Symplectically entangled states and their applications to coding

2004 J. Phys. A: Math. Gen. 37 3305

(http://iopscience.iop.org/0305-4470/37/9/017)

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

J. Phys. A: Math. Gen. **37** (2004) 3305–3319 PII: S0305-4470(04)68643-4

Symplectically entangled states and their applications to coding

A Vourdas

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

Received 8 September 2003, in final form 1 December 2003
Published 18 February 2004
Online at stacks.iop.org/JPhysA/37/3305 (DOI: 10.1088/0305-4470/37/9/017)

Abstract

An angular momentum $(2j + 1)$-dimensional Hilbert space H is considered. Symplectic transformations S on the tensor product of N of these spaces $H \otimes \cdots \otimes H$ are studied for the case when the $2j + 1$ is a power of a prime (Galois case). The corresponding operators are calculated numerically. The formalism is applied to quantum coding. A simple repetition code based on the space H_A spanned by the direct products of N angular momentum states with the same m, has distance 1. It is shown that a code based on the symplectically transformed space SH_A has (in general) larger distance. An example with three qutrits is discussed in detail.

PACS numbers: 03.67.−a, 03.65.Ca

1. Introduction

Quantum systems with finite Hilbert space were studied originally by Weyl and also by Schwinger [1]. More recently they have been studied by many authors [2, 3] both as a subject in its own right and also in the context of various applications. In a recent paper [4] we have considered a composite quantum system comprising two subsystems each of which is described by a d-dimensional Hilbert space. In this system we have studied unitary $SU(d^2)$ transformations, which we classified into local and entangling ones. We have also studied in more detail the symplectic $Sp(4, \mathcal{Z}(d))$ transformations (where $\mathcal{Z}(d)$ are the integers modulo d).

In this paper we consider a N-partite system comprising N angular momentum sub-systems each of which is described by a $(2j + 1)$-dimensional Hilbert space. In this system we study symplectic $Sp(2N, \mathcal{Z}(2j + 1))$ transformations and construct numerically the corresponding operators. The formalism is then applied to quantum coding.

Quantum coding introduces redundancy in order to protect qubits from errors. The simplest coding schemes are the three qubit repetition codes (reviewed in [5]). However it is easily seen that they protect qubits from a very limited class of errors. For example, the three qubit bit flip code cannot protect against phase errors; and the three qubit phase flip

code cannot protect against bit flip errors. For protection against larger classes of errors more qubits are required. Arbitrary errors at known positions (erasures) require at least four qubits [6]. More general errors require at least five qubits [7]. Other coding schemes which provide protection against any one-qubit error are Shor's nine qubit code [8] and the seven qubit code [9].

Much of the work on quantum computation and quantum coding has been based on qubits in two-dimensional Hilbert spaces. More recently the use of multi-dimensional Hilbert spaces (qudits) as a potentially more powerful tool has been studied [10]. A generalization of Shor's nine qubit code for qudits was studied in [11]. In this paper we show that the use of entangling symplectic transformations on a simple repetition code with N qudits, increases the distance of the code. As the distance of the code increases, errors on more qudits can be corrected.

In section 2 we briefly introduce the formalism for quantum systems with finite Hilbert spaces (qudits) with emphasis on the symplectic transformations. We have explained previously [3, 11] that when $2j+1 = p^n$ where p is a prime number, the $\mathcal{Z}(2j+1)$ is a Galois field (which we denote as $GF(p^n)$). In this case the phase space is a finite geometry [12] and symplectic transformations form the $Sp(2N, GF(p^n))$ group [13–15]. Here we explicitly discuss an example for the case $j = 4$ (i.e., $GF(9)$), in order to see in detail how the Galois theory is embodied into our formalism for qudits ('Galois qudits'). Codes over $GF(4)$ have been discussed in [16].

In section 3 we consider products of N finite Hilbert spaces (multiqudits) and study symplectic $Sp(2N, GF(p^n))$ transformations in them. We explain that some of these transformations are local and some are entangling ones.

In section 4 we consider repetition codes with qudits and apply symplectically entangling transformations on them. We show that in the resulting code space of symplectically entangled qudits, all generators of transformations involve simultaneous transformations on more than one qudits and therefore the distance of the code increases. The general formalism is applied to an example which consists of three qutrits and which is shown to have distance 2.

We conclude in section 5 with a discussion of our results.

2. Qudits

Quantum systems with finite Hilbert space have been studied for a long time [1–3]. In [3] we have applied these ideas in the context of the angle-angular momentum quantum phase space. In this section we first briefly review some of these ideas in the context of qudits and introduce the notation. We then study symplectic transformations, which are central for this work. As explained in [3] in the two cases of integer j (Bose case) and half-integer j (Fermi case) some of the formulae are slightly different. Below we give the formulae for the Bose case, and in appendix A we summarize briefly the required amendments for the Fermi case.

We denote as $|J; j\, m\rangle$ the usual angular momentum states. Here the symbol J is not a variable but it simply indicates that they are angular momentum states. m belongs to $\mathcal{Z}(2j+1)$. The states $|J, j\, m\rangle$ span the Hilbert space $H(2j+1)$. The finite Fourier transform is defined as

$$F = (2j+1)^{-1/2} \sum_{m,n} \omega(mn) |J; j\, m\rangle\langle J; j\, n| \tag{1}$$

$$\omega(\alpha) = \exp\left[\mathrm{i}\frac{2\pi\alpha}{2j+1}\right] \qquad FF^{\dagger} = F^{\dagger}F = \mathbf{1} \qquad F^4 = \mathbf{1}. \tag{2}$$

Using these Fourier transforms we have introduced [3] the θ-basis of angle states $|\theta;\, j\, m\rangle$ as follows:

$$|\theta;\, j\, m\rangle = F|J;\, j\, m\rangle = (2j+1)^{-1/2}\sum_n \omega(mn)|J;\, j\, n\rangle. \tag{3}$$

Here the symbol θ is not a variable but it simply indicates that they are angle states. We have also introduced the angle operators $\theta_+, \theta_-, \theta_z$

$$\theta_z = FJ_zF^\dagger \qquad \theta_+ = FJ_+F^\dagger \qquad \theta_- = FJ_-F^\dagger \tag{4}$$

which obey the $SU(2)$ algebra. The θ-operators act on the θ-states in an analogous way to the J-operators acting on the J-states. The displacement operators are defined as

$$X = \exp\left[-\mathrm{i}\frac{2\pi}{2j+1}\theta_z\right] \qquad Z = \exp\left[\mathrm{i}\frac{2\pi}{2j+1}J_z\right] \tag{5}$$

$$X^{2j+1} = Z^{2j+1} = \mathbf{1} \qquad X^\beta Z^\alpha = Z^\alpha X^\beta \omega(-\alpha\beta) \tag{6}$$

where α, β are integers in $\mathcal{Z}(2j+1)$. They perform displacements along the J_z and θ_z axes in the $J_z - \theta_z$ phase space (which is the toroidal lattice $\mathcal{Z}(2j+1) \times \mathcal{Z}(2j+1)$), as follows:

$$X^\beta|J;\, j\, m\rangle = |J;\, j\, m+\beta\rangle \qquad X^\beta|\theta;\, j\, m\rangle = \omega(-\beta m)|\theta;\, j\, m\rangle \tag{7}$$

$$Z^\alpha|J;\, j\, m\rangle = \omega(m\alpha)|J;\, j\, m\rangle \qquad Z^\alpha|\theta;\, j\, m\rangle = |\theta;\, j\, m+\alpha\rangle. \tag{8}$$

The general displacement operators are defined as

$$D(\alpha,\beta) = Z^\alpha X^\beta \omega(-2^{-1}\alpha\beta) \qquad [D(\alpha,\beta)]^\dagger = D(-\alpha,-\beta) \tag{9}$$

$$D(\alpha,\beta)D(\gamma,\delta) = \omega[2^{-1}(\alpha\delta-\beta\gamma)]D(\alpha+\gamma,\beta+\delta) \tag{10}$$

where 2^{-1} is the inverse of 2 within $\mathcal{Z}(2j+1)$ (which in fact is $j+1$, but for similarity with the harmonic oscillator case we prefer to keep the notation 2^{-1}).

We can prove that an arbitrary operator U can be expanded as

$$U = (2j+1)^{-1}\sum_{\alpha,\beta}\tilde{W}(U;-\alpha,-\beta)D(\alpha,\beta) \qquad \tilde{W}(U;\alpha,\beta) = \mathrm{Tr}[UD(\alpha,\beta)] \tag{11}$$

where $\tilde{W}(U;\alpha,\beta)$ is the Weyl function (which is the two-dimensional Fourier transform of the Wigner function). This can be proved if we take the matrix elements of both sides with regard to the states $\langle J;\, j\, n|$ and $|J;\, j\, m\rangle$.

2.1. Symplectic transformations

In the $\mathcal{Z}(2j+1) \times \mathcal{Z}(2j+1)$ phase space we consider the unitary transformations,

$$X' = SXS^\dagger = X^\alpha Z^\beta \qquad Z' = SZS^\dagger = X^\gamma Z^\delta \qquad \alpha\delta - \beta\gamma = 1(\mathrm{mod}(2j+1)) \tag{12}$$

where $\alpha, \beta, \gamma, \delta$ are integers in $\mathcal{Z}(2j+1)$.

These transformations preserve equations (6), i.e., $(X')^{2j+1} = (Z')^{2j+1} = \mathbf{1}$ and also $(X')^\beta(Z')^\alpha = (Z')^\alpha(X')^\beta\omega(-\alpha\beta)$. The 'new' operators X', Z' displace differently the various states in comparison with the 'old' operators X, Z; but since the $\alpha, \beta, \gamma, \delta$ are integers, the lattice phase space $\mathcal{Z}(2j+1) \times \mathcal{Z}(2j+1)$, is preserved. The symplectic transformations rotate and rescale the J_z and θ_z axes into $J'_z = SJ_zS^\dagger$ and $\theta'_z = S\theta_zS^\dagger$ in a way that the lattice phase space $\mathcal{Z}(2j+1) \times \mathcal{Z}(2j+1)$, is preserved.

The symplectic transformations of equation (12) contain four variables but because of the constraint, there are three independent variables. The question of the existence of the 'inverses' of the elements of $\mathcal{Z}(2j+1)$ arises here, because if they exist then for a given triplet

α, β, γ (with $\alpha \neq 0$) there exist $\delta = \alpha^{-1}(\beta\gamma + 1)$ which satisfies the constraint. When the $(2j + 1)$ is a power of a prime $p(2j + 1 = p^n)$, the $\mathcal{Z}(p^n)$ is a Galois field and all non-zero elements have an inverse. In Galois fields with $n \geqslant 2$, the addition and multiplication rules are different from the 'standard' ones, and in order to emphasize this we use the notation $GF(p^n)$. When the $(2j + 1)$ is not a power of a prime, the $\mathcal{Z}(2j + 1)$ is a commutative ring with a unity, and inverses do not necessarily exist.

For $n = 1$ it is easily seen that the $\mathcal{Z}(p)$ is a field. For higher values of n the concept of field extension of $\mathcal{Z}(p)$, of degree n is required (e.g., [17]). The elements are written as polynomials of an indeterminate ϵ with coefficients in $\mathcal{Z}(p)$. These polynomials are defined modulo with an irreducible polynomial $\pi(\epsilon)$ of degree n. Different irreducible polynomials of the same degree n lead to isomorphic finite fields, and in this sense there is only one finite field which we denote as $GF(p^n)$. For practical purposes, irreducible polynomials and the corresponding addition and multiplication tables can be found in computer libraries (e.g., MATLAB).

We call Galois qudits, the qudits associated with Hilbert spaces with dimension p^n. The phase space $GF(p^n) \times GF(p^n)$ of Galois qudits, is a finite geometry [12] and dilations, contractions and discrete rotations are well defined. In contrast, the phase space of non-Galois qudits, is a set of points with no geometrical structure.

Therefore, symplectic transformations on non-Galois qudits can be performed only if $\alpha, \beta, \gamma, \delta$ can be found such that $\alpha\delta - \beta\gamma = 1(\mathrm{mod}(2j + 1))$. For Galois qudits we make a much stronger statement that for any α, β, γ there exists the corresponding symplectic transformation. This is because the phase space is a finite geometry and discrete rotations are well defined. Below we discuss explicitly Galois qudits corresponding to $GF(9)$.

The transformations of equation (12) form the symplectic $Sp(2, GF(p^n))$ group of transformations (the analogue of $Sp(2, R)$ in the harmonic oscillator). For practical purposes it is useful to calculate the operator S. A numerical calculation of the matrix elements $\langle J; j\, n|S|J; j\, m\rangle$ has been presented in [4].

We should emphasize that there is no 'natural ordering' of the states in finite systems. Any ordering depends on how we define the operators and will be changed with symplectic transformations. As an example, we consider the case $j = 2$ the operators X and Z and the corresponding states $|J; 2m\rangle$ and $|\theta; 2m\rangle$. We perform the symplectic transformations $X' = X^2$, $Z' = Z^3$ and find the corresponding J-states (denoted with prime)

$$\begin{array}{lll} |J'; 2-2\rangle = |J; 2\,1\rangle & |J'; 2-1\rangle = |J; 2-2\rangle & |J'; 2\,0\rangle = |J; 2\,0\rangle \\ |J'; 2\,1\rangle = |J; 2\,2\rangle & |J'; 2\,2\rangle = |J; 2-1\rangle & \end{array} \tag{13}$$

and also the corresponding θ-states

$$\begin{array}{lll} |\theta'; 2-2\rangle = |\theta; 2-1\rangle & |\theta'; 2-1\rangle = |\theta; 2\,2\rangle & |\theta'; 2\,0\rangle = |\theta; 2\,0\rangle \\ |\theta'; 2\,1\rangle = |\theta; -2-2\rangle & |\theta'; 2\,2\rangle = |\theta; 2\,1\rangle. & \end{array} \tag{14}$$

We see that the symplectic transformations have reordered the J-states and also the θ-states.

2.2. Galois qudits in $GF(9)$

The field $GF(9)$ consists of the integers $n = n_A + \epsilon n_B$ where $n_A, n_B \in \mathcal{Z}(3)$. We use the terms 'A-Galois' ($\mathcal{A}_\mathcal{G}$) and 'B-Galois' ($\mathcal{B}_\mathcal{G}$) parts of n for the n_A and n_B correspondingly,

$$\mathcal{A}_\mathcal{G}(n) = n_A \qquad \mathcal{B}_\mathcal{G}(n) = n_B. \tag{15}$$

We choose the irreducible polynomial $\pi(\epsilon) = \epsilon^2 + \epsilon + 2$. We note that results of calculations do depend on the choice of the irreducible polynomial, but different choices lead to isomorphic results. For this irreducible polynomial we have

$$\epsilon^2 = -\epsilon - 2 = -\epsilon + 1 = 2\epsilon + 1. \tag{16}$$

Addition and multiplication are given by

$$\begin{aligned} n+m &= (n_A+m_A)+\epsilon(n_B+m_B) \\ nm &= n_Am_A+\epsilon(n_Am_B+n_Bm_A)+\epsilon^2 n_Bm_B \\ &= (n_Am_A+n_Bm_B)+\epsilon(n_Am_B+n_Bm_A-n_Bm_B). \end{aligned} \tag{17}$$

Some useful relations for later purposes are

$$n\epsilon = n_B+(n_A-n_B)\epsilon \qquad \mathcal{A}_{\mathcal{G}}(n\epsilon)=\mathcal{B}_{\mathcal{G}}(n) \qquad \mathcal{A}_{\mathcal{G}}(nm)=n_Am_A+n_Bm_B. \tag{18}$$

We consider the Hilbert space $H(9) = H_A(3)\otimes H_B(3)$ spanned by the angular momentum states

$$|J;4\,n\rangle \equiv |J_A;1\,n_A\rangle\otimes|J_B;1\,n_B\rangle \qquad n=n_A+\epsilon n_B. \tag{19}$$

We use the indices A and B for states and operators acting on $H_A(3)$ and $H_B(3)$, correspondingly. The angle states are defined as

$$|\theta;4\,m\rangle = |\theta_A;1\,m_A\rangle\otimes|\theta_B;1\,m_B\rangle = 3^{-1}\sum_{n_A,n_B}\omega[\mathcal{A}_{\mathcal{G}}(mn)]|J_A;1\,n_A\rangle\otimes|J_B;1\,n_B\rangle$$

$$\omega=\exp\left[\mathrm{i}\frac{2\pi}{3}\right]. \tag{20}$$

As we explained above, ordering of these states is arbitrary and changes with symplectic transformations.

We consider the operators Z and X acting on $H(3)$. We define the operator Z^α acting on $H(9)=H_A(3)\otimes H_B(3)$, where $\alpha=\alpha_A+\epsilon\alpha_B$ is in $GF(9)$, as

$$Z^\alpha = \left(Z_A^{\alpha_A}\right)\otimes\left(Z_B^{\alpha_B}\right). \tag{21}$$

Here the indices A and B indicate the Hilbert space on which these operators act. They are superfluous, in the sense that it is obvious that the first operator of the tensor product acts on $H_A(3)$ and the second on $H_B(3)$; but for more clarity we include them. Examples of equation (21) are, $Z=Z_A\otimes\mathbf{1}$ and $Z^\epsilon=\mathbf{1}\otimes Z_B$. It is easily seen that

$$Z^\alpha X^\beta = \left(Z_A^{\alpha_A}X_A^{\beta_A}\right)\otimes\left(Z_B^{\alpha_B}X_B^{\beta_B}\right) \tag{22}$$

and also that

$$X^\beta Z^\alpha = Z^\alpha X^\beta\omega[-\mathcal{A}_{\mathcal{G}}(\alpha\beta)]. \tag{23}$$

A consequence of that is

$$XZ^\epsilon = Z^\epsilon X. \tag{24}$$

More generally if $\alpha_B=\beta_A=0$ or if $\alpha_A=\beta_B=0$, then the X^β commutes with the Z^α.

Calculations of the power of a power need to take into account the multiplication rule of equation (17). For example,

$$(Z^m)^n = Z^{mn} = Z_A^{m_An_A+m_Bn_B}\otimes Z_B^{m_An_B+m_Bn_A-m_Bn_B}. \tag{25}$$

Powers of $X^\beta Z^\alpha$ are more complicated and they are discussed in appendix B. It is seen that the formalism of this section is *not* simply the direct product of two qutrits, because the Galois structure has been embodied in it.

The displacement operators $D(\alpha,\beta)$ defined earlier are in the present context given by

$$\begin{aligned} D(\alpha,\beta) &= Z^\alpha X^\beta\omega[-2^{-1}\mathcal{A}_{\mathcal{G}}(\alpha\beta)] \\ &= \left[Z_A^{\alpha_A}X_A^{\beta_A}\omega(-2^{-1}\alpha_A\beta_A)\right]\otimes\left[Z_B^{\alpha_B}X_B^{\beta_B}\omega(-2^{-1}\alpha_B\beta_B)\right] \end{aligned} \tag{26}$$

and obey the relation

$$D(\alpha,\beta)D(\gamma,\delta)=\omega[2^{-1}\mathcal{A}_{\mathcal{G}}(\alpha\delta-\beta\gamma)]D(\alpha+\gamma,\beta+\delta). \tag{27}$$

The Z^{α} act on the angular momentum states and angle states, as follows:

$$Z^{\alpha}|J;4\,m\rangle=\omega[\mathcal{A}_{\mathcal{G}}(m\alpha)]|J;4\,m\rangle \qquad Z^{\alpha}|\theta;4\,m\rangle=|\theta;4\,m+\alpha\rangle. \tag{28}$$

For example, if we act with these operators on the state $|\theta;4-1-\epsilon\rangle$, we get

$$\begin{array}{ll} Z^{-1}|\theta;4-1-\epsilon\rangle=|\theta;4\,1-\epsilon\rangle & Z^{-1-\epsilon}|\theta;4-1-\epsilon\rangle=|\theta;4\,1+\epsilon\rangle \\ Z^{-1+\epsilon}|\theta;4-1-\epsilon\rangle=|\theta;4\,1\rangle & Z^{\epsilon}|\theta;4-1-\epsilon\rangle=|\theta;4-1\rangle \\ Z^{-\epsilon}|\theta;4-1-\epsilon\rangle=|\theta;4-1+\epsilon\rangle & Z|\theta;4-1-\epsilon\rangle=|\theta;4-\epsilon\rangle \\ Z^{1-\epsilon}|\theta;4-1-\epsilon\rangle=|\theta;4\epsilon\rangle & Z^{1+\epsilon}|\theta;4-1-\epsilon\rangle=|\theta;4\,0\rangle. \end{array} \tag{29}$$

Symplectic transformations are given by

$$X'=SXS^{\dagger}=X^{\alpha}Z^{\beta} \qquad Z'=SZS^{\dagger}=X^{\gamma}Z^{\delta} \tag{30}$$

where $\alpha,\beta,\gamma,\delta$, are in $GF(9)$. We require the following commutation relation:

$$\omega X'Z'=Z'X'\rightarrow\mathcal{A}_{\mathcal{G}}(\alpha\delta-\beta\gamma)=1. \tag{31}$$

However this is not enough. In addition, according to equation (24) we require that

$$X'(Z')^{\epsilon}=(Z')^{\epsilon}X'\rightarrow\mathcal{A}_{\mathcal{G}}[\epsilon(\alpha\delta-\beta\gamma)]=0\rightarrow\mathcal{B}_{\mathcal{G}}(\alpha\delta-\beta\gamma)=0. \tag{32}$$

The two constraints of equations (31) and (32) can be combined into one constraint

$$\alpha\delta-\beta\gamma=1 \tag{33}$$

which is the same as in equation (12).

An example of symplectic transformations on these qudits is

$$\begin{aligned} X'&=SXS^{\dagger}=X^{1+\epsilon}Z^{-1+\epsilon}=\left(X_AZ_A^{-1}\right)\otimes(X_BZ_B) \\ Z'&=SZS^{\dagger}=X^{1-\epsilon}Z^{-\epsilon}=(X_A)\otimes\left(X_B^{-1}Z_B^{-1}\right). \end{aligned} \tag{34}$$

For practical purposes it is useful to calculate the operator S. A numerical calculation of S for the group $Sp(4,GF(5))$ has been presented in [4]. The calculation here is similar because as we explained qudits in $GF(9)$ are a direct product of two qudits in $GF(3)$, combined with the Galois structure. The two modes here are the 'A-Galois' and 'B-Galois'. In conjuction with the X' and Z' we also need to consider the $(X')^{\epsilon}$ and $(Z')^{\epsilon}$

$$\begin{aligned} (X')^{\epsilon}&=\omega^2XZ^{1+\epsilon}=\omega^2(X_AZ_A)\otimes Z_B \\ (Z')^{\epsilon}&=\omega X^{-1-\epsilon}Z^{-1+\epsilon}=\omega\left(X_A^{-1}Z_A^{-1}\right)\otimes\left(X_B^{-1}Z_B\right). \end{aligned} \tag{35}$$

We now construct numerically the common eigenstates of Z' and $(Z')^{\epsilon}$ which are the $|J';4\,n\rangle=S|J;4\,n\rangle$ up to a phase factor. We want to chose phases such that

$$(X')^{\beta}|J';4\,m\rangle=|J';4\,m+\beta\rangle \tag{36}$$

and we achieve this starting from the state $|J';4-1-\epsilon\rangle$ (for which we chose an arbitrary phase) and applying equation (36) numerically. In table 1 we present results for the

$$S(n,m)=\langle J;4\,n|S|J;4\,m\rangle=\langle J;4\,n|J';4\,m\rangle \tag{37}$$

with $m=1+\epsilon$.

We stress again that the results of this section depend on the choice of the irreducible polynomial. However, different choices lead to isomorphic results.

Table 1. The coefficients $S(n_A + \epsilon n_B, 1 + \epsilon)$ defined in equation (37). Here $z_1 = 0.333$, $z_2 = z_1\omega$ and $z_3 = z_1\omega^{-1}$.

	$n_B = -1$	$n_B = 0$	$n_B = 1$
$n_A = -1$	z_2	z_3	z_1
$n_A = 0$	z_2	z_2	z_2
$n_A = 1$	z_1	z_3	z_2

3. Local and entangling transformations on multiqudits

We consider N Hilbert spaces H_i which are all isomorphic to the H studied above and which describe N quantum systems. We also consider the product $\mathcal{H} = H_1 \otimes \cdots \otimes H_N$. On the Hilbert space $\mathcal{H}$ we consider operators similar to the ones used above and we use an index i to indicate the Hilbert space on which they act, with the operator $\mathbf{1}$ acting on the rest Hilbert spaces. For example, $Z_i = \mathbf{1} \otimes \cdots \otimes Z \otimes \cdots \otimes \mathbf{1}$. For the states we use the index i to indicate states in the H_i. For example, $|J_i; j\, n\rangle$ are the angular momentum states in the H_i. The Z_i has the $2j + 1$ eigenvalues ω^m and there is a degeneracy with $(2j + 1)^{N-1}$ eigenvectors corresponding to each eigenvalue. We consider the common eigenvectors of *all* Z_i with $i = 1, \ldots, N$ (which commute with each other) and to each set of eigenvalues $\{m_i\}$ corresponds (up to a phase factor) one normalized eigenvector

$$Z_i|\mathcal{J}; j\{m_\ell\}\rangle = \omega(m_i)|\mathcal{J}; j\{m_\ell\}\rangle \qquad |\mathcal{J}; j\{m_\ell\}\rangle \equiv |J_i; j\, m_1\rangle \otimes \cdots \otimes |J_i; j\, m_N\rangle. \tag{38}$$

In the space $\mathcal{H}$ we consider the groups

$$G_L = [SU(2j + 1)]^N \equiv SU(2j + 1) \times \cdots \times SU(2j + 1) \tag{39}$$

$$G_{LE} = SU[(2j + 1)^N] \qquad G_L \subset G_{LE}. \tag{40}$$

The group G_L describes local transformations (the index L indicates local). It performs independent unitary transformations on each of the N components of the system; and therefore if it acts on a factorizable pure state, it gives another factorizable pure state. It has the $N[(2j + 1)^2 - 1]$ generators $D_i(\alpha_i, \beta_i)$. The group G_{LE} is more general and describes both local and entangling transformations (the indices LE indicate local and entangling). It has the $(2j + 1)^{2N} - 1$ generators $D_1(\alpha_1, \beta_1) \ldots D_N(\alpha_N, \beta_N)$. From them the $N[(2j + 1)^2 - 1]$ generators contain only one non-trivial factor (the other factors are $\mathbf{1}$) and are associated, as we explained, with local transformations; the rest $(2j+1)^{2N} - 1 - N[(2j+1)^2 - 1]$ generators contain two or more non-trivial factors and describe entangling transformations. Therefore G_L is a subgroup of G_{LE} (the $\subset$ denotes subgroup).

In this paper we are interested in symplectic transformations in the $[GF(p^n) \times GF(p^n)]^N$ phase space (for $2j + 1 = p^n$). Here also we make the distinction between the groups

$$G'_L = [Sp(2, GF(p^n))]^N \qquad G'_L \subset G_L \tag{41}$$

$$G'_{LE} = Sp(2N, GF(p^n)) \qquad G'_L \subset G'_{LE} \subset G_{LE}. \tag{42}$$

G'_L describes local symplectic transformations and it is a straightforward generalization of our discussion in section 2.1. It performs independent symplectic transformations on each of the $[GF(p^n) \times GF(p^n)]$ phase spaces; and therefore if it acts on a factorizable pure state it gives another factorizable pure state. The symplectic transformations are unitary transformations and therefore the G'_L is a subgroup of G_L. In fact, the G'_L is a finite group that depends on $3N$ integers in $GF(p^n)$; while the G_L is a continuous group that depends on $N[(2j + 1)^2 - 1]$ real variables.

The more general G'_{LE} group describes both local and entangling symplectic transformations in the total phase space $[GF(p^n) \times GF(p^n)]^N$ and we study it below. The G'_L is a subgroup of G'_{LE} which as will see below is a finite group that depends on $2N^2 + N$ integers in $GF(p^n)$. The symplectic transformations are unitary transformations and therefore the G'_{LE} is a subgroup of G_{LE} which is a continuous group that depends on $(2j+1)^{2N} - 1$ real variables.

3.1. Symplectic $Sp(2N, GF(p^n))$ entangling transformations

We consider the following unitary transformations in the $[\mathcal{Z}(2j+1) \times \mathcal{Z}(2j+1)]^N$ phase space

$$\begin{aligned} X'_i &= SX_iS^\dagger = \left(X_1^{\alpha_{1i}} Z_1^{\beta_{1i}}\right) \dots \left(X_N^{\alpha_{Ni}} Z_N^{\beta_{Ni}}\right) \\ Z'_i &= SZ_iS^\dagger = \left(X_1^{\gamma_{1i}} Z_1^{\delta_{1i}}\right) \dots \left(X_N^{\gamma_{Ni}} Z_N^{\delta_{Ni}}\right). \end{aligned} \tag{43}$$

We require that they preserve equations (6) and also that for $i \neq k$ the X_i, Z_i commute with the X_k, Z_k. In other words we require that

$$\begin{aligned} &(X'_i)^{2j+1} = (Z'_i)^{2j+1} = \mathbf{1} \qquad (X'_i)^\beta (Z'_i)^\alpha = (Z'_i)^\alpha (X'_i)^\beta \omega(-\alpha\beta) \\ &i \neq k \rightarrow [X_i, X_k] = [X_i, Z_k] = [Z_i, X_k] = [Z_i, Z_k] = 0. \end{aligned} \tag{44}$$

Physically these transformations rotate and rescale the $J_{z1}, \dots, J_{zN}, \theta_{z1}, \dots, \theta_{zN}$ axes into $J'_{z1} = SJ_{z1}S^\dagger, \dots, J'_{zN} = SJ_{zN}S^\dagger, \theta'_{z1} = S\theta_{z1}S^\dagger, \dots, \theta'_{zN} = S\theta_{zN}S^\dagger$ in a way that the phase space which is the lattice $[\mathcal{Z}(2j+1) \times \mathcal{Z}(2j+1)]^N$, is preserved. These requirements lead to the constraints

$$\sum_{\ell=1}^{N} (\alpha_{\ell i}\beta_{\ell k} - \beta_{\ell i}\alpha_{\ell k}) = 0 \qquad \sum_{\ell=1}^{N} (\gamma_{\ell i}\delta_{\ell k} - \delta_{\ell i}\gamma_{\ell k}) = 0 \qquad \sum_{\ell=1}^{N} (\alpha_{\ell i}\delta_{\ell k} - \beta_{\ell i}\gamma_{\ell k}) = \delta(i,k). \tag{45}$$

We note that there are $4N^2$ integer parameters in these transformations and $2N^2 - N$ constraints. Therefore there are $2N^2 + N$ independent integer parameters. We make here a similar comment to that made earlier about Galois and non-Galois qudits. We can perform the above symplectic transformations on non-Galois qudits only if we can find $4N^2$ integers in $\mathcal{Z}(2j+1)$ which obey all these constraints. And this might be very difficult. But with Galois qudits ($2j+1 = p^n$) we simply choose $2N^2 + N$ integer parameters and then solve the constraints (45) (because the inverses exist) to find the rest of the parameters. Another way of putting it, is that for Galois qudits the phase space is a finite geometry and discrete rotations are well defined. The transformations of equation (43) are symplectic $Sp(2N, GF(p^n))$ transformations (the analogue of $Sp(2N, R)$ in the N-dimensional harmonic oscillator).

The various Z'_i commute with each other and we consider their common eigenvectors which we denote as $|\mathcal{J}'; j\{m_i\}\rangle$

$$Z'_i|\mathcal{J}'; j\,\{m_\ell\}\rangle = \omega(m_i)|\mathcal{J}'; j\,\{m_\ell\}\rangle \qquad |\mathcal{J}'; j\,\{m_\ell\}\rangle = S|\mathcal{J}; j\,\{m_\ell\}\rangle. \tag{46}$$

For each Z'_i there is degeneracy with $(2j+1)^{N-1}$ eigenvectors corresponding to each eigenvalue. But in equation (46) we consider the common eigenvectors of *all* Z'_i (which commute with each other) and to each set of eigenvalues $\{m_i\}$ corresponds (up to a phase factor) one normalized eigenvector. From a practical point of view, the problem of finding the common eigenvectors of all Z'_i is complex for large values of N, j. The numerical technique has been discussed in [4] for $Sp(4, GF(5))$ and is also discussed below, for the more complex case of $Sp(6, GF(3))$ (an example with three qutrits).

We can now calculate the matrix elements of the operator S,

$$S(m_1, \dots, m_N|n_1, \dots, n_N) \equiv \langle \mathcal{J}; j\,\{m_\ell\}|S|\mathcal{J}; j\,\{n_\ell\}\rangle = \langle \mathcal{J}; j\,\{m_\ell\}|\mathcal{J}'; j\,\{n_\ell\}\rangle. \tag{47}$$

4. Repetition codes

In a previous paper we generalized Shor's coding method for qudits. This is a concatenated code in two steps. In the first step we introduce J-redundancy (amplitude redundancy). We consider the following subspace of $\mathcal{H}$:

$$H_A = \text{span}\{|J_A;\, j\, m\rangle \equiv |J;\, j\, m\rangle \otimes \cdots \otimes |J;\, j\, m\rangle, m = -j, \ldots, j\} \tag{48}$$

where the notation span{} is self-evident. H_A is isomorphic to the Hilbert space H. In this space we have shown that

$$Z_A = Z_i \Pi_A \qquad X_A = X_1 \ldots X_N \Pi_A \qquad [Z_i, \Pi_A] = [X_1 \cdots X_N, \Pi_A] = 0 \tag{49}$$

where Π_A is the projection operator in H_A

$$\Pi_A = \sum_m |J;\, j\, m\rangle\langle J;\, j\, m| \otimes \cdots \otimes |J;\, j\, m\rangle\langle J;\, j\, m|. \tag{50}$$

We can easily see that the $Z_i Z_k^{-1}$ are stabilizers of all states in H_A. We call G_i the cyclic group of order $2j+1$, generated by $Z_i Z_{i+1}^{-1}$. The total Abelian finite group of the stabilizers is the direct product

$$G = G_1 \times \cdots \times G_{N-1} \qquad G_i = \left\{\mathbf{1}, Z_i Z_{i+1}^{-1}, \ldots, \left[Z_i Z_{i+1}^{-1}\right]^{2j}\right\} \tag{51}$$

and is of order $(2j+1)^{N-1}$. We note that both X_A and Z_A commute with all the stabilizers and that they are defined up to a stabilizer in the sense that the gX_A, gZ_A where g is any stabilizer in G, act on the states in H_A in the same way as the X_A, Z_A, correspondingly.

The generator Z_A contains only one Z_i (acting on one qudit). Therefore the distance of this code is one. In the second step we introduce θ-redundancy (phase redundancy) as discussed in [11]. This coding scheme requires NM qudits and for noise acting on one qudit we can take $N = M = 3$ which gives the 'nine qudit code'.

In this paper we show that the second step of this concatenated code (and the extra qudits that it involves) are unnecessary, if instead of the space H_A we use the space $H_S \equiv SH_A$ which comprises the states $S|f\rangle$ where $|f\rangle$ is a state in H_A and S are the symplectic transformations of equations (43). The space H_S is different from the space H_A. The symplectic transformations map $\mathcal{H}$ onto itself. H_A is a subspace of $\mathcal{H}$ and through symplectic transformations is mapped into H_S; which is also a subspace of $\mathcal{H}$ and which is isomorphic to H_A because the transformation is unitary. The distance of the code based on H_A is 1. We show that the distance of the code based on H_S is greater than 1. As the distance of the code increases, errors on more qudits can be corrected.

4.1. Repetition codes with symplectically entangled states

The $(2j+1)$-dimensional space $H_S \equiv SH_A$ is a subspace of $\mathcal{H}$ and is isomorphic to H_A. Using this isomorphism, we introduce the J-states in H_S,

$$\begin{aligned} |J_S;\, j\, m\rangle &= S|J_A;\, j\, m\rangle = S|J;\, j\, m\rangle \otimes \cdots \otimes |J;\, j\, m\rangle \\ &= \sum_{n_1,\ldots n_N} S(n_1, \ldots n_N|m, \ldots, m)|J;\, j\, n_1\rangle \otimes \cdots \otimes |J;\, j\, n_N\rangle \end{aligned} \tag{52}$$

and also the Z and X operators in H_S,

$$Z_S = SZ_AS^\dagger = SZ_iS^\dagger\Pi_S = Z_i'\Pi_S \tag{53}$$

$$X_S = SX_AS^\dagger = SX_1 \cdots X_NS^\dagger\Pi_S = X_1' \ldots X_N'\Pi_S \tag{54}$$

$$\Pi_S = S\Pi_A S^\dagger = \sum_m |J_S;\, j\, m\rangle\langle J_S;\, j\, m| \tag{55}$$

$$[Z_i', \Pi_S] = [X_1' \dots X_N', \Pi_S] = 0. \tag{56}$$

Here Π_S is the projection operator in H_S. Using equations (43) we find that

$$\begin{aligned} Z_S &= \left[\left(X_1^{\gamma_{1i}} Z_1^{\delta_{1i}}\right) \dots \left(X_N^{\gamma_{Ni}} Z_N^{\delta_{Ni}}\right)\right]\Pi_S \\ X_S &= \left[\left(X_1^{\alpha_{11}} Z_1^{\beta_{11}}\right) \dots \left(X_N^{\alpha_{N1}} Z_N^{\beta_{N1}}\right)\right] \dots \left[\left(X_1^{\alpha_{1N}} Z_1^{\beta_{1N}}\right) \dots \left(X_N^{\alpha_{NN}} Z_N^{\beta_{NN}}\right)\right]\Pi_S \\ &= \omega^\phi \left[\left(X_1^{\alpha_{1N}+\dots+\alpha_{1N}} Z_1^{\beta_{1N}+\dots+\beta_{1N}}\right) \dots \left(X_N^{\alpha_{N1}+\dots+\alpha_{NN}} Z_N^{\beta_{N1}+\dots+\beta_{NN}}\right)\right]\Pi_S \end{aligned} \tag{57}$$

where the phase ϕ is due to the non-commutativity of X and Z. It is seen that both X_S and Z_S are products of many operators acting on all qudits. Consequently the code based on H_S has (in general) distance greater than 1. Below we use the stabilizers to find the distance.

4.2. Stabilizers

We easily see that

$$Z_i'(Z_k')^{-1}|J_S;\, j\, m\rangle = |J_S;\, j\, m\rangle. \tag{58}$$

Therefore the $Z_i'(Z_k')^{-1}$ are stabilizers of all states in H_S. They form an Abelian finite group with $N-1$ generators

$$Z_i'(Z_{i+1}')^{-1} = \omega^{\phi_i} D_1(\delta_{1i} - \delta_{1,i+1}, \gamma_{1i} - \gamma_{1,i+1}) \dots D_N(\delta_{Ni} - \delta_{N,i+1}, \gamma_{Ni} - \gamma_{N,i+1}) \tag{59}$$

where $i = 1, \dots, N-1$ and $D_i(\alpha, \beta) = Z_i^\alpha X_i^\beta \omega(-2^{-1}\alpha\beta)$. We call G_i the cyclic group of order $2j+1$, generated by $Z_i'(Z_{i+1}')^{-1}$. The total Abelian finite group of the stabilizers is the direct product

$$G' = G_1' \times \dots \times G_{N-1}' \qquad G_i' = \{\mathbf{1}, Z_i'(Z_{i+1}')^{-1}, \dots, [Z_i'(Z_{i+1}')^{-1}]^{2j}\} \tag{60}$$

and is of order $(2j+1)^{N-1}$. The stabilizers g_ℓ ($\ell = 1, \dots, (2j+1)^{N-1}$) define the codespace H_S in the sense that if $g_\ell|c\rangle = |c\rangle$ for all stabilizers, then the state $|c\rangle$ belongs in H_S.

The stabilizers are of the form

$$g_\ell = D_1(s_{\ell 1}, t_{\ell 1}) \dots D_N(s_{\ell N}, t_{\ell N}). \tag{61}$$

Operators which commute with all stabilizers (and are not themselves stabilizers) take the states in H_S into other states within H_S; and conversely, operators which do that, commute with all stabilizers. Such operators can be used to find the distance of the code.

In order to see if the distance is 1 or greater than 1, we consider all operators $D_k(u, v)$ (for all $k = 1, \dots, N$ and all $u, v \in \mathcal{Z}(2j+1)$) which act on one qudit and calculate their commutators with all stabilizers,

$$\begin{aligned} [D_k(u, v), g_\ell] &= [D_k(u, v), D_1(s_{\ell 1}, t_{\ell 1}) \dots D_N(s_{\ell N}, t_{\ell N})] \\ &= 2\mathrm{i} \sin\left[\frac{\pi}{2j+1}(ut_{\ell k} - vs_{\ell k})\right] \\ &\quad \times D_1(s_{\ell 1}, t_{\ell 1}) \dots D_k(u + s_{\ell k}, v + t_{\ell k}) \dots D_N(s_{\ell N}, t_{\ell N}). \end{aligned} \tag{62}$$

If at least one of the $D_k(u, v)$ commutes with all the stabilizers g_ℓ, i.e., if there exists u, v such that

$$ut_{\ell k} - vs_{\ell k} = 0 (\mathrm{mod}\, 2j+1) \tag{63}$$

for all ℓ, then the distance of the code is 1. In this case the $D_k(u, v)$ acting on one codeword gives another codeword. If there exists no such u, v then the distance of the code is greater than 1. Indeed an arbitrary operator U_k acting on the k-qudit can be written according

to equation (11), as as a linear combination $\sum \mu(u,v)D_k(u,v)$ and at least some of its commutators with the stabilizers will be non-zero. Such an operator cannot act on codewords and produce other codewords.

This argument can be extended to larger distances, but at least for the example below this is sufficient.

5. Example with three qutrits

We consider the case with $j = 1$ and $N = 3$ where the Hilbert space H is three-dimensional and $\mathcal{H} = H \otimes H \otimes H$. In this case equation (6) becomes

$$X^3 = Z^3 = \mathbf{1} \qquad X^\beta Z^\alpha = Z^\alpha X^\beta \omega(-\alpha\beta) \qquad \omega = \exp(\mathrm{i}2\pi/3) \tag{64}$$

where α, β are integers in $\mathcal{Z}(3)$. As previously, we use the notation $X_1 \equiv X \otimes \mathbf{1} \otimes \mathbf{1}$, $X_2 \equiv \mathbf{1} \otimes X \otimes \mathbf{1}$, etc. The group of symplectic transformations is in this case $G'_{LE} = Sp(6, \mathcal{Z}(3))$ and we consider as an example the transformations,

$$\begin{aligned}
X'_1 &= SX_1S^\dagger = (Z_1)(X_2)(X_3^{-1}) \\
Z'_1 &= SZ_1S^\dagger = (X_1Z_1)(X_2)(X_3Z_3) \\
X'_2 &= SX_2S^\dagger = \left(X_1^{-1}\right)\left(Z_2^{-1}\right) \\
Z'_2 &= SZ_2S^\dagger = \left(X_1^{-1}Z_1^{-1}\right)\left(Z_2^{-1}\right)\left(X_3^{-1}\right) \\
X'_3 &= SX_3S^\dagger = \left(X_1^{-1}Z_1\right)(X_2Z_2)\left(X_3^{-1}Z_3^{-1}\right) \\
Z'_3 &= SZ_3S^\dagger = \left(X_1^{-1}\right)(Z_2)\left(X_3Z_3^{-1}\right)
\end{aligned} \tag{65}$$

which obey the constraints (45).

Using the formulae given earlier for the general case, we find the Abelian group (of order 9) of the stabilizers,

$$\begin{aligned}
G = \Big\{ &\mathbf{1}, \left(X_1^{-1}Z_1^{-1}\right)(X_2Z_2)\left(X_3^{-1}Z_3\right), (X_1Z_1)\left(X_2^{-1}Z_2^{-1}\right)\left(X_3Z_3^{-1}\right), \left(Z_1^{-1}\right)(Z_2)(X_3Z_3), \\
&(Z_1)\left(Z_2^{-1}\right)\left(X_3^{-1}Z_3^{-1}\right)\left(X_1^{-1}Z_1\right)\left(X_2Z_2^{-1}\right)\left(Z_3^{-1}\right), \\
&\left(X_1Z_1^{-1}\right)\left(X_2^{-1}Z_2\right)(Z_3)\left(X_1^{-1}\right)(X_2)(X_3), (X_1)\left(X_2^{-1}\right)\left(X_3^{-1}\right)\Big\}.
\end{aligned} \tag{66}$$

We can easily see that none of the operators $D_i(\alpha, \beta)$ commutes with all the stabilizers. Therefore there is no operator acting on one qutrit which can transform one codeword into another. Consequently the distance of the code is at least two.

Using equations (35), (54) and (65) we find the displacement operators in the space H_S,

$$Z_S = (X_1Z_1)(X_2)(X_3Z_3)\Pi_S = \left(X_1^{-1}Z_1^{-1}\right)\left(Z_2^{-1}\right)\left(X_3^{-1}\right)\Pi_S = \left(X_1^{-1}\right)(Z_2)\left(X_3Z_3^{-1}\right)\Pi_S \tag{67}$$

$$X_S = \left(X_1Z_1^{-1}\right)\left(X_2^{-1}\right)\left(Z_3^{-1}\right)\Pi_S. \tag{68}$$

We have already explained that instead of X_S we can use gX_S where g is any stabilizer. Using $g = \left(X_1^{-1}\right)(X_2)(X_3)$ we find $gX_S = \left(Z_1^{-1}\right)\left(X_3Z_3^{-1}\right)$. This implies the distance of the code 2.

We note that the distance is 2 for the transformations of equation (64). Different transformations might lead to different distance.

5.1. Numerical calculation of the codespace

In order to find the common eigenvectors $|\mathcal{J}'; 1\ \{m_1, m_2, m_3\}\rangle$ of Z'_1, Z'_2, Z'_3, we first consider the Z'_1 which consists of the three operators X_1Z_1, X_2, X_3Z_3, and in the basis $|\mathcal{J}; 1\ \{n_1, n_2, n_3\}\rangle$ is the Kronecker product of the three matrices $\delta(n_1, m_1 + 1)\omega(m_1)$, $\delta(n_2, m_2 + 1)$

Table 2. The coefficients $S(n_1, n_2, n_3|-1, -1, -1)$ used in the calculation of $|J_S; 1\, m\rangle$ in equation (69). Each cell contains three complex values for $n_3 = -1, 0, 1$ (in that order). Here $z_1 = -0.0380 + 0.1887\mathrm{i}$, $z_2 = z_1\omega^{-1}$ and $z_3 = z_1\omega^{-2}$.

	$n_1 = -1$	$n_1 = 0$	$n_1 = 1$
$n_2 = -1$	z_1, z_1, z_3	z_2, z_3, z_3	z_1, z_3, z_1
$n_2 = 0$	z_1, z_3, z_1	z_2, z_2, z_1	z_1, z_2, z_2
$n_2 = 1$	z_2, z_3, z_3	z_3, z_2, z_3	z_2, z_2, z_1

and $\delta(n_3, m_3 + 1)\omega(m_3)$. We calculated numerically this Kronecker product (which is a 27×27 matrix) and its eigenvalues and eigenvectors. The eigenvalues are ω, 1 and ω^{-1} and there are nine eigenvectors corresponding to each of these eigenvalues. We have constructed the three 27×9 matrices $V(m_1)$ ($m_1 = -1, 0, 1$) which have as columns the nine eigenvectors corresponding to the same eigenvalue $\omega(m_1)$. Clearly the $|\mathcal{J}'; 1\{m_1, m_2, m_3\}\rangle$ is a linear combination of the nine eigenvectors corresponding to the eigenvalue $\omega(m_1)$ and this in the matrix notation is $V(m_1)A(m_1, m_2, m_3)$ where $A(m_1, m_2, m_3)$ is a 9×1 vector of the appropriate coefficients.

We next calculated numerically the Kronecker product corresponding to Z_2'. Since the $V(m_1)A(m_1, m_2, m_3)$ is an eigenvector of Z_2' with eigenvalue m_2 this implies that $(Z_2' - \omega(m_2)\mathbf{1})V(m_1)A(m_1, m_2, m_3) = 0$ and therefore the $A(m_1, m_2, m_3)$ belongs in the null space of $(Z_2' - \omega(m_2)\mathbf{1})V(m_1)$ which we denote as $N(m_1, m_2)$ (and which is readily available in most computer libraries, e.g., MATLAB). In this case the null space is three-dimensional and the $N(m_1, m_2)$ is a 9×3 matrix. The vector $A(m_1, m_2, m_3)$ is a linear combination of the three vectors in the null space and can be written as $A(m_1, m_2, m_3) = N(m_1, m_2)B(m_1, m_2, m_3)$ where $B(m_1, m_2, m_3)$ is a 3×1 vector of the appropriate coefficients.

We next calculated numerically the Kronecker product corresponding to Z_3'. Since the $V(m_1)A(m_1, m_2, m_3) = V(m_1)N(m_1, m_2)B(m_1, m_2, m_3)$ is an eigenvector of Z_3' with eigenvalue m_3 this implies that $(Z_3' - \omega(m_3)\mathbf{1})V(m_1)N(m_1, m_2)B(m_1, m_2, m_3) = 0$ and therefore the $B(m_1, m_2, m_3)$ belongs in the null space of $(Z_3' - \omega(m_3)\mathbf{1})V(m_1)N(m_1, m_2)$ which in this case is one-dimensional (for fixed m_1, m_2, m_3). We have calculated this numerically and we have found the vector $B(m_1, m_2, m_3)$. In this way we have calculated all the eigenvectors $|\mathcal{J}'; 1\{m_1, m_2, m_3\}\rangle$ up to phase factors.

In order to calculate the phases, we started from the lowest state $|\mathcal{J}'; 1\ \{-1, -1, -1\}\rangle$ and used numerically the equation

$$(X_1')^{m_1+1}(X_2')^{m_2+1}(X_3')^{m_3+1}|\mathcal{J}'; 1\ \{-1, -1, -1\}\rangle = |\mathcal{J}'; 1\ \{m_1, m_2, m_3\}\rangle. \quad (69)$$

We checked that the $|\mathcal{J}'; 1\{m_1, m_2, m_3\}\rangle$ calculated through this equation differ from the corresponding vectors calculated above as common eigenvectors of the matrices Z_1', Z_2', Z_3', only by a phase factor. This is a test that the numerical work is correct and at the same time it provides the phases.

We then calculated the matrix elements of the operator $S(n_1, n_2, n_3|m_1, m_2, m_3)$ defined in equation (47). The three-dimensional space H_S is spanned by the three vectors

$$|J_S; 1\, m\rangle = \sum_{n_1,n_2,n_3} S(n_1, n_2, n_3|m, m, m)|J; 1\, n_1\rangle \otimes |J; 1\, n_2\rangle \otimes |J; 1\, n_3\rangle. \quad (70)$$

The coefficients $S_1(n_1, n_2, n_3|m, m, m)$ are given in tables 2, 3 and 4.

Table 3. The coefficients $S(n_1, n_2, n_3|0, 0, 0)$ used in the calculation of $|J_S; 1\,m\rangle$ in equation (69). Each cell contains three complex values for $n_3 = -1, 0, 1$ (in that order). Here $z_1 = -0.0380 + 0.1887\mathrm{i}$, $z_2 = z_1\omega^{-1}$ and $z_3 = z_1\omega^{-2}$.

	$n_1 = -1$	$n_1 = 0$	$n_1 = 1$
$n_2 = -1$	z_1, z_1, z_3	z_1, z_2, z_2	z_2, z_1, z_2
$n_2 = 0$	z_3, z_2, z_3	z_3, z_3, z_2	z_1, z_2, z_2
$n_2 = 1$	z_3, z_1, z_1	z_3, z_2, z_3	z_1, z_1, z_3

Table 4. The coefficients $S(n_1, n_2, n_3|1, 1, 1)$ used in the calculation of $|J_S; 1\,m\rangle$ in equation (69). Each cell contains three complex values for $n_3 = -1, 0, 1$ (in that order). Here $z_1 = -0.0380 + 0.1887\mathrm{i}$, $z_2 = z_1\omega^{-1}$ and $z_3 = z_1\omega^{-2}$.

	$n_1 = -1$	$n_1 = 0$	$n_1 = 1$
$n_2 = -1$	z_1, z_1, z_3	z_3, z_1, z_1	z_3, z_2, z_3
$n_2 = 0$	z_2, z_1, z_2	z_1, z_1, z_3	z_1, z_2, z_2
$n_2 = 1$	z_1, z_2, z_2	z_3, z_2, z_3	z_3, z_3, z_2

6. Discussion

We have studied symplectic $Sp(2N, GF(p^n))$ transformations in N-partite systems. They are given in equation (43) and contain $4N^2$ integer parameters and $2N^2 - N$ constraints. We have explained that in order to solve the constraints of equation (45) we need the existence of inverses of the parameters. For this reason we have considered Galois quantum systems where the dimension is a power of a prime. In this case all the parameters belong to the field $GF(p^n)$ and we can solve the constraints and we are left with $2N^2 + N$ independent integer parameters. We have discussed explicitly the case $GF(9)$ in order to show how the Galois theory can be embodied into the theory of finite quantum systems.

The symplectic operator S has been constructed numerically for the general case. This can be used in further studies of the entanglement properties of symplectically transformed states.

In this paper we have used symplectic transformations in the context of repetition codes. Repetition codes are the simplest possible codes and involve a small number of qudits. However they can only protect qudits from a very limited type of errors. Mathematically, they are based on the Hilbert space H_A of equation (48), they have distance 1 and they cannot protect against errors that involve the Z operator.

We have considered the space $H_S \equiv SH_A$ of equation (52) and shown that a code based on H_S has (in general) distance greater than 1. This is because the X_S and Z_S involve simultaneous transformations on more than one qudit. Larger distance means that errors on more qudits can be corrected.

For numerical simplicity we have considered an example with $N = 3$ qutrits and the transformations of equation (64). We have described explicitly the numerical procedure that calculates the states $|J_S; 1\,m\rangle$ and the result is given in equation (70). Explicit formulae for X_S, Z_S are given in equations (67) and (68). We have shown that the distance of the code is 2. This is not enough for general error correction on one qudit, but the example demonstrates that the distance increases in symplectically entangled repetition codes and also shows how to numerically construct the appropriate states and transformations. Examples with larger N (and therefore larger distance) can be constructed explicitly with the numerical method that we have described, although the calculation is longer.

The present work provides the theoretical background for the development of repetition codes with symplectically entangled Galois qudits.

Appendix A

The formulae given in section 2 are valid for integer j (Bose case) and small amendments to some of them are required for half-integer j (Fermi case) [9]. Equations (1), (5), (7) and (8) should be replaced with the equations

$$F = (2j+1)^{-1/2} \sum_{m,n} \omega \left[\left(m + \frac{1}{2} \right) \left(n + \frac{1}{2} \right) \right] |J; j\, m\rangle\langle J; j\, n| \tag{A.1}$$

$$X = \exp\left[-\mathrm{i} \frac{2\pi}{2j+1} \left(\theta_z + \frac{1}{2} \right) \right] \qquad Z = \exp\left[\mathrm{i} \frac{2\pi}{2j+1} \left(J_z + \frac{1}{2} \right) \right] \tag{A.2}$$

$$X^\beta |\theta; j\, m\rangle = \omega \left[-\beta \left(n + \frac{1}{2} \right) \right] |\theta; j\, m\rangle \tag{A.3}$$

$$Z^\alpha |J; j\, m\rangle = \omega \left[\alpha \left(m + \frac{1}{2} \right) \right] |J; j\, m\rangle \tag{A.4}$$

correspondingly. It is seen that the above equations replace the m which takes half-integer values with the $m + 1/2$ which take integer values. This is because the proof of a lot of these equations is based on the formula

$$(N)^{-1/2} \sum_{n=0}^{N} \exp\left[\mathrm{i} \frac{2\pi}{N} n(m - m') \right] = \delta(m, m') \tag{A.5}$$

which is valid for integers.

For qubits the above equations give

$$X\left|J; \tfrac{1}{2}\tfrac{1}{2}\right\rangle = \left|J; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle \qquad X\left|J; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle = \left|J; \tfrac{1}{2}\tfrac{1}{2}\right\rangle \tag{A.6}$$

$$Z\left|J; \tfrac{1}{2}\tfrac{1}{2}\right\rangle = -\left|J; \tfrac{1}{2}\tfrac{1}{2}\right\rangle \qquad Z\left|J; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle = \left|J; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle \tag{A.7}$$

$$\left|\theta; \tfrac{1}{2}\tfrac{1}{2}\right\rangle = \left|J; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle - \left|J; \tfrac{1}{2}\tfrac{1}{2}\right\rangle \qquad \left|\theta; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle = \left|J; \tfrac{1}{2} - \tfrac{1}{2}\right\rangle + \left|J; \tfrac{1}{2}\tfrac{1}{2}\right\rangle. \tag{A.8}$$

So for half integer j, we can either use the formulae given in this appendix or equivalently we can use the Bosonic formulae given section 2 with m taking the *integer* values from 0 to $2j$.

Appendix B

In this appendix we calculate the power $(X^\beta Z^\alpha)^s$. We know immediately that the result is of the form $\omega^\phi X^{\beta s} Z^{\alpha s}$ and here we calculate the phase ϕ

$$(X^\beta Z^\alpha)^s = (Q_A \otimes R_B)^s = (Q_A \otimes \mathbf{1})^s (\mathbf{1} \otimes R_B)^s \qquad Q = X^{\beta_A} Z^{\alpha_A} \qquad R = X^{\beta_B} Z^{\alpha_B}. \tag{B.1}$$

Then we have

$$(Q_A \otimes \mathbf{1})^s = Q_A^{s_A} \otimes Q_B^{s_B} \qquad (\mathbf{1} \otimes R_B)^s = [(R_A \otimes \mathbf{1})^\epsilon]^s = (R_A \otimes \mathbf{1})^{s\epsilon}. \tag{B.2}$$

Taking into account that $s\epsilon = s_B + \epsilon(s_A - s_B)$ we find

$$(X^\beta Z^\alpha)^s = \left(Q_A^{s_A} R_A^{s_B}\right) \otimes \left(Q_B^{s_B} R_B^{s_A - s_B}\right) = \omega^\phi X^{\beta s} Z^{\alpha s}$$

$$\phi = \tfrac{1}{2}\alpha_A\beta_A\left(s_A^2 - s_A + s_B^2 - s_B\right) + \tfrac{1}{2}\alpha_B\beta_B\left(s_A^2 - s_A + 2s_B^2 - 2s_A s_B\right) + \alpha_A\beta_B\left(2s_A s_B - s_B^2\right) \tag{B.3}$$

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 Bull R 1979 *Am. Math. Soc.* **1** 847
Hannay J H and Berry M V 1980 *Physica* D **1** 267
Balian R and Itzykson C 1986 *C. R. Acad. Sci.* **303** 773
Mehta M L 1987 *J. Math. Phys.* **28** 781
Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
Fairlie D B, Fletcher P and Zachos C K 1990 *J. Math. Phys.* **31** 1088
Varadarajan V S 1995 *Lett. Math. Phys.* **34** 319
Leonhardt U 1996 *Phys. Rev.* A **53** 2998
[3] 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 **29** 4275
Vourdas A 2004 *Rep. Prog. Phys.* **67** to be published
[4] Vourdas A 2003 *J. Opt. B: Quantum Semiclass. Opt.* **5** S581
[5] Nielsen M A and Chuang I L 2000 *Quantum Information and Quantum Computing* (Cambridge: Cambridge University Press)
Bouwmeester D, Ekert A and Zeilinger A 2000 *The Physics of Quantum Information* (Berlin: Springer)
Lomonaco S 2002 *Quantum Computation (Providence, American Mathematical Society)*
[6] Grassl M, Beth T and Pellizzari T 1997 *Phys. Rev.* A **56** 33
Cleve R, Gottesman D and Lo H-K 1999 *Phys. Rev. Lett.* **83** 648
[7] Laflamme R, Miquel C, Paz J P and Zurek W H 1996 *Phys. Rev. Lett.* **77** 198
Knill E and Laflamme R 1997 *Phys. Rev.* A **55** 900
Braunstein S and Smolin J A 1997 *Phys. Rev.* A **55** 945
[8] Shor P 1995 *Phys. Rev.* A **52** 2493
[9] Steane A 1996 *Phys. Rev. Lett.* **77** 793
Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098
[10] Rains E M 1999 *IEEE Trans. Inf. Theo.* **45** 1827
Gottesman D 1999 *Chaos Solitons Fractals* **10** 1749
Gottesman D 1999 *Lecture Notes Computer Science* **1509** 302
Gottesman D, Kitaev A and Preskill J 2001 *Phys. Rev.* A **64** 012310
Asikhmin A and Knill E 2001 *IEEE Trans. Inf. Theo.* **47** 3065
Bartlett S D, de Guise H and Sanders B C 2002 *Phys. Rev.* A **65** 052316
[11] Vourdas A 2002 *Phys. Rev.* A **65** 042321
[12] Lin S and Costello D J 1983 *Error Control Coding* (New Jersey: Prentice Hall)
Hirschfeld J W P 1979 *Projective geometries over finite fields* (Oxford: Oxford University Press)
[13] Gel'fand I M, Graev M I and Piatetskii-Shapiro I I 1990 *Representation Theory and Automorphic Functions* (London: Academic)
Gel'fand I M and Graev M I 1962 *Dokl. Akad. Nauk. SSSR* **147** 529
Piatetskii-Shapiro I I 1983 *Complex Representations of GL (2, K) for Finite Fields K* (Providence: AMS)
Terras A 1999 *Fourier Analysis on Finite Groups and Applications* (Cambridge: Cambridge University Press)
[14] Weil A 1964 *Acta Math.* **111** 143
Weil A 1965 *Acta Math.* **113** 1
[15] Tanaka S 1966 *Osaka J. Math.* **3** 229
Tanaka S 1967 *Osaka J. Math.* **4** 65
[16] Clairbank A R, Rains E M, Shor P W and Sloane N J A 1998 *IEEE Trans. Inf. Theor.* **44** 1369
[17] Birkhoff G and MacLane S 1995 *A Survey of Modern Algebra* (New York: MacMillan)
Garling D J H 1986 *A course in Galois theory* (Cambridge: Cambridge University Press)
Peterson W W and Weldon E J 1972 *Error Correcting Codes* (Cambridge: MIT Press)
Berlekamp E R 1968 *Algebraic coding theory* (New York: McGraw-Hill)
Van der Waerden B L 1953 *Modern Algebra* **1** and **2** (New York: Frederick Ungar)
Blahut R E 1985 *Fast Algorithms for Digital Signal Processing* (Reading, Mass: Addison-Wesley)