Engineering of quantum systems with variables in $GF(p^\ell)$

A. Vourdas
Department of Computing, University of Bradford, Bradford BD7 1DP, United Kingdom

A system comprised of $\ell$ subsystems, each of which is described with variables in $\mathbb{Z}_p$, is considered. Position and momentum states in this $\ell$-partite system can be labelled with elements in $GF(p^\ell)$. It is shown that the whole quantum formalism can be expressed in terms of Galois arithmetic, if and only if the Hamiltonian belongs to a particular subset of the set of all Hamiltonians of this $\ell$-partite system (we say that these Hamiltonians are compatible with $GF(p^\ell)$). Several examples of such Hamiltonians are presented.

I. INTRODUCTION

There is currently a lot of interest on finite quantum systems i.e., systems with positions and momenta in the ring $\mathbb{Z}_d$ of integers modulo $d$ (reviews are presented in [1, 2]). When $d = p$, where $p$ is a prime number, $\mathbb{Z}_p$ is a field and the system has stronger properties. (e.g., the number of mutually unbiased bases is equal to the maximum possible value $d + 1$ [3–9]).

In this general line of research we study systems with variables in a Galois field $GF(p^\ell)$ [10]. The aim is firstly to understand their properties, secondly to engineer such systems, and thirdly to use them for applications in the general area of information processing (both classical and quantum).

With regard to quantum engineering of these systems, in recent work [11] we have considered a system comprised of $\ell$ subsystems, each of which is described with variables in $\mathbb{Z}_p$ (e.g., spins with $j = (p - 1)/2$). Position and momentum states in this $\ell$-partite system can be labelled with elements in $GF(p^\ell)$. We have shown that the whole formalism can be expressed in terms of Galois arithmetic, if and only if the Hamiltonian belongs to a particular subset of the set of all Hamiltonians of these systems. We say that these Hamiltonians are compatible with $GF(p^\ell)$.

$GF(p^\ell)$ is similar to $[\mathbb{Z}_p]^\ell$ with regard to addition, but there is a lot of extra structure in $GF(p^\ell)$ related to multiplication and also other operations like the trace. Consequently, position and momentum states in the $\ell$-partite system which are labelled with elements in $[\mathbb{Z}_p]^\ell$, can also be labelled with elements in $GF(p^\ell)$. But only some of the Hamiltonians of the $\ell$-partite system can accommodate this extra mathematical structure, i.e., they are compatible with $GF(p^\ell)$. Related problem (which is also a problem in its own right) is the study of transformations of various quantum mechanical quantities, as the basis in $GF(p^\ell)$ changes.

In this paper we review briefly and extend this work, with emphasis on the physical aspects and with a minimum of technical details in terms of Galois theory. We also give several examples of specific Hamiltonians
which are compatible with $GF(p^\ell)$. They can be used for engineering these systems. In this sense the paper aims to bridge the gap between the mathematical aspects and the applied/engineering aspects of these systems.

In section II we present some aspects of Galois fields which are needed later. In particular we discuss transformations of the basis in $GF(p^\ell)$. In section III we present very briefly quantum systems with variables in $\mathbb{Z}_p$ in order to establish the notation. In section IV we discuss quantum systems with positions and momenta in $GF(p^\ell)$, and show that a change in the basis in $GF(p^\ell)$ is related to unitary transformations of the quantum states. In section V we give Hamiltonians which are compatible with $GF(p^\ell)$. The emphasis here is on examples rather than general theorems which have been presented in [11]. We conclude in section VI with a discussion of our results.

II. GALOIS FIELDS

We consider the Galois field $GF(p^\ell)$ (where $p$ is a prime number and $p \neq 2$). Its elements can be written in terms of the ‘indeterminate’ $\epsilon$ as

$$\alpha = \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \epsilon^\lambda; \quad \alpha_\lambda \in \mathbb{Z}_p,$$

and they are defined modulo an irreducible polynomial

$$P(\epsilon) \equiv c_0 + c_1 \epsilon + \ldots + c_{\ell-1} \epsilon^{\ell-1} + \epsilon^\ell; \quad c_i \in \mathbb{Z}_p.$$  

(2)

We use here the polynomial basis $\{1, \epsilon, ..., \epsilon^{\ell-1}\}$. We can go to another basis \cite{12} by using the relation

$$\mathcal{E}_\kappa = \sum_{\lambda} \epsilon^\lambda (V^{-1})_{\lambda\kappa}.$$  

(3)

where $V$ is a matrix in $GL(\ell, \mathbb{Z}_p)$ (the group of $\ell \times \ell$ invertible matrices with elements in $\mathbb{Z}_p$). Then

$$\alpha = \sum_{\lambda=0}^{\ell-1} A_\lambda \mathcal{E}_\lambda; \quad A_\lambda = \sum_{\kappa=0}^{\ell-1} V_{\lambda\kappa} \alpha_\kappa.$$  

(4)

Given a basis $\mathcal{E}_\kappa$ we define its dual basis $\overline{\mathcal{E}}_\kappa$ through the relation

$$\text{Tr}(\overline{\mathcal{E}}_\kappa \mathcal{E}_\lambda) = \delta_{\kappa\lambda}.$$  

(5)

Then

$$\alpha = \sum_{\lambda=0}^{\ell-1} \overline{\mathcal{E}}_\lambda \mathcal{E}_\lambda; \quad \overline{\mathcal{E}}_\lambda = \text{Tr}[\alpha \mathcal{E}_\lambda] = \sum_{\kappa=0}^{\ell-1} \mathcal{E}_\kappa (V^{-1})_{\kappa\lambda}.$$  

(6)

We use the notation $\{E_\lambda\}$ for the basis which is dual to $\epsilon^\lambda$ (i.e., $\text{Tr}(\epsilon^\kappa E_\lambda) = \delta_{\kappa\lambda}$).

For later use we define the symmetric matrices $g_V$ and $G_V$:

$$(g_V)_{\kappa\lambda} = \text{Tr}(\mathcal{E}_\kappa \mathcal{E}_\lambda); \quad G_V = g_V^{-1} = \text{Tr}(\overline{\mathcal{E}}_\kappa \overline{\mathcal{E}}_\lambda).$$  

(7)
We use the index $V$ in the notation, because these matrices are defined with respect to the basis $\mathcal{E}_k$, which is defined through the matrix $V$. We denote the matrices corresponding to the polynomial basis of Eq.(1), as $g$ and $G$. Then

$$g_V = (V^{-1})^T g V^{-1}; \quad G_V = g_V^{-1} = V G V^T$$

(8)

A. Trace

The trace of $\alpha \in GF(p^\ell)$ is defined as:

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

(9)

The trace does not depend on the basis.

We can express the trace of the product of $\alpha, \beta \in GF(p^\ell)$ in terms of their components as

$$\text{Tr}(\alpha\beta) = \sum_{\lambda, \kappa} (g_V)_{\lambda\kappa} A_\lambda B_\kappa = \sum_{\lambda, \kappa} (G_V)_{\lambda\kappa} \overline{A}_\lambda \overline{B}_\kappa = \sum_{\lambda} A_\lambda \overline{B}_\lambda.$$  

(10)

More generally we introduce the symmetric tensors

$$\left(g_V^{(N)}\right)_{\lambda_1 \ldots \lambda_N} \equiv \text{Tr}[\mathcal{E}_{\lambda_1} \ldots \mathcal{E}_{\lambda_N}]; \quad \left(G_V^{(N)}\right)_{\lambda_1 \ldots \lambda_N} \equiv \text{Tr}[\mathcal{E}_{\lambda_1} \ldots \mathcal{E}_{\lambda_N}]; \quad \lambda_i = 0, \ldots, \ell - 1$$

(11)

and express the trace of a product of $N$ elements of $GF(p^\ell)$, as

$$\text{Tr}\left[\alpha^{(1)} \ldots \alpha^{(N)}\right] = \sum \left(g_V^{(N)}\right)_{\lambda_1 \ldots \lambda_N} A_{\lambda_1}^{(1)} \ldots A_{\lambda_N}^{(N)} = \sum \left(G_V^{(N)}\right)_{\lambda_1 \ldots \lambda_N} \overline{A}_{\lambda_1}^{(1)} \ldots \overline{A}_{\lambda_N}^{(N)}.$$  

(12)

As above, the index $V$ in the notation indicates the basis used for these tensors (if there is no index it means that the polynomial basis of Eq.(1) has been used, i.e., $V = 1$).

We call $\mathfrak{S}(V)$ and $\overline{\mathfrak{S}}(V)$ the following sets of tensors

$$\mathfrak{S}(V) = \{g_V, g_V^{(3)}, g_V^{(4)}, \ldots\}; \quad \overline{\mathfrak{S}}(V) = \{G_V, G_V^{(3)}, G_V^{(4)}, \ldots\}.$$  

(13)

B. Characters

Additive characters in $GF(p^\ell)$ are given by

$$\chi(\alpha) = \omega[\text{Tr}(\alpha)];$$

(14)

where we use the notation

$$\omega(m) = \exp\left(\frac{2\pi i m}{p}\right); \quad m \in \mathbb{Z}_p.$$  

(15)

Using Eq.(10) we get

$$\chi(\alpha\beta) = \omega \left[\sum_{\lambda, \kappa} (g_V)_{\lambda\kappa} A_\lambda B_\kappa\right] = \omega \left[\sum_{\lambda, \kappa} (G_V)_{\lambda\kappa} \overline{A}_\lambda \overline{B}_\kappa\right] = \omega \left[\sum_{\lambda} A_\lambda \overline{B}_\lambda\right].$$  

(16)
More generally Eq.(12) leads to
\[
\chi \left[ \alpha^{(1)} \ldots \alpha^{(N)} \right] = \omega \left[ \sum \left( g_{V}^{(N)} \right)_{\lambda_1 \ldots \lambda_N} A_{\lambda_1}^{(1)} \ldots A_{\lambda_N}^{(N)} \right] = \omega \left[ \sum \left( G_{V}^{(N)} \right)_{\lambda_1 \ldots \lambda_N} \bar{A}_{\lambda_1}^{(1)} \ldots \bar{A}_{\lambda_N}^{(N)} \right]. \tag{17}
\]
We also define characters of diagonal matrices with elements in $\text{GF}(p)$. Let $\Theta$ be the $N \times N$ diagonal matrix
\[
\Theta = \text{diag}(\theta_{ii}). \tag{18}
\]
The character of $\Theta$ is defined to be the $N \times N$ complex diagonal matrix
\[
\chi(\Theta) = \text{diag}[\chi(\theta_{ii})]. \tag{19}
\]
The matrix $\Theta$ can also be written as
\[
\Theta = \Theta_0 \mathcal{E}_0 + \ldots + \Theta_{\ell-1} \mathcal{E}_{\ell-1}, \tag{20}
\]
where $\Theta_\lambda$ are diagonal matrices with elements in $\mathbb{Z}_p$. The Galois trace of $\Theta$ is a diagonal matrix with elements in $\mathbb{Z}_p$, defined by
\[
\text{Tr}_G \Theta = \Theta + \Theta p + \ldots + \Theta^{p^{\ell-1}}. \tag{21}
\]
Then the character of $\Theta$ can be expressed as
\[
\chi(\Theta) = \omega \left( \text{Tr}_G \Theta \right). \tag{22}
\]

### III. QUANTUM SYSTEMS WITH VARIABLES IN $\mathbb{Z}_p$

We consider a quantum system with positions and momenta in $\mathbb{Z}_p$, described by a $p$-dimensional Hilbert space $\mathcal{H}$. Let $|X; m\rangle$ be the orthonormal basis of position states and $|P; m\rangle$ the orthonormal basis of momentum states. Here $m \in \mathbb{Z}_p$ and the $X, P$ are used to indicate position and momentum bases. They are related through the Fourier transform
\[
|P; m\rangle = F|X; m\rangle; \quad F = p^{-1/2} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \omega(mn)|X; m\rangle\langle X; n| \tag{23}
\]
Position and momentum operators are defined as
\[
Q = \sum_{m} m|X; m\rangle\langle X; m|; \quad P = \sum_{m} m|P; m\rangle\langle P; m|. \tag{24}
\]
Displacement operators are defined as $D(\alpha, \beta) = Z^\alpha X^\beta \omega(-2^{-1} \alpha \beta)$ where
\[
Z = \omega(Q); \quad X = \omega(-P)
\]
\[
X^p = Z^p = 1; \quad X^\beta Z^\alpha = Z^\alpha X^\beta \omega(-\alpha \beta); \quad \alpha, \beta \in \mathbb{Z}_p. \tag{25}
\]
The $D(\alpha, \beta)\omega(\gamma)$ form a representation of the Heisenberg-Weyl group.
IV. QUANTUM SYSTEMS WITH VARIABLES IN $GF(p^\ell)$

We consider an $\ell$-partite system comprised of $\ell$ component systems of the type described in section III. Its Hilbert space $H = \mathcal{H} \otimes \ldots \otimes \mathcal{H}$ is $p^\ell$-dimensional. Using the polynomial basis in $GF(p^\ell)$, we label the position state $|X; m_0 \rangle \otimes \ldots \otimes |X; m_{\ell-1} \rangle$ in $H$, as follows:

$$|X; m \rangle \equiv |X; m_0 \rangle \otimes \ldots \otimes |X; m_{\ell-1} \rangle; \quad m = \sum_{\kappa=0}^{\ell-1} m_\kappa \epsilon^\kappa; \quad m_\kappa \in \mathbb{Z}_{p}. \quad (26)$$

The Fourier operator, is given by

$$F = p^{-\ell/2} \sum_{m,n \in GF(p^\ell)} \chi(mn)|X; m \rangle \langle X; n|$$

$$= p^{-\ell/2} \sum \omega \left[\sum g_{\kappa\lambda} m_\kappa n_\lambda \right] |X; m_0 \rangle \langle X; n_0| \otimes \ldots \otimes |X; m_{\ell-1} \rangle \langle X; n_{\ell-1}| \quad (27)$$

where $m = \sum m_\kappa \epsilon^\kappa$ and $n = \sum n_\kappa \epsilon^\kappa$.

The momentum states are given by

$$|P; m \rangle = F|X; m \rangle = p^{-\ell/2} \sum_n \chi(mn)|X; n \rangle \quad (28)$$

They can be expressed in terms of momentum states in the various component systems as

$$|P; m \rangle = |P; m_0 \rangle \otimes \ldots \otimes |P; m_{\ell-1} \rangle. \quad (29)$$

The dual components $\overline{m}_i$ of $m$ appear in the momentum states (see Eq.(16)).

The position and momentum operators are given by

$$Q = \sum_m m |X; m \rangle \langle X; m|; \quad P = \sum_m |P; m \rangle \langle P; m| = FF^\dagger \quad (30)$$

For later use we define characters of powers of $Q, P$:

$$\chi(\alpha^* Q^r) = \sum_{m \in GF(p^\ell)} \chi(am^r)|X; m \rangle \langle X; m|; \quad \chi(\beta^* P^r) = \sum_{m \in GF(p^\ell)} \chi(\beta m^r)|P; m \rangle \langle P; m| \quad (31)$$

where $\alpha, \beta \in GF(p^\ell)$. They are $p^\ell \times p^\ell$ complex matrices.

Displacement operators are given by:

$$Z^\alpha = \chi(\alpha Q); \quad X^\beta = \chi(-\beta P) \quad (32)$$

We can prove that

$$X^\beta Z^\alpha = Z^\alpha X^\beta \chi(-\alpha \beta). \quad (33)$$

General displacement operators are given by:

$$D(\alpha, \beta) = Z^\alpha X^\beta \chi(-2^{-1} \alpha \beta). \quad (34)$$
The displacement operators can be expressed in terms of displacement operators acting on the various subsystems as:

\[ D(\alpha, \beta) = D(\bar{\alpha}_0, \beta_0) \otimes \ldots \otimes D(\bar{\alpha}_{\ell-1}, \beta_{\ell-1}); \quad \alpha = \sum_{\lambda} \bar{\alpha}_\lambda E_\lambda; \quad \beta = \sum_{\lambda} \beta_\lambda E_\lambda, \]

where \( \bar{\alpha}_\lambda \) are the dual components of \( \alpha \), and \( \beta_\lambda \) the components of \( \beta \).

In this section up to now, we used a labelling method with the polynomial basis of \( GF(p^\ell) \). We can go to a labelling method with a different basis, with the unitary transformation

\[ U_V = \sum_{n \in GF(p^\ell)} |X; m(n)) \rangle \langle X; n|; \quad m(n) = \sum_\kappa T r(n \bar{E}_\kappa) (36) \]

For example

\[ |X; V; n) \equiv U_V |X; n) = |X; m(n)) = |X; T r(n \bar{E}_0) \rangle \otimes \ldots \otimes |X; T r(n \bar{E}_{\ell-1}) \rangle \]

Since \( \sum_\kappa T r(n \bar{E}_\kappa) = n \), we label this state as \( |X; V; n) \). The \( V \) in the notation indicates that the basis \( \{ \bar{E}_\kappa \} \) (defined through \( V \) in Eq.(3)) has been used in the labelling method. We can also introduce the displacement operators

\[ D_V(\alpha, \beta) \equiv U_V D(\alpha, \beta) U_V^\dag = D(\alpha', \beta'); \quad \alpha' = \sum_\kappa E_\kappa T r(\alpha \bar{E}_\kappa); \quad \beta' = \sum_\kappa E_\kappa T r(\beta \bar{E}_\kappa). \]

The \( U_V \) transformations form a unitary representation of the \( GL(\ell, Z_p) \) group.

V. HAMILTONIANS

We consider a system comprised of \( \ell \) subsystems, each of which is described with variables in \( Z_p \). We use the notation

\[ \Omega_\lambda = 1 \otimes \ldots \otimes 1 \otimes Q^{(\lambda)} \otimes 1 \otimes \ldots \otimes 1 \]

\[ \Psi_\lambda = 1 \otimes \ldots \otimes 1 \otimes P^{(\lambda)} \otimes 1 \otimes \ldots \otimes 1 \]

(39)

It is convenient to express the Hamiltonian of this system as

\[ h = h \left[ f_n \left( \sigma^{(n)} \right), f_n' \left( \tau^{(n)} \right) \right] \]

(40)

where \( f_n \left( \sigma^{(n)} \right), f_n' \left( \tau^{(n)} \right) \) are the complex matrices

\[ f_n \left( \sigma^{(n)} \right) = \omega \left[ \sum_\lambda \sigma^{(n)}_{\lambda_1 \ldots \lambda_n} \Omega_{\lambda_1} \ldots \Omega_{\lambda_n} \right] \]

\[ f_n' \left( \tau^{(n)} \right) = \omega \left[ \sum_\lambda \tau^{(n)}_{\lambda_1 \ldots \lambda_n} \Psi_{\lambda_1} \ldots \Psi_{\lambda_n} \right] \]

(41)

and the \( \sigma^{(n)}, \tau^{(n)} \) are symmetric tensors which take values in \( Z_p \). The \( \sum_\lambda \sigma^{(n)}_{\lambda_1 \ldots \lambda_n} \Omega_{\lambda_1} \ldots \Omega_{\lambda_n} \) and \( \sum_\lambda \tau^{(n)}_{\lambda_1 \ldots \lambda_n} \Psi_{\lambda_1} \ldots \Psi_{\lambda_n} \) are matrices with elements in \( Z_p \), whilst the \( f_n \left( \sigma^{(n)} \right) \) and \( f_n' \left( \tau^{(n)} \right) \) are complex matrices. It is convenient to work with complex matrices and for this reason we have written the Hamiltonian as a function of the latter.
In [11] we have proved that the Hamiltonian of Eq.(40) is compatible with $GF(p^\ell)$ if and only if there exists $V \in GL(l, \mathbb{Z}_p)$ (which does not depend on $n$) such that $\sigma^{(n)} \in \mathfrak{S}(V)$ and $\tau^{(n)} \in \overline{\mathfrak{S}}(V)$, for all $n$ that enter in the Hamiltonian. In this case the Hamiltonian of Eq.(40) can be written in terms of the characters in Eq.(31), as

$$ h = h \left[ \chi(\alpha_N Q_V^N), \chi(\beta_N P_V^N) \right] $$

(42)

Here the $Q_V^N$, $P_V^N$ are matrices with elements in $GF(p^\ell)$ but they enter in the Hamiltonian through their characters which are finite complex matrices. Then the time evolution operator is $\exp(ith)$. Examples are

$$ \exp(ith_1) = \left[ \chi(\alpha Q_V^N) \chi(\beta P_V^N) \right]^t $$

$$ \exp(ith_2) = \left[ \chi(\alpha P_V^N) \chi(\beta Q_V^N) \right]^t = F \exp(ith_1) F^t $$

$$ \exp(ith_3) = \left[ \chi(\alpha P_V^N) \chi(\beta Q_V^N) \chi(\gamma Q_V^N) \right]^t $$

(43)

The $\exp(ith_1)$ and $\exp(ith_2)$ contain quadratic terms of the position and momentum operators, while the $\exp(ith_3)$ also contains a quartic term of the position operator. There is no simple analytic relation between $\exp(ith_1)$ and $\exp(ith_2)$ (as in the harmonic oscillator case), but they are related through a Fourier transform, and therefore their eigenvalues are the same. We note that Eqs.(43), involve a real power of a complex matrix which is defined through logarithms and therefore is multivalued, but the principal value can be used.

A. Example with the $GF(9)$ in the polynomial basis

We consider the $GF(9)$ (i.e., $p = 3$ and $\ell = 2$) and its polynomial basis $1, \epsilon$. We choose the irreducible polynomial $P(\epsilon) = \epsilon^2 + \epsilon + 2$ and we calculate the matrices $g, G$:

$$ g = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}; \quad G = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix} $$

(44)

The dual basis in this case is $E_0 = -\epsilon$, $E_1 = -1 + \epsilon$ and an arbitrary element $m \in GF(9)$, can be written as

$$ m = m_0 + \epsilon m_1 = E_0 \overline{m}_0 + E_1 \overline{m}_1; \quad \overline{m}_0 = -m_0 - m_1; \quad \overline{m}_1 = -m_0. $$

(45)

A quantum system with variables in $GF(9)$ can be constructed as a bipartite system where each component system is described with variables in $\mathbb{Z}_3$. We have seen in Eqs.(26), (29), that position and momentum states in this bipartite system, can be labelled with elements of $GF(9)$. We now consider Hamiltonians describing this system. We first consider the polynomial basis and Hamiltonians with quadratic terms. Such Hamiltonians are compatible with $GF(9)$ if $h = h[f_1^2, f_2]$ where

$$ f_1 = \omega \sum G_{\lambda\mu} \Psi_{\lambda} \Psi_{\mu} = \omega \left[ 1 \otimes (P(1))^2 - 2 P(0) \otimes P(1) \right] $$

$$ f_2 = \omega \sum \bar{g}_{\lambda\mu} \bar{\Omega}_{\lambda} \bar{\Omega}_{\mu} = \omega \left[ (Q(0))^2 \otimes 1 - 2 Q(0) \otimes Q(1) \right] $$

(46)
Indeed, let

\[ |X; m\rangle = |X; m_0\rangle \otimes |X; m_1\rangle; \quad |P; m\rangle = |P; m_0\rangle \otimes |P; m_1\rangle \]

\[ Q = (Q^{(0)} \times 1) + \epsilon (1 \times Q^{(1)}); \quad P = E_0 (P^{(0)} \times 1) + E_1 (1 \times P^{(1)}) \] (47)

Then it is easily seen that

\[ f'_2 = \chi (P^2); \quad f_2 = \chi (Q^2) \] (48)

where the characters have been defined in Eq.(22). Therefore the bipartite system, is described entirely in terms of variables in \( GF(9) \). We note that the two component systems are coupled (the terms \( Q^{(0)} \otimes Q^{(1)} \) and \( P^{(0)} \otimes P^{(1)} \) in Eq.(46)).

We next add quartic terms of the position in the Hamiltonian. Then

\[ h = h[f'_2, f_2, f_4]; \quad f_4 = \omega \left[ \sum g^{(4)}_{\lambda_1 \lambda_2 \lambda_3 \lambda_4} \Omega_{\lambda_1} \Omega_{\lambda_2} \Omega_{\lambda_3} \Omega_{\lambda_4} \right]; \quad \lambda_i = 0, 1 \] (49)

The sum in \( f_4 \) has 16 terms but the fact that \( g^{(4)} \) is symmetric reduces the number of terms. We first calculate the

\[ g^{(4)}_{0000} = \text{Tr}(1) = -1; \quad g^{(4)}_{1000} = \text{Tr}(\epsilon) = -1; \quad g^{(4)}_{1100} = \text{Tr}(\epsilon^2) = 0 \]

\[ g^{(4)}_{1110} = \text{Tr}(\epsilon^3) = -1; \quad g^{(4)}_{1111} = \text{Tr}(\epsilon^4) = 1 \] (50)

and then

\[ f_4 = \omega \left[ -(Q^{(0)})^4 \otimes 1 - 4 (Q^{(0)})^3 \otimes Q^{(1)} - 4 Q^{(0)} \otimes (Q^{(1)})^3 + 1 \otimes (Q^{(1)})^4 \right] = \chi (Q^4) \] (51)

Here the factors 4 are related to the symmetry (but since all coefficients are defined modulo 3, they can be replaced with 1). The term \( (Q^{(0)})^2 \otimes (Q^{(1)})^2 \) is absent because \( g^{(4)}_{1100} = 0 \).

**B. Example with the \( GF(9) \) in an arbitrary basis**

Let \( V \in GL(2, \mathbb{Z}_3) \) be the matrix

\[ V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \quad V^{-1} = \frac{1}{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}; \quad \Delta = ad - bc \neq 0; \quad a, b, c, d \in \mathbb{Z}_3 \] (52)

and \( \mathcal{E}_x \) the corresponding basis defined by Eq.(3). We can calculate the corresponding \( g_V \) and \( G_V \) using Eqs.(8), and then an arbitrary element \( m \in GF(9) \), expressed in eq.(45) in the polynomial basis, can also be written in the \( \mathcal{E}_x \) basis and its dual, as

\[ m = \mathcal{E}_0 M_0 + \mathcal{E}_1 M_1 = \overline{\mathcal{E}_0 M_0} + \overline{\mathcal{E}_1 M_1} \]

\[ M_0 = am_0 + bm_1; \quad M_1 = cm_0 + dm_1 \]

\[ \overline{M}_0 = \frac{d \overline{m}_0 - c \overline{m}_1}{\Delta}; \quad \overline{M}_1 = \frac{-b \overline{m}_0 + a \overline{m}_1}{\Delta} \] (53)
Below we consider a diagonal basis where the two component systems become decoupled (in the case of quadratic Hamiltonians are compatible with \( GF \)).

Using various values of \( a, b, c, d \) we get a wide class of Hamiltonians with quadratic terms. These Hamiltonians are compatible with \( GF(9) \) and they are a subset of the set of all Hamiltonians with quadratic terms, in the corresponding bipartite system. For example, a Hamiltonian \( h[f_2(\kappa_2, \lambda_2, \mu_2)] \) where the \( \kappa_3, \lambda_3, \mu_3 \) are different from the \( \kappa_2, \lambda_2, \mu_2 \), is not compatible with \( GF(9) \).

In general the two component systems are coupled (the terms \( \mu_2 Q^{(0)} \otimes Q^{(1)} \) and \( \mu_1 P^{(0)} \otimes P^{(1)} \) in Eq.(55)). Below we consider a diagonal basis where the two component systems become decoupled (in the case of quadratic coupling).

**C. Example with the \( GF(9) \) in a diagonal basis**

We consider the matrix of Eq.(52) with \( a = 0 \) and \( d = c \neq 0, b \neq 0 \). This gives the diagonal basis \( \mathcal{E}_\kappa \) and its dual, as

\[
|X; m\rangle = |X; M_0 \rangle \otimes |X; M_1\rangle; \quad |P; m\rangle = |P; M_0 \rangle \otimes |P; M_1\rangle \\
Q_V = E_0(Q^{(0)} \otimes 1) + E_1(1 \otimes Q^{(1)}) ; \quad P_V = \mathcal{E}_0( 0 \otimes 1) + \mathcal{E}_1(1 \otimes 1)
\]

Here Hamiltonians with quadratic terms, which are compatible with \( GF(9) \) are

\[
h = h[f_2(\kappa_1, \lambda_1, \mu_1), f_2(\kappa_2, \lambda_2, \mu_2)] \\
f_2(\kappa_1, \lambda_1, \mu_1) = \omega \left[ \kappa_1 (P^{(0)})^2 \otimes 1 + \lambda_1 \mathbf{1} \otimes (P^{(1)})^2 + \mu_1 P^{(0)} \otimes P^{(1)} \right] = \chi(P^2) \\
f_2(\kappa_2, \lambda_2, \mu_2) = \omega \left[ \kappa_2 (Q^{(0)})^2 \otimes 1 + \lambda_2 \mathbf{1} \otimes (Q^{(1)})^2 + \mu_2 Q^{(0)} \otimes Q^{(1)} \right] = \chi(Q^2) \\
\kappa_1 = b^2 - 2ab; \quad \lambda_1 = d^2 - 2dc; \quad \mu_1 = 2(bd - ad - bc) \\
\kappa_2 = \frac{-\lambda_1}{\Delta^2}; \quad \lambda_2 = \frac{-\kappa_1}{\Delta^2}; \quad \mu_2 = \frac{\mu_1}{\Delta^2}; \quad \kappa_i, \lambda_i, \mu_i, \Delta \in \mathbb{Z}_3
\]

Using various values of \( a, b, c, d \in \mathbb{Z}_3 \) we get a wide class of Hamiltonians with quadratic terms. These Hamiltonians are compatible with \( GF(9) \) and they are a subset of the set of all Hamiltonians with quadratic terms, in the corresponding bipartite system. For example, a Hamiltonian \( \mu_2 Q^{(0)} \otimes Q^{(1)} \) in Eq.(55)). Below we consider a diagonal basis where the two component systems become decoupled (in the case of quadratic coupling).

\[
f_2 = \omega \left[ \frac{1}{2} (P^{(0)})^2 \otimes 1 - \frac{1}{c^2} \mathbf{1} \otimes (Q^{(1)})^2 \right]
\]

If the Hamiltonian has higher order terms, then even in this basis there is coupling between the subsystems.
VI. DISCUSSION

We have studied how to engineer a finite quantum system which is described with variables in $GF(p^\ell)$. This system is an $\ell$-partite system comprised of component systems each of which is described with variables in $\mathbb{Z}_p$ (e.g., spins with $j = (p - 1)/2$). The position and momentum states in such a system can be labelled with elements in $GF(p^\ell)$, as in Eqs (26), (29). We also require that the Hamiltonian (and more generally the whole formalism) should be expressed in terms of Galois arithmetic as opposed to arithmetic in $\mathbb{Z}_p$. $GF(p^\ell)$ is similar to $\mathbb{Z}_p^\ell$ with regard to addition, but it has a lot of extra structure related to multiplication, the trace, etc. Consequently, only some of the Hamiltonians of the $\ell$-partite system can be expressed within the Galois formalism and we called them Hamiltonians compatible with $GF(p^\ell)$. In [11] we gave general theorems about the compatibility of a Hamiltonian with $GF(p^\ell)$, and here we extended this work by giving several examples of such Hamiltonians, in a more physical and less technical language.

The next step in this line of research is to consider realistic physical systems (e.g., spins, superconducting Josephson devices, etc) and to study how we can adjust the parameters in order to get one of the desirable Hamiltonians. Another direction is to study applications of these devices in information processing. There are many applications of Galois fields in classical information processing (e.g., coding and cryptography in classical communications) and devices which operate with Galois arithmetic can be useful in this area. Applications to quantum information processing, could also be studied.

[1] A. Vourdas, Rep. Prog. Phys. 67, 267 (2004)
[2] M. Kibler, J. Phys. A42, 353001 (2009)
[3] W. Wootters, B.D. Fields, Ann. Phys. (NY), 191, 363 (1989)
   K. Gibbons, M.J. Hoffman, W. Wootters, Phys. Rev. A70, 062101 (2004)
[4] S. Chaturvedi, Phys. Rev. A65, 044301 (2002)
[5] S. Bandyopadhyay, P.O. Boykin, V.Roychowdhury, F. Vatan, Algorithmica 34, 512 (2002)
[6] G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, Prog. Optics 51, 469 (2008)
[7] M. Saniga, M. Planat, H. Rosu, J. Opt. B-Quantum Semiclass. Optics 6, L19 (2004)
[8] J. Tolar, G. Hadzitaskos, J. Phys. A42, 245306 (2009)
[9] T. Durt, B.G. Englert, I. Bengtsson, K. Zyczkowski, Int. J. Quantum Comp. 8, 535 (2010)
[10] A. Vourdas, J. Phys. A40, R285 (2007)
    A. Vourdas, J. Fourier Anal. Appl. 14, 102 (2008)
[11] A. Vourdas, J. Math. Phys. 51, 052102 (2010)
[12] Z.X. Wan, ‘Lectures on finite fields and Galois rings’ (World Scientific, Singapore, 2003)