

Quantum systems with positions and momenta on a Galois field

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

2008 J. Phys.: Conf. Ser. 104 012014

(<http://iopscience.iop.org/1742-6596/104/1/012014>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 38.107.179.213

The article was downloaded on 15/02/2012 at 12:00

Please note that [terms and conditions apply](#).

Quantum systems with positions and momenta on a Galois field

A. Vourdas

Department of Computing, University of Bradford,
Bradford BD7 1DP, United Kingdom

E-mail: A.Vourdas@Bradford.ac.uk

Abstract. Quantum systems with positions and momenta in the Galois field $GF(p^\ell)$, are considered. The Heisenberg-Weyl group of displacements and the $Sp(2, GF(p^\ell))$ group of symplectic transformations, are studied. Frobenius symmetries, are a unique feature of these systems and lead to constants of motion. The engineering of such systems from ℓ spins with $j = (p - 1)/2$, which are coupled in a particular way, is discussed.

1. Introduction

Finite quantum systems where the position and momentum take values in \mathbb{Z}_q (the integers modulo q) have been studied extensively in the literature (for a review with many references see [1]). Their phase space is the toroidal lattice $\mathbb{Z}_q \times \mathbb{Z}_q$ and we can define displacements and the corresponding Heisenberg-Weyl group $HW[\mathbb{Z}_q]$. Difficulties appear if we try to define symplectic transformations (and related concepts like quantum tomography). The root of these difficulties is that \mathbb{Z}_q is in general, a ring. However when q is equal to a prime number p , \mathbb{Z}_p is a field, inverses exist and the symplectic transformations are well-defined.

The algebraic concept of field extension, starts from the field \mathbb{Z}_p and constructs the Galois fields $GF(p^\ell)$. In this paper we study a ‘Galois quantum system’ with positions and momenta in $GF(p^\ell)$ [2, 3] (for a review see [4]). It is comprised of ℓ subsystems each of which is p -dimensional (e.g., ℓ spins with $j = (p - 1)/2$), which are coupled in a special way. This special coupling is related to the special multiplication rule in Galois fields.

There are several motivations for studying Galois quantum systems. The first is that they are finite systems with isotropic phase space in which we can define symplectic transformations (and related techniques like quantum tomography). The second motivation is related to the problem of mutually unbiased bases in finite quantum systems, and is not discussed here [5, 6, 7, 8, 9, 10]. The third motivation is the fact that Galois fields are used extensively in classical information processing and their use in quantum mechanics is the starting point for generalizing these techniques from classical to quantum information processing. The fourth motivation is mathematical and is related to the fact that this work combines ideas from field extension in algebra with quantum mechanics and applied harmonic analysis. It also studies representations of the Heisenberg-Weyl group and the symplectic group over Galois fields.

We stress that the phase space of the harmonic oscillator is a plane (continuum) whilst the phase space of finite systems is a toroidal lattice. In general, lattices have less symmetry than the continuum, but when they are based on Galois fields they are a finite geometry with more

symmetry than the continuum. In Galois quantum systems we can define the Heisenberg-Weyl group and the symplectic group (as in the harmonic oscillator), but we also have for $\ell \geq 2$ the Frobenius symmetry which is a discrete symmetry with no analogue in the harmonic oscillator case.

In this paper we review the work on Galois quantum systems. The aim is to provide a concise description of the physical aspects of these systems, without the technical details of the ‘Galois mathematics’ (which have been presented in [4]).

2. Galois fields

The elements of $GF(p^\ell)$ are the polynomials

$$\alpha = \alpha_0 + \alpha_1\epsilon + \dots + \alpha_{\ell-1}\epsilon^{\ell-1}; \quad \alpha_\lambda \in \mathbb{Z}_p \quad (1)$$

which are defined modulo the irreducible polynomial

$$P(\epsilon) \equiv c_0 + c_1\epsilon + \dots + c_{\ell-1}\epsilon^{\ell-1} + \epsilon^\ell; \quad c_\lambda \in \mathbb{Z}_p \quad (2)$$

The α_λ are the components of α in the basis $\{1, \epsilon, \dots, \epsilon^{\ell-1}\}$.

The $\alpha, \alpha^p, \dots, \alpha^{p^{\ell-1}}$ are Galois conjugates and the trace of α is defined as:

$$\text{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \dots + \alpha^{p^{\ell-1}}; \quad \text{Tr}(\alpha) \in \mathbb{Z}_p \quad (3)$$

We introduce the following symmetric $\ell \times \ell$ matrices with elements in \mathbb{Z}_p [4]

$$g_{\lambda\kappa} \equiv \text{Tr}(\epsilon^{\lambda+\kappa}); \quad G \equiv g^{-1}; \quad \kappa, \lambda = 0, \dots, \ell-1 \quad (4)$$

These matrices are intimately connected to the Galois multiplication rule and the Galois trace, and they will carry later, Galois theory into quantum mechanics.

It is convenient to express the elements of $GF(p^\ell)$ as

$$\alpha = \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \bar{\alpha}_\lambda E_\lambda \quad (5)$$

where $E_\kappa = \sum_\lambda G_{\kappa\lambda} \epsilon^\lambda$ and

$$\alpha_\lambda = \text{Tr}[\alpha E_\lambda]; \quad \bar{\alpha}_\lambda = \text{Tr}[\alpha \epsilon^\lambda] \quad (6)$$

$\{E_\lambda\}$ is a basis ‘dual’ to $\{\epsilon^\lambda\}$ and $\bar{\alpha}_\lambda$ are the dual components of α . We can now express the trace of any product $\alpha\beta$ as:

$$\text{Tr}(\alpha\beta) = \sum_{\lambda,\kappa} g_{\lambda\kappa} \alpha_\lambda \beta_\kappa = \sum_\lambda \alpha_\lambda \bar{\beta}_\lambda = \sum_\lambda \bar{\alpha}_\lambda \beta_\lambda \quad (7)$$

We next define the additive characters:

$$\chi(\alpha) = \omega[\text{Tr}(\alpha)]; \quad \omega(m) = \exp\left(i \frac{2\pi m}{p}\right) \quad (8)$$

and show that

$$\frac{1}{p^\ell} \sum_{\alpha \in GF(p^\ell)} \chi(\alpha\beta) = \delta(\beta, 0); \quad \beta \in GF(p^\ell) \quad (9)$$

3. Finite quantum systems

We consider a quantum system with positions and momenta in \mathbb{Z}_p (where p is an odd prime number). Let $|\mathcal{X}; m\rangle$ (with $m \in \mathbb{Z}_p$) be an orthonormal basis in the p -dimensional Hilbert space \mathcal{H} of this system, which we call ‘position states’.

The Fourier transform is defined as:

$$\mathcal{F} = p^{-1/2} \sum_{m,n \in \mathbb{Z}_p} \omega(mn) |\mathcal{X}; m\rangle \langle \mathcal{X}; n|; \quad \mathcal{F}^4 = \mathbf{1} \quad (10)$$

Acting with the Fourier operator on the position states we get the ‘momentum states’:

$$|\mathcal{P}; m\rangle = \mathcal{F} |\mathcal{X}; m\rangle = p^{-1/2} \sum_{n \in \mathbb{Z}_p} \omega(mn) |\mathcal{X}; n\rangle \quad (11)$$

The position-momentum phase space of this system is the toroidal lattice $\mathbb{Z}_p \times \mathbb{Z}_p$. In this phase space we define the displacement operators

$$\begin{aligned} \mathcal{Z}(\alpha) &= \sum_{n \in \mathbb{Z}_p} \omega(n\alpha) |\mathcal{X}; n\rangle \langle \mathcal{X}; n| \\ \mathcal{X}(\beta) &= \sum_{n \in \mathbb{Z}_p} \omega(-n\beta) |\mathcal{P}; n\rangle \langle \mathcal{P}; n|; \quad \alpha, \beta \in \mathbb{Z}_p \end{aligned} \quad (12)$$

General displacement operators are given by

$$\mathcal{D}(\alpha, \beta) = \mathcal{Z}(\alpha) \mathcal{X}(\beta) \omega(-2^{-1}\alpha\beta) \quad (13)$$

We can show that:

$$\mathcal{D}(\alpha_1, \beta_1) \mathcal{D}(\alpha_2, \beta_2) = \mathcal{D}(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \omega[2^{-1}(\alpha_1\beta_2 - \alpha_2\beta_1)] \quad (14)$$

The operators $\mathcal{D}(\alpha, \beta) \omega(\gamma)$ form a representation of the Heisenberg-Weyl group $HW[\mathbb{Z}_p]$.

4. Galois quantum systems

A Galois quantum system consists of ℓ subsystems each of which has p -dimensional Hilbert space \mathcal{H} . Its Hilbert space H is

$$H = \mathcal{H} \otimes \dots \otimes \mathcal{H} \quad (15)$$

The position states $|X; m\rangle$ where $m = \sum m_\lambda \epsilon^\lambda$ are defined as

$$|X; m\rangle \equiv |\mathcal{X}; m_0\rangle \otimes \dots \otimes |\mathcal{X}; m_{\ell-1}\rangle; \quad m \in GF(p^\ell); \quad m_\lambda \in \mathbb{Z}_p \quad (16)$$

The Fourier transform in H is given by:

$$\begin{aligned} F &= (p^\ell)^{-1/2} \sum_{m,n \in GF(p^\ell)} \chi(mn) |X; m\rangle \langle X; n| \\ &= (p^\ell)^{-1/2} \sum_{m_\lambda, n_\kappa} \omega \left(\sum g_{\lambda\kappa} m_\lambda n_\kappa \right) |\mathcal{X}; m_0\rangle \langle \mathcal{X}; n_0| \otimes \dots \otimes |\mathcal{X}; m_0\rangle \langle \mathcal{X}; n_0| \end{aligned} \quad (17)$$

It is seen that through the matrix g , Galois theory enters into the Fourier transform of these systems. In particular, the non-diagonal elements of g couple the ℓ component systems, in a special way which is intimately connected to the Galois multiplication rule and the Galois trace. This is seen more clearly in the Hamiltonian

$$h(\hat{Q}, \hat{P}) = h(\hat{Q}, F\hat{Q}F^\dagger) \quad (18)$$

where \hat{Q}, \hat{P} are position and momentum operators. The Hamiltonian is a function of \hat{Q} and F and therefore it contains the matrix g which carries Galois theory into the quantum system.

We can construct a Galois quantum system from ℓ spins with $j = (p-1)/2$, if we can couple them in the special way described by the Hamiltonian of Eq.(18).

5. The Heisenberg-Weyl group

The position-momentum phase space of a Galois system is the toroidal lattice $GF(p^\ell) \times GF(p^\ell)$. The displacement operators in this case are given by

$$\begin{aligned} Z(\alpha) &= \sum_{n \in GF(p^\ell)} \chi(\alpha n) |X; n\rangle \langle X; n| \\ X(\beta) &= \sum_{n \in GF(p^\ell)} \chi(-\beta n) |P; n\rangle \langle P; n|; \end{aligned} \quad (19)$$

where $\alpha, \beta \in GF(p^\ell)$. They obey the relation:

$$Z(\alpha)X(\beta) = X(\beta)Z(\alpha)\chi(\alpha\beta). \quad (20)$$

General displacement are defined as:

$$D(\alpha, \beta) = Z(\alpha)X(\beta)\chi(-2^{-1}\alpha\beta); \quad [D(\alpha, \beta)]^\dagger = D(-\alpha, -\beta) \quad (21)$$

We easily show that

$$D(\alpha, \beta)D(\gamma, \delta) = \chi[2^{-1}(\alpha\delta - \beta\gamma)] D(\alpha + \gamma, \beta + \delta) \quad (22)$$

It is seen that Eqs(21),(22) are analogous to Eqs(13),(14) with an extra trace in the characters for the Galois case.

We can express $D(\alpha, \beta)$ in terms of displacement operators \mathcal{D} which act on the various components of the system as:

$$D(\alpha, \beta) = \mathcal{D}(\bar{\alpha}_0, \beta_0) \otimes \dots \otimes \mathcal{D}(\bar{\alpha}_{\ell-1}, \beta_{\ell-1}) \quad (23)$$

The dual components of α appear in this relation, which as we have seen in Eq.(6) contain the matrix g which carries the Galois multiplication rule and the Galois trace into the quantum theory.

6. Symplectic transformations

We consider the following transformations on the operators $Z(\alpha)$ and $X(\beta)$ which lead to the ‘prime operators’ $Z'(\alpha)$ and $X'(\beta)$:

$$\begin{aligned} Z'(\alpha) &= S Z(\alpha) S^\dagger = D(t\alpha, s\alpha) \\ X'(\beta) &= S X(\beta) S^\dagger = D(r\beta, q\beta); \quad q, r, s, t \in GF(p^\ell) \end{aligned} \quad (24)$$

It is easily seen that the $Z'(\alpha)$ and $X'(\beta)$ obey Eq.(20) if

$$qt - rs = 1 \quad (25)$$

Since q, r, s, t belong to the field $GF(p^\ell)$, for any triplet (q, r, s) we can find $t = q^{-1}(1 + rs)$ which obeys Eq.(25). Therefore the operators $S(q, r, s)$ are functions of three independent variables.

The operators $Z'(\alpha)$ and $X'(\beta)$ perform displacements in different directions, in comparison with their counterparts $Z(\alpha)$ and $X(\beta)$. The $GF(p^\ell) \times GF(p^\ell)$ phase space is isotropic and all properties with respect to one set of position-momentum axes, are also valid with respect to other (rotated) sets of position-momentum axes.

The matrix elements of the symplectic operators $S(q, r, s)$ are given by [4]

$$\langle X; n | S(q, r, s) | X; m \rangle = p^{-\ell} G(A) \chi [(2q)^{-1}(s^{-1} + r)n^2 - s^{-1}nm + (2s)^{-1}qm^2] \quad (26)$$

where $G(A)$ is the Gauss sum [11]

$$G(A) = \sum_{r \in GF(p^\ell)} \chi(Ar^2) \quad (27)$$

and $A = -2^{-1}(1 + rs)^{-1}qs$.

We can show that the operators $S(q, r, s)$ form a group which is the symplectic group $Sp(2, GF(p^\ell))$.

7. Frobenius symmetry

An important property of Galois fields is the Frobenius map

$$\sigma(\alpha) = \alpha^p; \quad \sigma^\ell = \mathbf{1} \quad (28)$$

This is an automorphism in $GF(p^\ell)$ which leaves the elements of \mathbb{Z}_p fixed, i.e.,

$$\alpha \in \mathbb{Z}_p \rightarrow \sigma(\alpha) = \alpha \quad (29)$$

The $\{\mathbf{1}, \sigma, \dots, \sigma^{\ell-1}\}$ form a cyclic group of order ℓ which is known as the Galois group.

This symmetry of $GF(p^\ell)$, which is the position space in our context, is expected to have implications for the symmetries of our physical system. We introduce the Frobenius transformations in the Hilbert space H as follows:

$$\mathcal{G} = \sum_m |X; m^p\rangle \langle X; m| \quad (30)$$

It is easily seen that

$$\mathcal{G}\mathcal{G}^\dagger = \mathbf{1}; \quad \mathcal{G}^\ell = \mathbf{1}; \quad [\mathcal{G}, F] = 0 \quad (31)$$

Acting with \mathcal{G}^λ on position and momentum states we get

$$\mathcal{G}^\lambda |X; m\rangle = |X; m^{p^\lambda}\rangle; \quad \mathcal{G}^\lambda |P; m\rangle = |P; m^{p^\lambda}\rangle \quad (32)$$

Therefore we can think of them as transformations of position and momentum into position to a power and momentum to a power. We stress that both positions and momenta take a finite number of values, and these transformations are simply a reordering. There is no analogue of these transformations in the harmonic oscillator case.

Acting with \mathcal{G}^λ on displacement and symplectic operators we get

$$\begin{aligned} \mathcal{G}^\lambda D(\alpha, \beta) (\mathcal{G}^\dagger)^\lambda &= D(\alpha^{p^\lambda}, \beta^{p^\lambda}) \\ \mathcal{G}^\lambda S(q, r, s) (\mathcal{G}^\dagger)^\lambda &= S(q^{p^\lambda}, r^{p^\lambda}, s^{p^\lambda}) \end{aligned} \quad (33)$$

The fact that $\mathcal{G}^\ell = \mathbf{1}$ implies that:

$$\begin{aligned} \mathcal{G} &= \varpi(0) + \Omega(1)\varpi(1) + \dots + \Omega(\ell-1)\varpi(\ell-1) \\ \Omega(m) &= \exp\left(\frac{i2\pi m}{\ell}\right) \end{aligned} \quad (34)$$

Here $\varpi(\lambda)$ are orthogonal projectors to the eigenspaces corresponding to the eigenvalues $\Omega(\lambda)$ of \mathcal{G} . We can show that:

$$\varpi(\lambda) = \frac{1}{\ell} \left\{ \mathbf{1} + \mathcal{G}\Omega(-\lambda) + [\mathcal{G}\Omega(-\lambda)]^2 + \dots + [\mathcal{G}\Omega(-\lambda)]^{\ell-1} \right\} \quad (35)$$

If the Hamiltonian h of the system, commutes with \mathcal{G}

$$[\mathcal{G}, h] = [\varpi(\lambda), h] = 0 \quad (36)$$

then there are constants of motion. Let $\rho(0)$ be the density matrix of the system at $t = 0$. Then at time t , its density matrix is:

$$\rho(t) = \exp(iht) \rho(0) \exp(-iht) \quad (37)$$

Using Eq.(36) we can show that the eigenvalues of $\varpi(\lambda)\rho(t)\varpi(\lambda)$ are constant in time. We express this using the characteristic polynomial, as:

$$\det[y\mathbf{1} - \varpi(\lambda)\rho(t)\varpi(\lambda)] = \det[y\mathbf{1} - \varpi(\lambda)\rho(0)\varpi(\lambda)] \quad (38)$$

A special case of this result is that the probabilities $\text{tr}[\rho(t)\varpi(\lambda)]$ are constant in time:

$$\text{tr}[\rho(t)\varpi(\lambda)] = \text{tr}[\rho(0)\varpi(\lambda)] \quad (39)$$

8. Discussion

We have studied quantum systems with positions and momenta in the Galois field $GF(p^\ell)$. We have explained that systems can be constructed from ℓ spins with $j = (p - 1)/2$, which are coupled in the way described by the Hamiltonian of Eq.(18). This special coupling corresponds to the Galois multiplication rule and the Galois trace. More specifically, the Fourier transform F of Eq.(17), which enters in the Hamiltonian h , contains the matrix g of Eq.(4) which is intimately related with the Galois multiplication rule and the Galois trace.

We have studied the Heisenberg-Weyl group of displacements. In Eq.(23) we have expressed the displacement operator in terms of displacement operators in the ℓ subsystems. The Galois theory also enters here through the matrix g , which is contained in the dual components of α .

We have also studied the $Sp(2, GF(p^\ell))$ group of symplectic transformations and gave the matrix elements of the symplectic operators in Eq.(26).

A unique feature of these systems is the Frobenius transformations of Eq.(30). If they commute with the Hamiltonian we get the constants of motion in Eqs(38), (39).

The work brings concepts from field extension in algebra into the context of quantum mechanics and applied harmonic analysis. It also studies group representations (in particular the Heisenberg-Weyl and the symplectic groups) over Galois fields.

References

- [1] Vourdas A 2004 *Rep. Prog. Phys.* **67** 267
- [2] Vourdas A 2005 *J. Phys.* **A38** 8453
 Vourdas A 2006 *Acta Appl. Math.* **93** 197
 Vourdas A 2006 *J. Math. Phys.* **47** 092104
 Vourdas A *J Fourier Anal. Appl.* to appear
- [3] Neuhauser M 2002 *J. Lie Theory* **12** 15
 Feichtinger H G, Hazewinkel M, Kaiblinger N, Matusiak E and Neuhauser M *Q. J. Math.* to appear
- [4] Vourdas A 2007 *J. Phys.* **A 40** R285
- [5] Wootters W 1987 *Ann. Phys. (NY)* **176** 1
 Wootters W and Fields B D 1989 *Ann. Phys. (NY)* **191** 363
 Gibbons K Hoffman M J and Wootters W 2004 *Phys. Rev.* **A70** 062101
- [6] Chaturvedi S 2002 *Phys. Rev.* **A65** 044301
- [7] Klimov A, Sanchez-Soto L and de Guise H 2005 *J. Phys.* **A38** 2747
 Klimov A Sanchez-Soto L and de Guise H 2005 *J. Opt. B:Quantum Semiclass. Opt.* **7** 283
 Romero J L Bjork G, Klimov A B and Sanchez-Soto L L 2005 *Phys. Rev.* **A72** 062310
 Klimov A B Munoz C and Romero J L 2006 *J. Phys.* **A39** 14471
 Bjork G, Romero J L, Klimov A B and Sanchez-Soto L L 2007 *J. Opt. Soc. Amer.* **B24** 371

- [8] Kibler M R and Planat M 2006 *Intern. J. Mod. Phys.* **B20** 1802
Kibler M R 2006 *Intern. J. Mod. Phys.* **B20** 1792
- [9] Saniga M, Planat M and Rosu H 2004 *J. Opt. B-Quantum Semiclass. Optics* **6** L19
Planat M and Rosu H 2005 *Eur. Phys. J.* **D36** 133
Saniga M and Planat M 2006 *J. Phys.* **A39** 435
- [10] Bengtsson I, Bruzda W, Ericsson A, Larsson J A, Tadej W and Zyczkowski K 2007 *J. Math. Phys.* **48** 052106
- [11] Berndt B C Evans R J and Williams K S 1998 *Gauss and Jacobi sums* (NY: Wiley)
Konyagin S V and Shparlinski I E 1999 *Character sums with exponential functions and their applications* (Cambridge: Cambridge Univ. Press)