ_3 form a subgroup of $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$, and the same is true for the operators $S(1, \xi_2, 0)$, and also for the operators $S(1, 0, \xi_1)$. Related symplectic transformations from an abstract mathematical point of view have been studied in [27–30].

We next show that

$$S(\kappa, \lambda, \mu)D(\alpha, \beta)S^\dagger(\kappa, \lambda, \mu) = D(\alpha\nu + \beta\lambda, \alpha\mu + \beta\kappa). \tag{56}$$

The symplectic operators acting on H cannot be expressed as a simple tensor product of symplectic operators $\mathcal{S}$ acting on the various p-dimensional Hilbert spaces $\mathcal{H}$ (not even in simple special cases). We have seen the analogue of this for the displacement operators in equation (43), but here the situation is more complex. The root of this complexity is the trace in Fourier transform of equation (30). In order to get more insight into this, we discuss below a different type of symplectic transformations and explain that they are different from those in equation (52).

5.1. *Their relation to* $\mathrm{Sp}(2\ell, \mathcal{Z}_p)$ *symplectic transformations*

We introduce the displacement operators

$$\begin{aligned} &\mathbb{X}_i \equiv X^{\epsilon^i} = \mathbf{1} \otimes \cdots \otimes \mathbf{1} \otimes \mathcal{X} \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1} \\ &\mathbb{Z}_i \equiv Z^{E_i} = \mathbf{1} \otimes \cdots \otimes \mathbf{1} \otimes \mathcal{Z} \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1} \end{aligned} \tag{57}$$

which act on the i-Hilbert space $\mathcal{H}$ only. We stress that the transformation from X, Z and their powers to $\mathbb{X}_1, \mathbb{Z}_1, \ldots, \mathbb{X}_{\ell-1}, \mathbb{Z}_{\ell-1}$ is *not* a $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ symplectic transformation (the product $-E_i\epsilon^i$ is not 1).

The operators $\mathbb{X}_i, \mathbb{Z}_i$ are related to each other through the Fourier transform $\mathcal{F} \otimes \cdots \otimes \mathcal{F}$. In this paper, we use the Fourier transform of equation (30) which has the Galois trace in it. All our results depend on g_{ij} which is intimately connected to the choice of the irreducible polynomial and the Galois multiplication. Consequently, the Galois theory is deeply embedded into our construction.

We briefly introduce symplectic transformations for the operators $\mathbb{X}_1, \mathbb{Z}_1, \ldots, \mathbb{X}_{\ell-1}, \mathbb{Z}_{\ell-1}$ so that it becomes clear that they are different from the symplectic transformations of equation (52) which are relevant to this paper. They are defined as

$$\begin{aligned} &\mathbb{Z}'_i = S\mathbb{Z}_i S^\dagger = \mathcal{D}(\lambda_{0i}, \kappa_{0i}) \otimes \cdots \otimes \mathcal{D}(\lambda_{\ell-1,i}, \kappa_{\ell-1,i}) \\ &\mathbb{X}'_i = S\mathbb{X}_i S^\dagger = \mathcal{D}(\nu_{0i}, \mu_{0i}) \otimes \cdots \otimes \mathcal{D}(\nu_{\ell-1,i}, \mu_{\ell-1,i}) \end{aligned} \tag{58}$$

where the parameters $\lambda_{ji}, \kappa_{ji}, \mu_{ji}, \nu_{ji}$ are integers in $\mathcal{Z}_p$. We require that these transformations preserve equation (9) and also that for $i \neq k$ the $\mathbb{X}'_i, \mathbb{Z}'_i$ commute with the $\mathbb{X}'_k, \mathbb{Z}'_k$.

This requirement leads to the constraints

$$\begin{aligned} &\sum_{j=0}^{\ell-1}(\kappa_{ji}\lambda_{jk} - \lambda_{ji}\kappa_{jk}) = 0 \\ &\sum_{j=0}^{\ell-1}(\mu_{ji}\nu_{jk} - \nu_{ji}\mu_{jk}) = 0 \\ &\sum_{j=0}^{\ell-1}(\kappa_{ji}\nu_{jk} - \lambda_{ji}\mu_{jk}) = \delta(i, k). \end{aligned} \tag{59}$$

There are $4\ell^2$ integers in $\mathcal{Z}_p$ in these transformations and $2\ell^2 - \ell$ constraints. Therefore, there are $2\ell^2 + \ell$ independent integer parameters. These transformations form the symplectic $\mathrm{Sp}(2\ell, \mathcal{Z}_p)$ group. In the special case,

$$\kappa_{ji} = \lambda_{ji} = \mu_{ji} = \nu_{ji} = 0; \qquad i \neq j, \tag{60}$$

the above transformations form the $\mathrm{Sp}(2, \mathcal{Z}_p) \times \cdots \times Sp(2, \mathcal{Z}_p)$ subgroup of 'independent symplectic transformations in each of the ℓ subsystems'.

This clarifies the difference between the $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ symplectic transformations on X, Z and the $\mathrm{Sp}(2\ell, \mathcal{Z}_p)$ symplectic transformations on $\mathbb{X}_1, \mathbb{Z}_1, \ldots, \mathbb{X}_{\ell-1}, \mathbb{Z}_{\ell-1}$. The $\mathrm{Sp}(2, \mathcal{Z}_p) \times \cdots \times Sp(2, \mathcal{Z}_p)$ is a subgroup of $\mathrm{Sp}(2\ell, \mathcal{Z}_p)$.

5.2. Radon transforms

Acting with the symplectic operator $S(\kappa, \lambda, \mu)$ on both sides of equation (45), we get

$$\begin{aligned} \frac{1}{d}\sum_{\epsilon,\zeta} D(\epsilon, \zeta)\delta(\kappa\epsilon - \lambda\zeta, \alpha) &= |P'; 2^{-1}\alpha\rangle\langle P'; -2^{-1}\alpha| \\ \frac{1}{d}\sum_{\epsilon,\zeta} D(\epsilon, \zeta)\delta(-\mu\epsilon + \nu\zeta, \beta) &= |X'; 2^{-1}\beta\rangle\langle X'; -2^{-1}\beta| \end{aligned} \tag{61}$$

where the 'prime states' are related to the original ones through the symplectic transform

$$|X'; 2^{-1}\beta\rangle = S(\kappa, \lambda, \mu)|X; 2^{-1}\beta\rangle; \qquad |P'; 2^{-1}\beta\rangle = S(\kappa, \lambda, \mu)|P; 2^{-1}\beta\rangle. \tag{62}$$

In these equations, we sum over all points on the lines $\kappa\epsilon - \lambda\zeta = \alpha$ and $-\mu\epsilon + \nu\zeta = \beta$. The summation along one of the lines is the analogue in our context of the integration of a two-dimensional function $f(x, y)$ along a line in the Euclidean plane x–y which is the Radon transform. Therefore, equation (61) are the Radon transform in a finite geometry.

In a similar way, we act with the symplectic operator $S(\kappa, \lambda, \mu)$ on both sides of equation (50) and we get

$$\begin{aligned} \frac{1}{d}\sum_{\epsilon,\zeta} P(\epsilon, \zeta)\delta(\kappa\epsilon - \lambda\zeta, \alpha) &= |P'; \alpha\rangle\langle P'; \alpha| \\ \frac{1}{d}\sum_{\epsilon,\zeta} P(\epsilon, \zeta)\delta(-\mu\epsilon + \nu\zeta, \beta) &= |X'; \beta\rangle\langle X'; \beta|. \end{aligned} \tag{63}$$

These relations can be used for quantum tomography in finite quantum systems. A general tomography algorithm for all finite quantum systems has been presented in [31]. In the case of Galois quantum systems, we can define and use as observables the projectors on the right-hand side of equation (63) which are along the various directions of the finite geometry which is the phase space of these systems.

6. Frobenius transformations

The Frobenius transformations of equation (14) map Galois conjugates to each other. The implications of this in our context is that the full Hilbert space splits naturally into 'Frobenius subspaces' comprised by states labelled with Galois conjugates. In this section, we introduce these subspaces and study transformations which leave them invariant.

The subfields of $\mathrm{GF}(p^\ell)$ are all $\mathrm{GF}(p^r)$ where r is a divisor of ℓ. For simplicity, in this and the next section we assume that ℓ is a prime number, and then there is only one proper subfield $\mathcal{Z}_p$. In this case, $y^{p^\ell} - y$ is the product of all distinct irreducible polynomials of

degree 1 and ℓ. There are $(p^\ell - p)/\ell$ irreducible polynomials of degree ℓ, and to each of them correspond ℓ Galois conjugates to each other. In addition to that we have p polynomials of degree 1, they are $x - m$ where $m \in \mathcal{Z}_p$ (they are Galois self-conjugates).

We split the Hilbert space H into subspaces, each of which is spanned by the states $|X; \alpha\rangle$ where α are Galois conjugates to each other. We recall here that Galois conjugates have the same trace, because this is needed for the proof of some of the formulae below. We label each of these subspaces with the corresponding irreducible polynomial:

$$\begin{aligned} &H_X[f(y)] = \text{span}\{|X; m\rangle, |X; m^p\rangle, \ldots, |X; m^{p^{\ell-1}}\rangle\} \\ &f(y) = (y-m)(y-m^p)\cdot(y-m^{p^{\ell-1}}). \end{aligned} \tag{64}$$

The index X is used to indicate that in the definition we use the states $|X; m\rangle$. If we use the states $|P; m\rangle$, we get different subspaces which we denote as $H_P[f(y)]$. We call them X- and P-Frobenius subspaces, correspondingly. For prime ℓ, there are $(p^\ell - p)/\ell$ X-Frobenius subspaces which are ℓ-dimensional, and p which are one-dimensional. The Hilbert space H is the direct sum of all X-Frobenius subspaces.

We call $\Pi_X[f(y)]$ the projection operators into $H_X[f(y)]$ and $\Pi_P[f(y)]$ the projection operators into $H_P[f(y)]$. The space $H_X[f(y)]$ is the null space of the operator $f(\hat{x})$ and $H_P[f(y)]$ is the null space of the operator $f(\hat{p})$. Therefore,

$$f(\hat{x})\Pi_X[f(y)] = 0; \qquad f(\hat{p})\Pi_P[f(y)] = 0. \tag{65}$$

An example is presented in the appendix.

Motivated by the Frobenius map $\sigma(\alpha) = \alpha^p$, we consider the unitary transformations

$$\mathcal{G} \equiv \sum_m |X; m^p\rangle\langle X; m| = \sum_m |P; m^p\rangle\langle P; m|. \tag{66}$$

We call them Frobenius transformations. The above equality can be proved if we express the momentum states as the Fourier transform of the position states (equation (32)) and use equation (28). We can show that

$$\mathcal{G}\mathcal{G}^\dagger = \mathbf{1}; \qquad \mathcal{G}^\ell = \mathbf{1}; \qquad [\mathcal{G}, F] = 0. \tag{67}$$

The $\{\mathbf{1}, \mathcal{G}, \ldots, \mathcal{G}^{\ell-1}\}$ form a cyclic group of order ℓ. The X-Frobenius subspaces $H_X[f(y)]$ (and also the P-Frobenius subspaces $H_P[f(y)]$) are invariant under the $\mathcal{G}$ transformations

$$[\mathcal{G}, \Pi_X[f(y)]] = [\mathcal{G}, \Pi_X[f(y)]] = 0. \tag{68}$$

We next show that

$$\mathcal{G}^i X^\beta (\mathcal{G}^\dagger)^i = X^{\beta^{p^i}}; \qquad \mathcal{G}^i Z^\alpha (\mathcal{G}^\dagger)^i = Z^{\alpha^{p^i}} \tag{69}$$

and more generally that

$$\begin{aligned} &\mathcal{G}^i D(\alpha, \beta)(\mathcal{G}^\dagger)^i = D\big(\alpha^{p^i}, \beta^{p^i}\big) \\ &\mathcal{G}^i S(\kappa, \lambda, \mu)(\mathcal{G}^\dagger)^i = S\big(\kappa^{p^i}, \lambda^{p^i}, \mu^{p^i}\big). \end{aligned} \tag{70}$$

Clearly for parameters in $\mathcal{Z}_p\mathcal{G}$ commutes with $D(\alpha, \beta)$ and $S(\kappa, \lambda, \mu)$.

7. Galois subsystems

In this section, we construct explicitly a Galois subsystem with Hilbert space h, where the position and momentum take values in the subfield $\mathcal{Z}_p$. We also compare and contrast displacement and symplectic transformations Θ in the two spaces. In order to do this we start with transformations Θ in H, we restrict the variables of Θ into the subfield $\mathcal{Z}_p$ and

calculate the projection $\varpi\Theta\varpi$, where ϖ is the projection operator from H to h. We will show that the projection of displacements in H are displacements in h. For the symplectic transformations, we will show that in some special cases (not always) the projection is a symplectic transformation in h. After we have constructed explicitly one Galois subsystem, we can get many of them with unitary transformations.

We consider the direct sum of the p one-dimensional X-Frobenius spaces $H_X[y-\alpha]$ where α belongs to the base field $\mathcal{Z}_p$:

$$h = \sum_{\alpha\in\mathcal{Z}_p} H_X[y-\alpha] = \text{span}\{|X;\alpha\rangle = |\mathcal{X};\alpha\rangle \otimes |\mathcal{X};0\rangle \otimes \cdots \otimes |\mathcal{X};0\rangle\}. \tag{71}$$

This is an example of a Galois subsystem. The projection operator ϖ into h is given by

$$\varpi = \sum_{\alpha\in\mathcal{Z}_p} \Pi_X[y-\alpha] = \mathbf{1} \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0|. \tag{72}$$

We next consider Fourier transforms and show that

$$\varpi F \varpi = \sum_{m,n\in\mathcal{Z}_p} \omega(\mathcal{E}_0 mn)|\mathcal{X};m\rangle\langle\mathcal{X};n| \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \tag{73}$$

where $\mathcal{E}_0 = \text{Tr}\,1 = \ell$. We first consider the case $\mathcal{E}_0 \neq 0$ (ℓ different than a multiple of p) and we see that $\varpi F\varpi$ is effectively $\mathcal{F} \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0|$ with the only difference that instead of ω it contains $\omega^{\mathcal{E}_0}$. Mathematically, the two are connected with a symplectic transformation as follows:

$$\begin{aligned} &\varpi F\varpi = [\mathcal{S}(\mathcal{E}_0,0,0)\mathcal{F}] \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \\ &\mathcal{S}(\kappa,0,0) = \sum_{m\in\mathcal{Z}_p} |\mathcal{X};\kappa m\rangle\langle\mathcal{X};m|; \qquad \kappa \in \mathcal{Z}_p. \end{aligned} \tag{74}$$

This clarifies the relation between Fourier transforms in H and Fourier transforms in h.

We stress here that the momentum states $|P,m\rangle$, introduced through the Fourier transform F in equation (32), even when $m \in \mathcal{Z}_p$, are mostly outside the space h. Indeed, for $m \in \mathcal{Z}_p$ we get $M_i = m\mathcal{E}_i$ and equation (33) shows that

$$|P;m\rangle = F|X;m\rangle = |\mathcal{P};m\mathcal{E}_0\rangle \otimes \cdots \otimes |\mathcal{P};m\mathcal{E}_{\ell-1}\rangle; \qquad m \in \mathcal{Z}_p. \tag{75}$$

In contrast to this if we act with the Fourier transform $\mathcal{F} \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0|$ on $|X;m\rangle$ (with $m \in \mathcal{Z}_p$) we get $|\mathcal{P};m\rangle \otimes |\mathcal{X};0\rangle \otimes \cdots \otimes |\mathcal{X};0\rangle$ which belongs to h, and similarly if we act with the Fourier transform of equation (73) on $|X;m\rangle$ we get the state $|\mathcal{P};m\mathcal{E}_0\rangle \otimes |\mathcal{X};0\rangle \otimes \cdots \otimes |\mathcal{X};0\rangle$.

7.1. Displacements

Using equation (43), we show that for $\alpha, \beta \in \mathcal{Z}_p$ (and for $\mathcal{E}_0 \neq 0$)

$$\begin{aligned} &D(\alpha,\beta)\varpi = \mathcal{D}(\alpha\mathcal{E}_0,\beta) \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \\ &[D(\alpha,\beta),\varpi] = [P(\alpha,\beta),\varpi] = 0. \end{aligned} \tag{76}$$

When α takes all values in $\mathcal{Z}_p$, $\alpha\mathcal{E}_0$ also takes all values in $\mathcal{Z}_p$. This equation shows that the projection of displacements in H are displacements in h.

We also compare and contrast the marginal properties of the displacements in these two spaces. Using equation (76), we prove that for $\alpha, \beta \in \mathcal{Z}_p$ (and $\mathcal{E}_0 \neq 0$)

$$\begin{aligned}
&\frac{1}{p}\sum_{\alpha\in\mathcal{Z}_p} D(\alpha,\beta)\varpi = |X; 2^{-1}\beta\rangle\langle X; -2^{-1}\beta|; \qquad \beta \in \mathcal{Z}_p \\
&\frac{1}{p}\sum_{\beta\in\mathcal{Z}_p} D(\alpha,\beta)\varpi = |R(2^{-1}\alpha\mathcal{E}_0)\rangle\langle R(-2^{-1}\alpha\mathcal{E}_0)|; \qquad \alpha \in \mathcal{Z}_p \\
&\frac{1}{p}\sum_{\alpha,\beta\in\mathcal{Z}_p} D(\alpha,\beta)\varpi = \mathcal{P}(0,0)\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|\otimes\cdots\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|
\end{aligned} \tag{77}$$

where

$$|R(\alpha)\rangle \equiv |\mathcal{P};\alpha\rangle\otimes|\mathcal{X};0\rangle\otimes\cdots\otimes|\mathcal{X};0\rangle. \tag{78}$$

These relations should be compared and contrasted with equation (45). Multiplication with the parity operator of equation (46) gives the marginal properties of the displaced parity operators in the space h:

$$\begin{aligned}
&\frac{1}{p}\sum_{\alpha\in\mathcal{Z}_p} P(\alpha,\beta)\varpi = |X;\beta\rangle\langle X;\beta|; \qquad \beta \in \mathcal{Z}_p \\
&\frac{1}{p}\sum_{\beta\in\mathcal{Z}_p} P(\alpha,\beta)\varpi = |R(\alpha\mathcal{E}_0)\rangle\langle R(\alpha\mathcal{E}_0)|; \qquad \alpha \in \mathcal{Z}_p \\
&\frac{1}{p}\sum_{\alpha,\beta\in\mathcal{Z}_p} P(\alpha,\beta)\varpi = \mathbf{1}\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|\otimes\cdots\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|
\end{aligned} \tag{79}$$

where $\alpha, \beta \in \mathcal{Z}_p$ (and $\mathcal{E}_0 \neq 0$). These relations should be compared and contrasted with equation (50) which give the marginal properties of the displaced parity operators in the space H.

In the case $\ell = p$, we consider instead of the space of equation (71), the space

$$h' = \text{span}\{|X;\alpha\epsilon\rangle = |\mathcal{X};0\rangle\otimes|\mathcal{X};\alpha\rangle\otimes|\mathcal{X};0\rangle\otimes\cdots\otimes|\mathcal{X};0\rangle\} \tag{80}$$

where $\alpha \in \mathcal{Z}_p$, and we repeat the above argument. For example, if ϖ' is the projection operator in h', we can show that $\varpi' F \varpi'$ is effectively $|\mathcal{X};0\rangle\langle\mathcal{X};0|\otimes\mathcal{F}\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|\otimes\cdots\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|$ with the only difference that instead of ω it contains $\omega^{\mathcal{E}_2}$. In this way, we avoid the difficulty with $\mathcal{E}_0 = 0$.

7.2. *Symplectic transformations*

We first consider the subgroup of symplectic transformations comprised by the operators $S(1,\xi_2,0)$ with $\xi_2 \in \mathcal{Z}_p$ and show that

$$\begin{aligned}
&S(1,\xi_2,0)\varpi = \mathcal{S}(1,\xi_2\mathcal{E}_0,0)\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|\otimes\cdots\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0| \\
&[S(1,\xi_2,0),\varpi] = 0.
\end{aligned} \tag{81}$$

Similarly, we consider the subgroup of symplectic transformations comprised by the operators $S(\xi_3,0,0)$ with $\xi_3 \in \mathcal{Z}_p$ and show that

$$\begin{aligned}
&S(\xi_3,0,0)\varpi = \mathcal{S}(\xi_3,0,0)\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0|\otimes\cdots\otimes|\mathcal{X};0\rangle\langle\mathcal{X};0| \\
&[S(\xi_3,0,0),\varpi] = 0.
\end{aligned} \tag{82}$$

These two equations show that in these cases the projection of symplectic transformations in H are symplectic transformations in h. We next show that $\varpi S(1,0,\xi_1)\varpi$ with $\xi_1 \in \mathcal{Z}_p$, is *not* a symplectic transformation in h:

$$\begin{aligned} &\varpi S(1,0,\xi_1)\varpi = U \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \otimes \cdots \otimes |\mathcal{X};0\rangle\langle\mathcal{X};0| \\ &U = p^{(1-\ell)} \sum_{m\in \mathrm{GF}(p^\ell)} \omega[-2^{-1}\xi_1 \operatorname{Tr}(m^2)]|\mathcal{P};M_0\rangle\langle\mathcal{P};M_0| \\ &M_0 = \operatorname{Tr}(m). \end{aligned} \tag{83}$$

7.3. Wigner and Weyl functions

Wigner and Weyl functions for finite quantum systems have been studied in [7, 9, 10, 21, 32]. The Weyl functions $\tilde{W}(\alpha,\beta)$ are intimately connected to the displacement operators and the Wigner functions $W(\alpha,\beta)$ to the displaced parity operators. For a density matrix ρ they are given by

$$\tilde{W}(\alpha,\beta) = \operatorname{Tr}[\rho D(\alpha,\beta)]; \qquad W(\alpha,\beta) = \operatorname{Tr}[\rho P(\alpha,\beta)]. \tag{84}$$

The properties of the displacement operators and of the displaced parity operators studied earlier lead to analogous properties of the Weyl and Wigner functions (simply by multiplying with the density matrix and by taking the trace). For example, equation (51) will lead to the result that the Wigner and Weyl functions are related through a two-dimensional Fourier transform, equation (45) will lead to marginal properties for the Weyl functions and equation (50) will lead to marginal properties for the Wigner functions.

We are interested to use Wigner and Weyl functions in the context of the relationship of a subsystem with the full system. If ρ is the density matrix of a system described with the Hilbert space H, its projection in h is described with the (normalized) density matrix

$$\rho_{\mathrm{sub}} = \frac{\varpi\rho\varpi}{\operatorname{Tr}[\varpi\rho]}. \tag{85}$$

Let $\tilde{W}(\alpha,\beta)$ be the Weyl function of the full system (with $\alpha,\beta \in \mathrm{GF}(p^\ell)$) and $\tilde{W}_{\mathrm{sub}}(\alpha,\beta)$ be the Weyl function of its projection in h (with $\alpha,\beta \in \mathcal{Z}_p$). Taking the trace of the operators in equation (77) times ρ, we get

$$\begin{aligned} &\frac{1}{p}\sum_{\alpha\in\mathcal{Z}_p} \tilde{W}_{\mathrm{sub}}(\alpha,\beta) = \frac{1}{\operatorname{Tr}(\rho\varpi)}\langle X;-2^{-1}\beta|\rho|X;2^{-1}\beta\rangle; \qquad \beta\in\mathcal{Z}_p \\ &\frac{1}{p}\sum_{\beta\in\mathcal{Z}_p} \tilde{W}_{\mathrm{sub}}(\alpha,\beta) = \frac{1}{\operatorname{Tr}(\rho\varpi)}\langle R(-2^{-1}\alpha\mathcal{E}_0)|\rho|R(2^{-1}\alpha\mathcal{E}_0)\rangle; \qquad \alpha\in\mathcal{Z}_p \end{aligned} \tag{86}$$

where the state $|R(\alpha)\rangle$ has been given in equation (78). For the Wigner function we take the trace of the operators in equation (79) times ρ:

$$\begin{aligned} &\frac{1}{p}\sum_{\alpha\in\mathcal{Z}_p} W_{\mathrm{sub}}(\alpha,\beta) = \frac{1}{\operatorname{Tr}(\rho\varpi)}\langle X;\beta|\rho|X;\beta\rangle; \qquad \beta\in\mathcal{Z}_p \\ &\frac{1}{p}\sum_{\beta\in\mathcal{Z}_p} W_{\mathrm{sub}}(\alpha,\beta) = \frac{1}{\operatorname{Tr}(\rho\varpi)}\langle R(\alpha\mathcal{E}_0)|\rho|R(\alpha\mathcal{E}_0)\rangle; \qquad \alpha\in\mathcal{Z}_p. \end{aligned} \tag{87}$$

These relations give the marginal properties of the Wigner and Weyl functions for the projection of the system in h described with the (normalized) density matrix ρ_{sub} in terms of probabilities associated with the full system.

8. Discussion

Galois quantum systems have stronger properties than other finite quantum systems. Position and momentum take values in a field and the corresponding phase space is a finite geometry. Consequently, we can define symplectic transformations which form a group, Radon transforms, tomographic techniques, etc. Most of the properties used in the harmonic oscillator phase space can be extended in the context of Galois quantum systems.

Field extension is a technique that constructs large fields from smaller ones. We started from quantum systems where the position and momentum take values in a small field and using field extension we constructed quantum systems where the position and momentum take values in a large field. The Hilbert space H is the tensor product $\mathcal{H}\otimes\cdots\otimes\mathcal{H}$. But we have stressed that the Galois trace enters in the Fourier transform, and consequently F is different from $\mathcal{F}\otimes\cdots\otimes\mathcal{F}$. In equation (43), we have explained the connection between displacements in H and displacements within the various Hilbert spaces $\mathcal{H}$.

In section 5, we have studied the $\mathrm{Sp}(2,\mathrm{GF}(p^{\ell}))$ group of symplectic transformations. They are intimately connected to rotations in the finite geometry which is the phase space of these systems. We have also explained the difference between the $\mathrm{Sp}(2,\mathrm{GF}(p^{\ell}))$ group and the $\mathrm{Sp}(2\ell,\mathcal{Z}_p)$ group of symplectic transformations.

The next step was to transfer some important features of Galois theory into the quantum context. And the most basic ones are Frobenius maps among Galois conjugates and the relationship between a big field with its subfields. In section 7, we have introduced the Frobenius subspaces which are invariant under the Frobenius transformations. In section 8, we have studied the relationship of a large Galois quantum system with its subsystems (where the position and momentum take values in a subfield). In the language of the finite geometry phase space, this corresponds to the relationship between a large finite geometry and its subgeometries. We have shown in equation (76) that the projection of displacements in H are displacements in h. The marginal properties of the displacement operators (and also of the displaced parity operators) in the two spaces have been compared and contrasted (equations (77), (45) and also equations (79), (50)). For the symplectic transformations we have shown that in some cases (equations (81), (82)), but not always (equation (83)), the projection from H to h is a symplectic transformation. In this part of the paper we have considered for simplicity prime ℓ, in which case there is only one proper subfield of $\mathrm{GF}(p^{\ell})$ the $\mathcal{Z}_p$. In general there is a more complicated 'Russian doll' type of structure, where we have many subfields one inside the other. Such structure can be transferred into the corresponding quantum systems.

Galois fields and the theory of polynomials are a deep branch of mathematics which has also important applications in classical information processing. Quantum systems and quantum phase space methods (and the related area of applied harmonic analysis) are a totally different subject. In Galois quantum systems, we have blended these two areas and this is interesting from an academic point of view; and at the same time it might have applications to areas such as quantum maps [33], the magnetic translation group in condensed matter, quantum information processing, etc.

Appendix

We consider the Galois fields GF(9) (where $p=3,\ell=2$) and calculate the matrix g which enters in the calculation of the trace, and the Frobenius subspaces. The irreducible polynomials are y, $y-1$, $y-2$, y^2+1, y^2+y+2, y^2+2y+2 and

$$y^9-y=y(y-1)(y-2)(y^2+1)(y^2+y+2)(y^2+2y+2) \tag{A.1}$$

where all the coefficients are in $\mathcal{Z}_3$. The practical calculations depend on the choice of the irreducible polynomial, although various choices lead to isomorphic results. Below we present results for two irreducible polynomials.

A.1. The polynomial $\epsilon^2 + \epsilon + 2$

Here, we choose the irreducible polynomial $\epsilon^2 + \epsilon + 2$. For this irreducible polynomial, we easily find that

$$\mathcal{E}_0 = -1; \qquad \mathcal{E}_1 = -1; \qquad \mathcal{E}_2 = 0 \tag{A.2}$$

and also that

$$g = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}; \qquad G = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}. \tag{A.3}$$

The dual basis is in this case $E_0 = 2\epsilon$ and $E_1 = 2 + \epsilon$. As an example we mention that $1 + \epsilon = E_0 - E_1$.

There are three pairs of Galois conjugates which are given below together with the corresponding irreducible polynomial:

$$\begin{aligned} (1+\epsilon, 2\epsilon) \quad &\leftrightarrow \quad y^2 + 2y + 2 \\ (\epsilon, 2+2\epsilon) \quad &\leftrightarrow \quad y^2 + y + 2 \\ (1+2\epsilon, 2+\epsilon) \quad &\leftrightarrow \quad y^2 + 1. \end{aligned} \tag{A.4}$$

The Hilbert space H splits into six Frobenius subspaces as follows:

$$\begin{aligned} &H_X[y] = \{|X;0\rangle\}; \qquad H_X[y-1] = \{|X;1\rangle\}; \quad H_X[y-2] = \{|X;2\rangle\} \\ &H_X[y^2+2y+2] = \mathrm{span}\{|X;1+\epsilon\rangle, |X;2\epsilon\rangle\} \\ &H_X[y^2+y+2] = \mathrm{span}\{|X;\epsilon\rangle, |X;2+2\epsilon\rangle\} \\ &H_X[y^2+1] = \mathrm{span}\{|X;1+2\epsilon\rangle, |X;2+\epsilon\rangle\}. \end{aligned} \tag{A.5}$$

According to equation (65), we have

$$\begin{aligned} &\hat{x}\Pi_X[y] = 0 \\ &(\hat{x}-1)\Pi_X[y-1] = 0 \\ &(\hat{x}-2)\Pi_X[y-2] = 0 \\ &(\hat{x}^2+2\hat{x}+2)\Pi_X[y^2+2y+2] = 0 \\ &(\hat{x}^2+\hat{x}+2)\Pi_X[y^2+y+2] = 0 \\ &(\hat{x}^2+1)\Pi_X[y^2+1] = 0. \end{aligned} \tag{A.6}$$

The displacement operators Z and X can be written in terms of the projection operators to the various Frobenius spaces as

$$\begin{aligned} Z = {} & (\Pi_X[y] + \Pi_X[y^2+1]) + \omega^{-1}(\Pi_X[y-1] + \Pi_X[y^2+y+2]) \\ & + \omega(\Pi_X[y-2] + \Pi_X[y^2+2y+2]) \\ X = {} & (\Pi_P[y] + \Pi_P[y^2+1]) + \omega^{-1}(\Pi_P[y-1] + \Pi_P[y^2+y+2]) \\ & + \omega(\Pi_P[y-2] + \Pi_P[y^2+2y+2]). \end{aligned} \tag{A.7}$$

A consequence of the degeneracy is that an eigenvector of Z is not necessarily eigenvector of Z^ϵ which can be written as

$$Z^{\epsilon} = (|X;0\rangle\langle X;0| + |X;\epsilon\rangle\langle X;\epsilon| + |X;2\epsilon\rangle\langle X;2\epsilon|)$$
$$+\omega^{-1}(|X;1\rangle\langle X;1| + |X;1+\epsilon\rangle\langle X;1+\epsilon| + |X;1+2\epsilon\rangle\langle X;1+2\epsilon|)$$
$$+\omega(|X;2\rangle\langle X;2| + |X;2+\epsilon\rangle\langle X;2+\epsilon| + |X;2+2\epsilon\rangle\langle X;2+2\epsilon|). \tag{A.8}$$

For example, $2^{-1/2}[|X;0\rangle + |X;1+2\epsilon\rangle]$ is an eigenvector of Z, but is not an eigenvector of Z^{ϵ}.

A.2. The polynomial $\epsilon^2 + 2\epsilon + 2$

Here, we choose the irreducible polynomial $\epsilon^2 + 2\epsilon + 2$. For this irreducible polynomial, we easily find that

$$\mathcal{E}_0 = -1; \qquad \mathcal{E}_1 = 1; \qquad \mathcal{E}_2 = 0 \tag{A.9}$$

and

$$g = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}; \qquad G = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \tag{A.10}$$

The dual basis is in this case $E_0 = \epsilon$ and $E_1 = 1 + \epsilon$.

There are three pairs of Galois conjugates which are given below together with the corresponding irreducible polynomial:

$$\begin{aligned} &(\epsilon, 1+2\epsilon) \quad \leftrightarrow \quad y^2 + 2y + 2 \\ &(2\epsilon, 2+\epsilon) \quad \leftrightarrow \quad y^2 + y + 2 \\ &(1+\epsilon, 2+2\epsilon) \quad \leftrightarrow \quad y^2 + 1. \end{aligned} \tag{A.11}$$

The Hilbert space H splits into six Frobenius subspaces as follows:

$$\begin{aligned} &H_X[y] = \{|X;0\rangle\}; \qquad H_X[y-1] = \{|X;1\rangle\}; \qquad H_X[y-2] = \{|X;2\rangle\} \\ &H_X[y^2 + 2y + 2] = \text{span}\{|X;\epsilon\rangle, |X;1+2\epsilon\rangle\} \\ &H_X[y^2 + y + 2] = \text{span}\{|X;2\epsilon\rangle, |X;2+\epsilon\rangle\} \\ &H_X[y^2 + 1] = \text{span}\{|X;1+\epsilon\rangle, |X;2+2\epsilon\rangle\}. \end{aligned} \tag{A.12}$$

The displacement operators Z and X can be expressed in terms of the projection operators to the various Frobenius spaces, in exactly the same way as in equation (A.7). But the vectors which belong to a given Frobenius space are here different (in general) from the ones in the previous subsection.

References

[1] Weyl H 1950 *Theory of Groups and Quantum Mechanics* (New York: Dover)
Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 570
Schwinger J 1970 *Quantum Kinematics and Dynamics* (New York: Benjamin)
[2] Auslander L and Tolimieri R 1979 *Bull. Am. Math. Soc.* **1** 847
[3] Hannay J H and Berry M V 1980 *Physica* D **1** 267
[4] Balian R and Itzykson C 1986 *C. R. Acad. Sci.* **303** 773
[5] Mehta M L 1987 *J. Math. Phys.* **28** 781
[6] Fairlie D B, Fletcher P and Zachos C K 1990 *J. Math. Phys.* **31** 1088
[7] Vourdas A 1990 *Phys. Rev.* A **41** 1653
Vourdas A 1991 *Phys. Rev.* A **43** 1564
Vourdas A and Bendjaballah C 1993 *Phys. Rev.* A **47** 3523
Vourdas A 1996 *J. Phys. A: Math. Gen.* **29** 4275
[8] Varadarajan V S 1995 *Lett. Math. Phys.* **34** 319

[9] Leonhardt U 1996 *Phys. Rev.* A **53** 2998
[10] Vourdas A 2004 *Rep. Prog. Phys.* **67** 267
[11] Hirschfeld J W P 1979 *Projective Geometries Over Finite Fields* (Oxford: Oxford University Press)
Batten L M 1997 *Combinatorics of Finite Geometries* (Cambridge: Cambridge University Press)
[12] Klimov A, Sanchez-Soto L and de Guise H 2005 *J. Phys. A: Math. Gen.* **38** 2747
[13] Neuhauser M 2002 *J. Lie Theory* **12** 15
[14] Wootters W K and Fields B D 1989 *Ann. Phys., NY* **191** 363
Gibbons K, Hoffman M J and Wootters W 2004 *Phys. Rev.* A **70** 062101
[15] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512
[16] Pittenger A O and Rubin M H 2004 *Linear Algebra Appl.* **390** 255
Pittenger A O and Rubin M H 2005 *J. Phys. A: Math. Gen.* **38** 6005
[17] Klappenecker A and Rotteler M 2004 *Lect. Notes Comp. Sci.* **2948** 137
[18] Wocjan P and Beth T 2004 *Preprint* quant-ph/0407081
[19] Saniga M, Planat M and Rosu H 2004 *J. Opt. B: Quantum Semiclass. Opt.* **6** L19
Planat M, Rosu H, Perrine S and Saniga M 2004 *Preprint* quant-ph/0409081
[20] Durt T 2005 *J. Phys. A: Math. Gen.* **38** 5267
[21] Calvao E F 2005 *Phys. Rev.* A **71** 042302
[22] Englert B G and Aharonov Y 2001 *Phys. Lett.* A **284** 1
[23] Grassl M and Beth T 2000 *Proc. R. Soc.* A **456** 2689
[24] Asikhmin A and Knill E 2001 *IEEE Trans. Inform. Theor.* **47** 3065
[25] Barnum H, Crepeau C, Gottesman D, Smith A and Tapp A 2002 *Proc. 43th Annual Symposium on Foundations of Computer Science (FOCS) (IEEE Computer Society, Los Alamitos, CA)* pp 449–58
[26] Vourdas A 2002 *Phys. Rev.* A **65** 042321
Vourdas A 2004 *J. Phys. A: Math. Gen.* **37** 3305
[27] Gel'fand I M, Graev M I and Piatetskii-Shapiro I I 1990 *Representation Theory and Automorphic Functions* (London: Academic)
Piatetskii-Shapiro I I 1983 *Complex Representations of $GL(2, K)$ for Finite Fields K* (Providence, RI: American Mathematical Society)
[28] Weil A 1964 *Acta Math.* **111** 143
Weil A 1965 *Acta Math.* **113** 1
[29] Tanaka S 1966 *Osaka J. Math.* **3** 229
Tanaka S 1967 *Osaka J. Math.* **4** 65
[30] Terras A 1999 *Fourier Analysis on Finite Groups and Applications* (Cambridge: Cambridge University Press)
[31] D'Ariano G M, Maccone L and Paris M G A 2001 *J. Phys. A: Math. Gen.* **34** 93
[32] Paz J P 2002 *Phys. Rev.* A **65** 062311
Miquel C, Paz J P, Saraceno M, Knill E, Laflamme R and Negrevergne C 2002 *Nature* **418** 59
[33] Vivaldi F 1992 *Nonlinearity* **5** 133