IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **47** (2014) 435303 (23pp) doi:10.1088/1751-8113/47/43/435303

Discrete phase-space approach to mutually orthogonal Latin squares

Mario Gaeta[1], Olivia Di Matteo[2,3], Andrei B Klimov[1] and Hubert de Guise[2]

[1] Departamento de Física, Universidad de Guadalajara, 44420 Guadalajara, Jalisco, Mexico
[2] Department of Physics, Lakehead University, Thunder Bay, Ontario P7B 5E1, Canada

E-mail: hubert.deguise@lakeheadu.ca

Received 8 April 2014, revised 27 August 2014
Accepted for publication 29 August 2014
Published 13 October 2014

Abstract
We show there is a natural connection between Latin squares and commutative sets of monomials defining geometric structures in finite phase-space of prime power dimensions. A complete set of such monomials defines a mutually unbiased basis (MUB) and may be associated with a complete set of mutually orthogonal Latin squares (MOLS). We translate some possible operations on the monomial sets into isomorphisms of Latin squares, and find a general form of permutations that map between Latin squares corresponding to unitarily equivalent mutually unbiased sets.

Keywords: mutually unbiased bases, finite fields, Latin squares, phase space
PACS numbers: 42.50.Dv, 03.65.Ta, 03.65.Fd

1. Introduction

Relations between mutually orthogonal Latin squares (MOLS) [1, 2] and mutually unbiased bases (MUBs) [3–6] have been the subject of renewed interest [7–11]. MOLS have been studied since Euler; they find applications in the design of experiments [12], coding theory (see for instance the text on Latin squares by [2]), compressed sensing [13, 14] and a variety of areas in pure and applied mathematics [15]. MUBs [16, 17] on the other hand, have a much shorter history; a complete set of MUBs constitutes an optimal experimental choice for reconstructing the density matrix of a system, a property that strongly suggests a connection between MUBs and MOLS.

[3] Current address: Department of Physics and Astronomy, Institute for Quantum Computing, University of Waterloo, Canada.

One (of many possible) way of obtaining a complete set of MUBs is based on the construction of eigenstates of disjoint sets of commuting monomials [4, 18–20]. In prime power dimensions, the explicit construction of such sets can be carried out in terms of symplectic spreads [21, 22] or planar functions [23]. There is a simple correspondence between these types of MUBs and MOLS [3, 7–10]. One concludes from this correspondence that sets of commuting monomials can be nicely represented as particular geometrical structures in a finite phase-space [24]. This opens up a possibility of connecting phase-space geometry with MOLS.

Here we focus on the relation between MOLS and MUBs from the perspective of phase-space. In particular, we analyze what types of MUBs can be directly converted into MOLS, and find the image of some useful Clifford transformations of the MUBs on the corresponding MOLS. We also discuss the factorization structure of MUBs [19, 25] on the level of MOLS: it will be shown that for MUBs associated to MOLS, a set of 'legal' transformations on MUBs (comprising transformations of the CNOT type on multi-particle MUBs, plus some specific local transformations) induce isomorphisms between the corresponding MOLS. In particular, starting with MUBs associated with Desarguesian MOLS, 'legal' transformations will produce a new set of MUBs also associated to Desarguesian MOLS. This leads to the observation that, although CNOT operations change the separability properties of MUBs, they do not affect the type of MOLS.

Finally, we analyze the inverse relation between MOLS and MUBs of monomial type and propose an explicit procedure to identify MOLS that are related to such MUBs.

2. MUBs, monomials and commutative curves

We start by enumerating elements in the field $\mathbb{F}_{p^n}$ as

$$\mathbb{F}_{p^n} = \left\{ \sigma^i,\ i = 0,\ \ldots,\ p^n - 1 \right\}, \tag{1}$$

with

$$\sigma^i = \begin{cases} 0 & \text{if } i = 0, \\ \sigma^i & \text{if } i = 1,\ \ldots,\ p^n - 1, \end{cases} \tag{2}$$

where $\sigma \in \mathbb{F}_{p^n}$ is a primitive element (a root of a minimal irreducible polynomial). We alert the reader to our unusual notation, where $\sigma^0 = 0$: this choice is very convenient as we will construct Latin squares from the exponents of a primitive element in the finite field $\mathbb{F}_{p^n}$. Generic elements in $\mathbb{F}_{p^n}$ are denoted by α and β. It is sometimes convenient to think of α and β as parametric functions on $\mathbb{F}_{p^n}$, in which case we write $\alpha(\sigma^i)$ and $\beta(\sigma^i)$. All arithmetic is done over the finite field.

2.1. Monomials

To each $\sigma^i \in \mathbb{F}_{p^n}$ we associate a ket vector $|\sigma^i\rangle$ so that $\{|\sigma^i\rangle,\ i = 0,\ \ldots,\ p^n - 1\}$ is an orthonormal basis in the Hilbert space of an n qudit system: $\langle\sigma^i|\sigma^j\rangle = \delta_{ij}$.

We introduce two families of basic operators $\{Z_\alpha,\ \alpha \in \mathbb{F}_{p^n}\}$ and $\{X_\beta,\ \beta \in \mathbb{F}_{p^n}\}$, conveniently taken to be of the form

$$Z_\alpha = \sum_{i=0}^{p^n-1} \chi(\alpha\sigma^i)|\sigma^i\rangle\langle\sigma^i|, \qquad X_\beta = \sum_{i=0}^{p^n-1} |\sigma^i + \beta\rangle\langle\sigma^i|, \tag{3}$$

where

$$\chi(\alpha) = \exp\left[\frac{2\pi i}{p}\,\mathrm{Tr}\,(\alpha)\right], \quad \mathrm{Tr}\,(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}} \pmod p, \tag{4}$$

and Tr is the usual trace mapping $\mathbb{F}_{p^n} \to \mathbb{F}_p$ [20]. Note this implies $Z_0 = X_0 \equiv \mathbb{1}$.

It will prove extremely useful to consider $\mathbb{F}_{p^n}$ as an n-dimensional linear space, so that any $\alpha \in \mathbb{F}_{p^n}$ can be expressed as a linear combination of elements of the (almost) self-dual basis $\{\theta_1, \ldots, \theta_n\}$

$$\alpha = \sum_{i=1}^{n} a_i\theta_i, \quad a_i \in \mathbb{Z}_p, \qquad \beta = \sum_{i=1}^{n} b_i\theta_i, \quad b_i \in \mathbb{Z}_p,$$
$$\mathrm{Tr}\,(\theta_i\theta_j) = c_j\delta_{ij}, \quad c_j \in \mathbb{Z}_p. \tag{5}$$

It is always possible to enumerate the basis elements $\{\theta_i\}$ in an order where $c_j = 1$ for $j > 1$. We can then write

$$Z_\alpha = \mathcal{Z}^{c_1a_1} \otimes \ldots \otimes \mathcal{Z}^{c_na_n}, \quad X_\beta = \mathcal{X}^{b_1} \otimes \ldots \otimes \mathcal{X}^{b_n}, \tag{6}$$

where $\mathcal{Z}$ and $\mathcal{X}$ are the generalized p-dimensional Pauli matrices. The monomials

$$Z_\alpha X_\beta = \mathcal{Z}^{c_1a_1}\mathcal{X}^{b_1} \otimes \mathcal{Z}^{c_2a_2}\mathcal{X}^{b_2} \otimes \ldots \otimes \mathcal{Z}^{c_na_n}\mathcal{X}^{b_n} \tag{7}$$

are then elements of the generalized Pauli group $\mathcal{P}_n$, i.e. satisfy $Z_\alpha X_\beta = \chi(\alpha\beta)X_\beta Z_\alpha$.

2.2. Additive and commutative curves

First, recall that two orthonormal bases $\{|A_i\rangle, i = 1, \ldots, d\}$ and $\{|B_j\rangle, j = 1, \ldots, d\}$ are said to be mutually unbiased if

$$|\langle A_i \mid B_j \rangle| = \frac{1}{\sqrt{d}}, \quad \forall\, i, j. \tag{8}$$

The set $\{|A_i\rangle\}$ can taken as the common eigenvectors of $d-1$ commuting operators $\{|A_i\rangle\langle A_i|\}$, while $\{|B_j\rangle\}$ is constructed from another set of commuting operators, disjoint from the set used to construct $\{|A_i\rangle\}$. Two sets of commuting operators are traditionally referred to as being mutually unbiased if they have eigenvectors satisfying the condition of equation (8).

If $d+1$ disjoint mutually unbiased sets of commuting operators exist, we have a complete set of MUBs. With $d = p^n$ and p a prime, it is known that (in general, several) complete sets of MUBs exist. Here we will focus on complete sets of commuting *monomials* [18, 20] of the form given in equation (7). Such sets can be:

(a) unitarily equivalent, but not locally equivalent; these sets are distinguished by their factorization structure [19, 25],
(b) unitarily inequivalent [22].

It is convenient to label sets of commuting monomials by points of additive, commutative curves [24] $\{Z_{\alpha(\sigma^i)}X_{\beta(\sigma^i)}, i = 1, \ldots, p^n - 1\}$ in discrete phase-space. For a system of n qudits phase-space is a discrete grid of $p^n \times p^n$ points $\{(\alpha, \beta), \alpha, \beta \in \mathbb{F}_{p^n}\}$ [16, 26, 27], whose axes are labelled by elements of the finite field $\mathbb{F}_{p^n}$, endowing the grid with standard

geometrical properties [28]. With this geometrical structure, an operator $Z_\alpha X_\beta$ is mapped to a unique point in phase-space.

If the points (α, β) of a curve are given in parametric form

$$\alpha = \alpha(\sigma^i), \qquad \beta = \beta(\sigma^i), \tag{9}$$

then *additive curves* satisfy the requirement

$$\alpha(\sigma^i + \sigma^j) = \alpha(\sigma^i) + \alpha(\sigma^j), \qquad \beta(\sigma^i + \sigma^j) = \beta(\sigma^i) + \beta(\sigma^j), \tag{10}$$

for any $\sigma^i, \sigma^j \in \mathbb{F}_{p^n}$. To enforce the commutativity of operators within a set, namely

$$\left[Z_{\alpha(\sigma^i)} X_{\beta(\sigma^i)}, Z_{\alpha(\sigma^j)} X_{\beta(\sigma^j)}\right] = 0, \tag{11}$$

we must consider *commutative curves*, by which we understand such curves satisfy

$$\mathrm{Tr}\left(\alpha(\sigma^i)\beta(\sigma^j)\right) = \mathrm{Tr}\left(\alpha(\sigma^j)\beta(\sigma^i)\right). \tag{12}$$

3. Latin squares and commutative curves

3.1. Invertibility and unbiasedness

We focus on commutative curves defined by invertible functions. Invertibility means there is a one-to-one correspondence between coordinates α and β on the curve; alternatively, no particular value $\alpha(\sigma^i)$ or $\beta(\sigma^i)$ occurs more than once in a given curve, so $\alpha(\sigma^i)$ and $\beta(\sigma^i)$ are just the field elements enumerated in some order generally different from that given in equation (1).

Hence, points on an invertible curve can be written in the form $\beta = f(\alpha)$, where $f(\alpha)$ is a non-singular (invertible) function such that

$$f(\alpha) = \sum_{i=0}^{n-1} \phi_i \, \alpha^{p^i}, \qquad \phi_k := \phi_{n-k}^{p^k}, \; k = 1, \ldots, [(n-1)/2], \tag{13}$$

and $\phi_i, \alpha \in \mathbb{F}_{p^n}$. Here, [ ] denotes the integer part. If n is even, there is the additional requirement $\phi_{n/2} = \phi_{n/2}^{p^{n/2}}$ [24, 29]. We can thus also write $\alpha = f^{-1}(\beta)$.

Let us recall that a (general) Latin square is a $d \times d$ array where the symbols $0, \ldots, d-1$ occur once and only once in each row and each column. Two Latin squares $L^{(1)}$ and $L^{(2)}$ are mutually orthogonal if all the pairs $(L_{ij}^{(1)}, L_{ij}^{(2)})$, $i, j = 0, \ldots d-1$, occur once and only once.

It is straightforward to see that to each *invertible* curve $\beta = f(\alpha)$ corresponds a Latin square with entries

$$L_{ij}^{(f)} = \sigma^j + f(\sigma^i) \equiv \sigma^k, \qquad i, j = 0, \ldots, N-1, \tag{14}$$

where, as indicated in equation (2), σ^k is the k'th power of a primitive element $\sigma \in \mathbb{F}_{p^n}$. For specified f and all i, j, equation (14) produces some other element σ^k in the field; for simplicity, the entry $L_{ij}^{(f)}$ at position (i, j) of the Latin square will be written as k. The LS constructed according to (14) is *standard*, since the symbols of the first row are ordered in increasing powers of σ.

As a simple illustration of equation (14) we consider a two-qubit system, for which the relevant field is $\mathbb{F}_{2^2}$, with elements constructed using the irreducible polynomial $\sigma^2 + \sigma + 1$. Choose the function $\beta = f(\sigma^i) = \sigma\sigma^i$ (for instance). Indexing rows and columns from 0, the resultant square is

$$L^{(\sigma\alpha)} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}. \tag{15}$$

Disjoint sets of commuting monomials $\{Z_\alpha X_{f_\xi(\alpha)}, \xi = 0, 1, \dots, p^n - 2\}$ are mapped to curves with no point in common (except at the origin) [24].

For example, one easily verifies that the set of operators $\{Z_{\sigma^i} X_{\lambda\sigma^i}, i = 0, \dots p^n - 1\}$, for some fixed $\lambda \in \mathbb{F}^*_{p^n} \equiv \mathbb{F}_{p^n} \backslash \{0\}$, commute with each other. The set of points $\{(\sigma^i, \lambda\sigma^i)\}$ is a straight line (a ray) with slope λ in discrete phase-space.

The connection between MUBs and MOLS is that, under the proper conditions, the same 'bundle' of nonintersecting curves $\{f_\xi\}$ is used to simultaneously construct a complete set of MUBs and MOLS: to a set of MUBs described by $p^n - 1$ invertible, nonintersecting curves corresponds a complete set of MOLS. Since the curves in the bundle do not intersect (except at the origin), the associated Latin squares will be orthogonal. The maximum number of invertible curves in a bundle describing a complete set of MUBs is $p^n - 1$. (It would appear there are two curves missing, as we need $p^n + 1$ sets of commuting operators, but only have $p^n - 1$ invertible curves. This is because two of the curves are always non-invertible. For instance, the curve $\beta = 0$ corresponding to operators of the type Z_α, and the curve $\alpha = 0$ corresponds to operators of the type X_β, are not invertible. The squares corresponding to these curves have identical entries across each column and row, respectively. These special curves and resulting squares are excluded from our discussion.)

3.2. The adjacency matrix

We can use the (almost) self-dual basis $\{\theta_1, \dots, \theta_n\}$ to write equation (14) in a compact form useful for later analysis. Let us expand

$$\sigma^i = \sum_k s^i_k c_k^{-1} \theta_k, \qquad s^i_k = \mathrm{Tr}\left[\sigma^i \theta_k\right], \tag{16}$$

with c_i given in equation (5), and define

$$\mathbf{s}^i = \left(s^i_1, \dots, s^i_n\right), \quad \boldsymbol{\theta} = \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} c_1 & \dots & 0 \\ 0 & \ddots & \vdots \\ 0 & \dots & c_n \end{pmatrix}. \tag{17}$$

As mentioned at the start of section 2, the Latin squares are not constructed from the element σ^i but rather from its exponent. Thus, in transforming Latin squares we are ultimately interested in the exponent i of the vector $\mathbf{s}^i$ associated with the element σ^i.

We introduce the adjacency matrix [29] associated to a curve f

$$\boldsymbol{\Gamma}^{(f)}_{k\ell} = \mathrm{Tr}\Big(c_\ell^{-1}\theta_\ell\, f\left(c_k^{-1}\theta_k\right)\Big) \in \mathbb{F}_p. \tag{18}$$

The adjacency matrix has a number of useful properties.

(a) For invertible curves, $\det[\boldsymbol{\Gamma}^{(f)}] \neq 0$.
(b) A necessary and sufficient condition for an adjacency matrix to describe an additive, commutative curve f is that it be symmetric: $\boldsymbol{\Gamma}^{(f)}_{k\ell} = \boldsymbol{\Gamma}^{(f)}_{\ell k}$ [29].

(c) For composition of two functions f and g

$$\boldsymbol{\Gamma}^{(f\,\circ\,g)} = \boldsymbol{\Gamma}^{(g)}\ \mathbf{C}\,\boldsymbol{\Gamma}^{(f)}. \tag{19}$$

(d) For the inverse of a curve, f^{-1}

$$\boldsymbol{\Gamma}^{\left(f^{-1}\right)} = \mathbf{C}^{-1}\left(\boldsymbol{\Gamma}^{(f)}\right)^{-1}\mathbf{C}^{-1}. \tag{20}$$

In addition, if f is the identity function Id such that $\mathrm{Id}(\sigma^i) = \sigma^i$, then $\boldsymbol{\Gamma}^{(\mathrm{Id})} = \mathbf{C}^{-1}$. It follows from equations (16)–(17) that

$$\sigma^j = \mathbf{s}^j\,\mathbf{C}^{-1}\boldsymbol{\theta} = \mathbf{s}^j\,\boldsymbol{\Gamma}^{(\mathrm{Id})}\,\boldsymbol{\theta}, \qquad f\left(\sigma^i\right) = \mathbf{s}^i\,\boldsymbol{\Gamma}^{(f)}\,\boldsymbol{\theta}, \tag{21}$$

and we can rewrite equation (14) quite compactly as the matrix product

$$L^{(f)}_{ij} = \left(\mathbf{s}^j\,\mathbf{C}^{-1} + \mathbf{s}^i\,\boldsymbol{\Gamma}^{(f)}\right)\boldsymbol{\theta}. \tag{22}$$

4. Standard and non-standard Latin squares

The points of a curve f need not necessarily be listed in increasing powers of σ but can also be given in parametric form $(\alpha(\sigma^i), \beta(\sigma^i))$ where both $\alpha(\sigma^i)$ and $\beta(\sigma^i)$ are invertible functions, so that $f(\sigma^i) = \beta(\alpha^{-1}(\sigma^i))$. We make the important observation that the parametric $(\alpha(\sigma^i), \beta(\sigma^i))$ and explicit $f(\sigma^i)$ forms of a curve differ only by the order in which points are enumerated. We need to use both forms as we will show that different orderings correspond to Latin squares differing by a permutation of columns.

If we consider the adjacency matrices $\Gamma^{(\alpha)}$ and $\Gamma^{(\beta)}$ of a parametric curve $(\alpha(\sigma^i), \beta(\sigma^i))$, we obtain from equation (19)

$$\boldsymbol{\Gamma}^{(f)} = \left(\boldsymbol{\Gamma}^{(\alpha)}\mathbf{C}\right)^{-1}\boldsymbol{\Gamma}^{(\beta)}. \tag{23}$$

A LS can be constructed using this ordering

$$\tilde{L}^{(f)}_{ij} = \left(\mathbf{s}^j\,\boldsymbol{\Gamma}^{(\alpha)} + \mathbf{s}^i\,\boldsymbol{\Gamma}^{(\beta)}\right)\boldsymbol{\theta}, \tag{24}$$

but it is not standard. We use $\tilde{L}$ to denote such a non-standard square.

The columns and rows of $\tilde{L}^{(f)}_{ij}$ are related to those of standard LS of equation (22) as follows. Consider the very first row, $i = 0$, and compare the ordering of the symbols in this row for both $\tilde{L}$ and L: the entry $(0, j)$ of $\tilde{L}^{(f)}$ contains symbol k such that

$$\tilde{L}^{(f)}_{0j} = \alpha\left(\sigma^j\right) = \mathbf{s}^j\,\boldsymbol{\Gamma}^{(\alpha)}\boldsymbol{\theta} = \mathbf{s}^k\mathbf{C}^{-1}\boldsymbol{\theta} \qquad \text{for some } k. \tag{25}$$

Thus, the column permutation

$$\text{column } j \to k \text{ with } k \text{ such that} \quad \mathbf{s}^k = \mathbf{s}^j\,\boldsymbol{\Gamma}^{(\alpha)}\mathbf{C} \tag{26}$$

will bring $\tilde{L}^{(f)}$ to a standard square which still differs from $L^{(f)}$ by row permutations. Now, set $j = 0$ in $\tilde{L}^{(f)}$ so the entries of the first column are

$$\tilde{L}^{(f)}_{i0} = \beta(\sigma^i) = \mathbf{s}^i \boldsymbol{\Gamma}^{(\beta)}\boldsymbol{\theta} = \mathbf{s}^k \boldsymbol{\Gamma}^{(f)}\boldsymbol{\theta}$$
$$= \mathbf{s}^k \left(\boldsymbol{\Gamma}^{(\alpha)}\mathbf{C}\right)^{-1}\boldsymbol{\Gamma}^{(\beta)}\boldsymbol{\theta} \quad \text{for some } k, \tag{27}$$

where equation (23) has been used. Thus, the row permutation

$$\text{row } i \to k \text{ with } k \text{ such that } \quad \mathbf{s}^k = \mathbf{s}^i\left(\boldsymbol{\Gamma}^{(\alpha)}\mathbf{C}\right), \tag{28}$$

combined with the column permutation of equation (26) will bring $\tilde{L}^{(f)}$ to $L^{(f)}$. We note here that the permutations of row and columns commute.

5. Operations on individual monomials and corresponding Latin squares

Since any unitary transformation applied to an n-qudit state can be decomposed into a product of CNOT-type operations and local transformations [30], we consider the result of these operations on monomials and the corresponding permutations of rows, columns and symbols of Latin squares such operations induce. For this purpose, it is simplest to initially list fields elements in increasing powers of σ.

5.1. CNOT transformations

The standard CNOT operation performed on qudits p and q is defined as

$$\text{CNOT}_{pq}\,|\lambda\rangle = |\lambda + \text{Tr}(\lambda c_p^{-1}\theta_p)\theta_q\rangle, \qquad \lambda \in \mathbb{F}_{p^n}, \tag{29}$$

so that under the action of the mth power CNOT (with $m = 0, 1, \ldots, p-1$)

$$\text{CNOT}^m_{pq}\,|\lambda\rangle = |\lambda + m\,\text{Tr}(\lambda c_p^{-1}\theta_p)\theta_q\rangle, \tag{30}$$

the monomials are transformed as

$$\ldots \otimes Z_p^{c_p a_p} X_p^{b_p} \otimes \ldots \otimes Z_q^{c_q a_q} X_q^{b_q} \otimes \ldots$$
$$\to \ldots \otimes Z_p^{c_p a_p - m\, c_q a_q} X_p^{b_p} \otimes \ldots \otimes Z_q^{c_q a_q} X_q^{m\, b_p + b_q} \otimes \ldots . \tag{31}$$

In terms of field elements, $Z_{\sigma^i}X_{f(\sigma^i)}$ is transformed into $Z_{\alpha(\sigma^i)}X_{\beta(\sigma^i)}$, where [29]

$$\alpha(\sigma^i) = \sigma^i - m\,\text{Tr}\left(\sigma^i\theta_q\right)c_p^{-1}\theta_p,$$
$$\beta(\sigma^i) = f(\sigma^i) + m\,\text{Tr}\left(f(\sigma^i)c_p^{-1}\theta_p\right)\theta_q. \tag{32}$$

The action of CNOT transforms the adjacency matrix of a standard LS to a new adjacency matrix given by

$$\boldsymbol{\Gamma}^{(g)} = \left(\mathbf{X}^m_{p,\,q}\right)^T \boldsymbol{\Gamma}^{(f)} \mathbf{X}^m_{p,\,q}, \tag{33}$$

where T denotes transposition. Since $\det[\mathbf{X}^m_{p,\,q}] \neq 0$, the CNOT operation does not change the invertibility property of a curve.

The Latin square associated with the set $Z_{\alpha(\sigma^i)}X_{\beta(\sigma^i)}$ is obtained using equation (24), with new adjacency matrices

$$\boldsymbol{\Gamma}^{(\alpha)} = \left(\mathbf{X}^{-m}_{p,\,q}\right)^T \mathbf{C}^{-1}, \quad \boldsymbol{\Gamma}^{(\beta)} = \boldsymbol{\Gamma}^{(f)}\mathbf{X}^m_{p,\,q}, \tag{34}$$

where we use

$$\left(\mathbf{X}^{m}_{p,\,q}\right)_{ij} = \delta_{ij} + m\delta_{ip}\delta_{jq}, \tag{35}$$

to represent the CNOT operation. The resulting non-standard LS is

$$\tilde{L}^{(g)}_{ij} = \left(\mathbf{s}^{j}\left(\mathbf{X}^{\,-m}_{p,q}\right)^{T}\mathbf{C}^{-1} + \mathbf{s}^{i}\left(\mathbf{X}^{-m}_{p,\,q}\right)^{T}\boldsymbol{\Gamma}^{(g)}\right)\boldsymbol{\theta}, \tag{36}$$

where equation (23) (with $f \to g$) and $\left(\mathbf{X}^{m}_{p,\,q}\right)^{-1} = \left(\mathbf{X}^{-m}_{p,\,q}\right)$ have been used.

The Latin square $\tilde{L}^{(g)}$ of equation (36) is then clearly related to $L^{(g)}$ by the permutations

$$\begin{aligned} &\text{row } i \to k \text{ with } k \text{ such that } \mathbf{s}^{k} = \mathbf{s}^{i}\left(\mathbf{X}^{\,-m}_{p,q}\right)^{T},\\ &\text{column } j \to k \text{ with } \ k \text{ such that } \mathbf{s}^{k} = \mathbf{s}^{j}\left(\mathbf{X}^{-m}_{p,\,q}\right)^{T}. \end{aligned} \tag{37}$$

We can also obtain the sequence of permutations taking $\tilde{L}^{(g)}$ of equation (36) for the curve g to the original, standard form LS of f, $L^{(f)}$. We can manipulate equation (36) to the form

$$\tilde{L}^{(g)}_{ij} = \left(\mathbf{s}^{j}\,\mathbf{W}\,\mathbf{C}^{-1} + \mathbf{s}^{i}\,\boldsymbol{\Gamma}^{(f)}\right)\left[\mathbf{X}^{m}_{p,\,q}\boldsymbol{\theta}\right], \tag{38}$$

where $\mathbf{W} := \left(\mathbf{X}^{-m}_{p,\,q}\right)^{T}\mathbf{C}^{-1}\mathbf{X}^{-m}_{p,\,q}\mathbf{C}$. $\tilde{L}^{(g)}$ is thus transformed back to the original square $L^{(f)}$ by the following permutations

$$\begin{aligned} &\text{no permutation of rows,}\\ &\text{column } j \to k \text{ with } k \text{ such that} \quad \mathbf{s}^{k} = \mathbf{s}^{j}\,\mathbf{W},\\ &\text{symbol } k \to j \text{ with } k \text{ such that} \quad \mathbf{s}^{k} = \mathbf{s}^{j}\,\mathbf{C}^{-1}\mathbf{X}^{m}_{p,\,q}\mathbf{C} := \mathbf{s}^{j}\,\mathbf{V}. \end{aligned} \tag{39}$$

The symbol swap is inferred from equation (16): in going to the new basis $\left[\mathbf{X}^{m}_{p,\,q}\boldsymbol{\theta}\right]$

$$\sigma^{j} = \mathbf{s}^{j}\,\mathbf{C}^{-1}\,\boldsymbol{\theta} \to \mathbf{s}^{j}\,\mathbf{C}^{-1}\,\mathbf{X}^{m}_{p,\,q}\,\boldsymbol{\theta} = \mathbf{s}^{j}\,\mathbf{V}\,\mathbf{C}^{-1}\,\boldsymbol{\theta} = \mathbf{s}^{k}\,\mathbf{C}^{-1}\,\boldsymbol{\theta}, \tag{40}$$

yielding the last of equation (39).

Write $L^{(g)}$ in the form of equation (22) and compare it to $L^{(f)}$

$$\begin{aligned} L^{(g)}_{ij} &= \left(\mathbf{s}^{j}\,\mathbf{C}^{-1} + \mathbf{s}^{i}\,\boldsymbol{\Gamma}^{(g)}\right)\boldsymbol{\theta}\\ &= \left(\mathbf{s}^{j}\,\mathbf{C}^{-1}\mathbf{X}^{-m}_{p,\,q} + \mathbf{s}^{i}\left(\mathbf{X}^{m}_{p,\,q}\right)^{T}\boldsymbol{\Gamma}^{(f)}\right)\mathbf{X}^{m}_{p,\,q}\boldsymbol{\theta}\\ &= \left(\mathbf{s}^{j}\,\mathbf{V}^{-1}\,\mathbf{C}^{-1} + \mathbf{s}^{i}\left(\mathbf{X}^{\,m}_{p,q}\right)^{T}\boldsymbol{\Gamma}^{(f)}\right)\mathbf{X}^{m}_{p,\,q}\boldsymbol{\theta}. \end{aligned} \tag{41}$$

Comparing this to the form of equation (22), we can see that the following transformation brings us from $L^{(g)}$ back to $L^{(f)}$:

$$\begin{aligned} &\text{row } i \to k \text{ with } k \text{ such that} \quad \mathbf{s}^{k} = \mathbf{s}^{i}\left(\mathbf{X}^{m}_{p,\,q}\right)^{T}\\ &\text{column } j \to k \text{ with } k \text{ such that} \quad \mathbf{s}^{k} = \mathbf{s}^{j}\,\mathbf{V}^{-1},\\ &\text{symbol } k \to j \text{ with } k \text{ such that} \quad \mathbf{s}^{k} = \mathbf{s}^{j}\,\mathbf{V}. \end{aligned} \tag{42}$$

5.2. Local Clifford operations

Recall that our monomials $Z_\alpha X_\beta$ of equation (7) decompose into direct products

$$Z_\alpha X_\beta = \mathcal{Z}^{c_1 a_1}\mathcal{X}^{b_1} \otimes \mathcal{Z}^{c_2 a_2}\mathcal{X}^{b_2} \otimes \ldots \otimes \mathcal{Z}^{c_n a_n}\mathcal{X}^{b_n}.$$

We consider a class of local Clifford operations $\mathbf{U} = \mathbf{U}_1 \otimes \mathbf{U}_2 \otimes \ldots \mathbf{U}_n$, with $\mathbf{U}_i$ acting locally on qudit i, that result in a map from $Z_\alpha X_\beta$ to another Pauli operator

$$\mathbf{U}\Big(Z_\alpha X_\beta\Big)\mathbf{U}^\dagger = Z_{\alpha'} X_{\beta'} = \mathcal{Z}^{c_1 m_1}\mathcal{X}^{\ell_1} \otimes \mathcal{Z}^{c_2 m_2}\mathcal{X}^{\ell_2} \otimes \ldots \otimes \mathcal{Z}^{c_n m_n}\mathcal{X}^{\ell_n}, \tag{43}$$

where $\mathcal{Z}^{c_i m_i}\mathcal{X}^{\ell_i} = \mathbf{U}_i\Big(\mathcal{Z}^{c_i a_i}\mathcal{X}^{b_i}\Big)\mathbf{U}_i^\dagger$.

The $p \times p$ matrix $\mathbf{U}_i$ must therefore induce on the exponents a_i and b_i a map T

$$\mathbf{U}_i \to T\big(\mathbf{U}_i\big) = \begin{pmatrix} k_{11}^i & k_{12}^i \\ k_{21}^i & k_{22}^i \end{pmatrix}, \qquad k_{st}^i \in \mathbb{Z}_p, \quad \det\big[\mathbf{U}_i\big] = 1, \tag{44}$$

so that $\mathcal{Z}^{c_i a_i}\mathcal{X}^{b_i}$ goes to $\mathcal{Z}^{c_i m_i}\mathcal{X}^{\ell_i}$, where

$$\begin{pmatrix} m_i \\ \ell_i \end{pmatrix} = T\big(\mathbf{U}_i\big)\begin{pmatrix} a_i \\ b_i \end{pmatrix}. \tag{45}$$

The effect of local Clifford operations has been investigated in [31], and we borrow their formalism. The analysis is simplified by noting that a set of commuting monomials, augmented with the identity matrix, is an Abelian group of order p^n, obtained from a set $G = \{g_1, g_2, \ldots g_n | g_i \in \mathbb{F}_{p^n}\}$ of n generating elements. Conjugation by $\mathbf{U}$ simply maps the original set G of generating elements to another generating set $G' = \{g_1', g_2', \ldots g_n'\}$.

We introduce, following [31], the $n \times 2n$ generator matrix $\mathbf{A}^{(f)}$, defined on generating elements g_i by

$$\mathbf{A}^{(f)}_{k,\,i} = \mathrm{Tr}\Big[\theta_k\, g_i\Big], \quad \mathbf{A}^{(f)}_{k,\,i+n} = \mathrm{Tr}\Big[c_k^{-1}\theta_k\, f\,(g_i)\Big], \qquad k, i = 1, \ldots, n. \tag{46}$$

The generator matrix $\mathbf{A}^{(f)}$ has the additional property that for non-degenerate curves, it is a non-degenerate matrix, i.e. both $n \times n$ submatrices of the matrix have non-zero determinants.

Choosing $G = \{g_i = c_i^{-1}\theta_i,\, i = 1, \ldots, n\}$ such that the monomials have the form $Z_{c_i^{-1}\theta_i} X_{f(c_i^{-1}\theta_i)}$ reduces the matrix $\mathbf{A}^{(f)}$ to a suitably simple form

$$\mathbf{A}^{(f)} = \big(\mathbb{1} \,|\, \boldsymbol{\Gamma}^{(f)}\big), \tag{47}$$

while for a parametric curve $(\alpha(\sigma^i), \beta(\sigma^i))$, the generator matrix $\mathbf{A}^{(f)}$ is of the form

$$\mathbf{A}^{(\alpha,\beta)} = \big(\boldsymbol{\Gamma}^{(\alpha)}\mathbf{C} \,|\, \boldsymbol{\Gamma}^{(\beta)}\big). \tag{48}$$

It is then easy to verify that conjugation by $\mathbf{U}$ transforms $\mathbf{A}^{(f)}$ to

$$\begin{aligned} \mathbf{A}^{(f)} \to \mathbf{A}^{(\alpha',\beta')} &= \Big(\ \mathbb{1} \,|\, \boldsymbol{\Gamma}^{(f)}\ \Big)\begin{pmatrix} \mathbf{K}_{11} & \mathbf{K}_{12} \\ \mathbf{K}_{21} & \mathbf{K}_{22} \end{pmatrix} \\ &= \Big(\mathbf{K}_{11} + \boldsymbol{\Gamma}^{(f)}\mathbf{K}_{21} \;\Big|\; \mathbf{K}_{12} + \boldsymbol{\Gamma}^{(f)}\mathbf{K}_{22}\Big), \end{aligned} \tag{49}$$

where the diagonal matrices

$$\mathbf{K}_s = \begin{pmatrix} k_s^1 & 0\ldots & 0 \\ 0 & \ddots & 0 \\ 0 & \ldots 0 & k_s^n \end{pmatrix}, \quad s = (11), (12), (21), (22). \tag{50}$$

The new generator matrix has entries $\mathbf{A}^{(\alpha',\beta')}$ resulting in a transformation of the curve $\beta = f(\alpha)$ to (α', β'). The new curve is invertible if $\det[\boldsymbol{\Gamma}^{(\alpha')}] \neq 0$ and $\det[\boldsymbol{\Gamma}^{(\beta')}] \neq 0$. The LS corresponding to these adjacency matrices is given as before in (24). Equation (23), which describes the composition $f = \beta \circ \alpha^{-1}$, can be used to bring $\mathbf{A}^{(\alpha',\beta')}$ to the form $(\mathbb{1} \mid \boldsymbol{\Gamma}^{(f')})$ from which the standard LS can be constructed using f'.

5.3. Composition of curves

The adjacency matrix of a composed curve $\beta = f(g(\alpha))$ is just the product of the corresponding adjacency matrices as in equation (23). Thus we observe that LS transform under composition as

$$L_{ij}^{f \circ g} = \left(\mathbf{s}^j\, \mathbf{C}^{-1} + \mathbf{s}^i\, \boldsymbol{\Gamma}^{(g)}\, \mathbf{C}\, \boldsymbol{\Gamma}^{(f)}\right)\boldsymbol{\theta}. \tag{51}$$

The transformation $\mathbf{s}^i \to \mathbf{s}^i\, \boldsymbol{\Gamma}^{(g)}\, \mathbf{C}$ is a column permutation, so the composition rule allows the construction of *orbits* of LS in the same set of MOLS. Such orbits are obtained by repeated composition of the type $\beta = f \circ f \circ \cdots \circ f(\alpha)$. In the particular case of the so-called Desarguesian bundle $\beta = \lambda\alpha$, the corresponding MOLS contain a single orbit, generated from $f(\alpha) = \sigma\alpha$. In this way all LS in this set of MOLS can be obtained by (cyclic) permutations of rows in the LS corresponding to the $\beta = \sigma\alpha$ orbit.

6. Operations on complete sets of MUBs and MOLS

We are now in a position to discuss operations on a complete set of MUBs described by the maximum number $p^n - 1$ of distinct invertible curves. These distinct curves produce a complete set of $p^n - 1$ MOLS. Although an individual curve admits a large number of unitaries that keep it invertible, the situation is drastically different if we consider all the invertible curves from a set of MUBs described by a bundle of curves corresponding to a set of MOLS.

It is known that a complete set of MOLS (of dimension $d \times d$) exists if and only if a finite projective plane of order d also exists [1, 2]. Of relevance to our discussions are Desarguesian planes, which are based on linear equations over finite fields, i.e. curves of the form $\{f_\lambda(\sigma^i) = \lambda\sigma^i;\ \lambda \in \mathbb{F}_{p^n}^*\}$ with $N = p^n$. A Desarguesian plane exists whenever $d = p^n$. Beyond their associations to Desarguesian planes, the set (or bundle) of linear curves can also be used to obtain monomials describing a complete set of MUBs. It is therefore natural to speak of 'Desarguesian MUBs'.

Additional planes, not of the Desarguesian type, can also exist; these additional planes are not based on linear equations over finite fields. Although there are MOLS associated with those planes, we have not found examples of bundles of curves describing non-Desarguesian planes which result in a complete set of MUBs of the monomial type. We should also point out that there may be MUBs not of the monomial type which could be associated with MOLS.

In this section we explore transformations of one set of MUBs to another while preserving mutual unbiasedness; we map one set of associated MOLS to another and find that such transformations correspond to an isomorphism of the corresponding MOLS. Two sets of

MOLS are isomorphic iff there exists permutations of rows, columns, and symbols such that if applied to every square in the first set one obtains every square in the second set [1]. Two sets of MOLS are also isomorphic if they are 'built' on the same affine (and consequently projective) plane [2].

6.1. CNOT for a complete set of invertible curves

A CNOT operation does not change the invertibility property of curves, as per equation (33). Suppose then, we have a complete set of MUBs described by the maximum number $p^n - 1$ distinct invertible curves; associated to this set (or bundle) of curves is a complete set of $p^n - 1$ MOLS. Applying the same CNOT transformation to each curve, we obtain another set of invertible curves, associated to a different but isomorphic set of MOLS.

To see the action of a CNOT transformation on a complete set of curves, let us choose as our initial bundle the rays associated to the MOLS in standard form

$$f_\lambda(\alpha) = \lambda\alpha, \qquad \lambda \in \mathbb{F}^*_{p^n}. \tag{52}$$

Thus

$$\begin{aligned} g_\lambda(\alpha) &= \mathrm{CNOT}_{pq}\Big[f_\lambda(\alpha)\Big] \\ &= \Big(\alpha + \mathrm{Tr}\big(\alpha\theta_q\big)\mathrm{c}_p^{-1}\theta_p\Big)\lambda + \Big(\mathrm{Tr}\Big(\lambda\alpha\mathrm{c}_p^{-1}\theta_p\Big) + \mathrm{Tr}\big(\alpha\theta_q\big)\,Tr\,\Big(\lambda\mathrm{c}_p^{-2}\theta_p^2\Big)\Big)\theta_q. \end{aligned} \tag{53}$$

Since every invertible curve f_λ transforms under the CNOT to some new invertible curve g_λ, we can use equation (33) to obtain the adjacency matrices of each g_λ after application, and then equation (22) to recover their Latin square in standard form. This gives a new set of LS in standard form. An explicit example is provided in Appendix A.1.

For each new Latin square so obtained, we can use equation (42) to compute the permutations required to take us back to the corresponding Desarguesian squares. These permutations are all identical, meaning that initial and transformed sets are indeed isomorphic.

The CNOT transformation given above yields isomorphic MOLS but changes the separability structure of the associated MUBs. This structure is a common means of classifying MUBs, as MUBs with different factorization structures cannot be related by local unitary transformations [19, 25, 32]. Thus, a phase-space approach where monomials are eventually associated with MOLS provides structural information about the MUBs not contained in their factorization structure. Alternatively, the factorization structure of the MUBs is not reflected at the level of phase-space.

In summary, even if there is a change in the factorization properties resulting from application of a CNOT transformation, the associated MOLS will remain isomorphic and will be isomorphic to the Desarguesian set.

6.2. MOLS and local operations

The transformation properties of *individual* curves was discussed using the generator matrix **A** of section 5.2. We now look at restrictions of these transformations when they are applied to a *bundle* of curves, using again the generator matrix **A**. A local unitary transformation is determined by 4 field elements k_s through the map of equation (45), so we can obtain necessary conditions by examining a limited number of functions carefully chosen to fully constrain these parameters.

A bundle of invertible curves $f_i(\alpha)$, $i = 1, \ldots, p^n - 1$ correspond to both a complete set of MUBs and MOLS. Since MUBs consist of disjoint sets there will always be one and only

one function in the bundle which, for σ_k fixed but otherwise arbitrary, maps some σ_i to this σ_k. For some fixed q, there exists a function–let's call it F^q_m—with the property that

$$F^q_m(\theta_q) = mc_q\theta_q, \qquad m \in \mathbb{Z}^*_p. \tag{54}$$

In other words, they map one (almost) self-dual basis element to a multiple of itself. We will continue by limiting the discussion to two particles; this argument can of course be generalized to any number of particles.

The virtue of F^q_m is that the matrix $\mathbf{A}^{(F^q_m)}$ takes a useful form on the generating elements $\{c_k^{-1}\theta_k\}$: the adjacency matrix will have in the kth row and the kth column a single diagonal entry with value m:

$$\left(\boldsymbol{I}^{(F^q_m)}\right)_{kq} = \mathrm{Tr}\left[\, c_k^{-1}\theta_k F^q_m\left(c_q^{-1}\theta_q\right)\right] = m\delta_{kq}, \tag{55}$$

where k and q label the generating elements. Selecting $q = 1$ for the purpose of the argument, and denoting entries unnecessary to our argument by *, we see that, under a local unitary transformation $\mathbf{U}_1$ on the first particle, with 2×2 representation $T(\mathbf{U}_1)$, $\mathbf{A}^{(F^1_m)}$ is transformed to

$$\begin{aligned}
\mathbf{A}^{(F'^1_m)} &= \left(\begin{array}{cc|cc} 1 & 0 & m & 0 \\ 0 & 1 & 0 & * \end{array}\right)\left(\begin{array}{cc:cc} k^1_{11} & 0 & k^1_{12} & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline k^1_{21} & 0 & k^1_{22} & 0 \\ 0 & 0 & 0 & 1 \end{array}\right), \\
&= \left(\begin{array}{cc|cc} k^1_{11} + mk^1_{21} & 0 & k^1_{12} + mk^1_{22} & 0 \\ 0 & 1 & 0 & * \end{array}\right).
\end{aligned} \tag{56}$$

We are assuming $\det[T(\mathbf{U}_1)] = k^1_{11}k^1_{22} - k^1_{12}k^1_{21} = 1$. In order to preserve non-degeneracy of the resulting curve, we must additionally have

$$k^1_{11} + mk^1_{12} \neq 0, \quad \text{and} \quad k^1_{21} + mk^1_{22} \neq 0. \tag{57}$$

There are thus only two possible forms for the matrix $T(\mathbf{U}_1)$. One possibility is to suppose $k^1_{11} \neq 0$. Then, to guarantee the first of equation (57) we must have $k^1_{21} = 0$. To guarantee the condition on the determinant, we must now have $k^1_{22} \neq 0$, which in turn implies $k^1_{12} = 0$ since equation (57) must hold for arbitrary m. In fact, using the determinant condition we find $k^1_{22} = (k^1_{11})^{-1}$. One then obtains $\mathbf{K}$ as

$$\left(\begin{array}{cc} \mathbf{K}_{11} & \mathbf{K}_{12} \\ \mathbf{K}_{21} & \mathbf{K}_{22} \end{array}\right) = \left(\begin{array}{cc:cc} k^1_{11} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & (k^1_{11})^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{cc} \mathbf{K}_{11} & \mathbf{0} \\ \mathbf{0} & (\mathbf{K}_{11})^{-1} \end{array}\right) \tag{58}$$

Acting on qudit j, this is a *scaling* transformation

$$T\left(\mathbf{U}^{\mathrm{S}}_j\right) = \left(\begin{array}{cc} k_j & 0 \\ 0 & k_j^{-1} \end{array}\right), \tag{59}$$

(S for scaling): under $\mathbf{U}_j^{\mathrm{S}}(k)$ the monomials transform as

$$\mathcal{Z}^{c_1 a_1}\mathcal{X}^{b_1} \to \mathcal{Z}^{c_1 k_j a_1}\mathcal{X}^{k_j^{-1} b_1} = \left(\mathcal{Z}^{c_1 a_1}\right)^{k_j}\left(\mathcal{X}^{b_1}\right)^{k_j^{-1}}, \tag{60}$$

sending $\mathcal{Z} \to \mathcal{Z}^{k_j}$ and $\mathcal{X} \to \mathcal{X}^{k_j^{-1}}$. We call a matrix of the type

$$\begin{pmatrix} \mathbf{K}_{11} & 0 \\ 0 & \left(\mathbf{K}_{11}\right)^{-1} \end{pmatrix} \tag{61}$$

a *type S transformation.*

For the second case, suppose instead that $k_{11}^1 = 0$. Necessarily $k_{21}^1 \neq 0$ and $k_{12}^1 \neq 0$ to preserve $\det\left[T\left(\mathbf{U}_1\right)\right] = 1$. But we can choose to work with any F_m^q, meaning m is arbitrary, which implies in turn that $k_{22}^1 = 0$ to guarantee the second of equation (57) always holds. The same conclusion is reached starting with the assumption $k_{22}^1 = 0$.

We then obtain

$$\begin{pmatrix} \mathbf{K}_{11} & \mathbf{K}_{12} \\ \mathbf{K}_{21} & \mathbf{K}_{22} \end{pmatrix} = \left(\begin{array}{cc:cc} 0 & 0 & -k_j^{-1} & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline k_j & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} \mathbf{K}_{11} & -\overline{\mathbf{K}}_{21} \\ \mathbf{K}_{21} & \mathbf{K}_{11} \end{pmatrix} \tag{62}$$

where $\overline{\mathbf{K}}_s$ is the matrix with the inverses of the non-zero elements of $\mathbf{K}_s$. Recalling

$$T\left(\mathbf{U}_j\right) = \begin{pmatrix} 0 & -k_j^{-1} \\ k_j & 0 \end{pmatrix} \tag{63}$$

we can see that the transformation on the monomials is now

$$\mathcal{Z}^{c_1 a_1}\mathcal{X}^{b_1} \to \mathcal{Z}^{k_j b_1}\mathcal{X}^{-c_i k_j^{-1} a_1} \tag{64}$$

and the indices a_1 and b_1 are interchanged.

Consider the two qubit case, for which $c_1 = 1$ and $a_i, b_i \in \mathbb{Z}_2$. If $a_1 = 0$ and $b_1 = 1$, $\mathcal{X} \to \mathcal{Z}$ and $\mathcal{Z} \to \mathcal{X}$. This means that in the qubit case, this transformation collapses to a Fourier swap of $\mathcal{Z}$ and $\mathcal{X}$. Thus, we call a transformation having the form of equation (62) a *type F transformation*.

These transformations have a form where they explicitly act on the j'th qudit:

$$\mathbf{U}_j^{\mathrm{S}}(r) = \sum_t |t_j\rangle\langle r t_j|, \quad \mathbf{U}_j^{\mathrm{F}}(r) = \sum_{t,m} \frac{\omega^{rmt_j}}{\sqrt{d}}\, |t_j\rangle\langle m_j|. \tag{65}$$

The conditions on the k_s^i are necessary conditions for all curves in the bundle: if they do not hold then at least some of the F_m^q curves will not be invertible. We establish now that when applied on *any* curve, a combination of type S and type F transformations produces at least one non-invertible curve.

Suppose, using our two-particle system, we apply a type S transformation to the first particle, and a type F to the second. Then, for instance

$$T\left(\mathbf{U}_1^{\mathrm{S}}(r)\right) = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}, \qquad T\left(\mathbf{U}_2^{\mathrm{F}}(t)\right) = \begin{pmatrix} 0 & -t^{-1} \\ t & 0 \end{pmatrix} \tag{66}$$

and

$$\mathbf{K} = \left(\begin{array}{cc:cc} r & 0 & 0 & 0 \\ 0 & 0 & 0 & -t^{-1} \\ \hdashline 0 & 0 & r^{-1} & 0 \\ 0 & t & 0 & 0 \end{array}\right) = \begin{pmatrix} \mathbf{K}_{11} & -\overline{\mathbf{K}}_{21} \\ \mathbf{K}_{21} & \overline{\mathbf{K}}_{11} \end{pmatrix}. \tag{67}$$

Applying this to $\mathbf{A}^{(f)} = (\mathbb{1}|\boldsymbol{\Gamma}^{(f)})$, we obtain a transformed generator matrix

$$\begin{aligned} \mathbf{A}^{(f')} = \mathbf{A}^{(f)}\mathbf{K} &= \left(\mathbf{K}_{11} + \boldsymbol{\Gamma}^{(f)}\mathbf{K}_{21}\right| - \overline{\mathbf{K}}_{21} + \boldsymbol{\Gamma}^{(f)}\overline{\mathbf{K}}_{11}\Big) \\ &= \left(\begin{array}{cc|cc} r & \Gamma^{(f)}_{12}t & \Gamma^{(f)}_{11}r^{-1} & 0 \\ 0 & \Gamma^{(f)}_{22}t & \Gamma^{(f)}_{21}r^{-1} & -t^{-1} \end{array}\right). \end{aligned} \tag{68}$$

In a bundle of $p^n - 1$ curves, there will always be one curve such that $f(\theta_1) \propto \theta_2$ (otherwise it would not be complete). For this curve, $\Gamma^{(f)}_{11} = 0$, and thus the second half of the transformed generator matrix will be degenerate, meaning this curve is no longer invertible. This argument can be generalized to any number of particles. Thus, we are limited to local transformations where *all* transformations on the particles are either type S, or type F.

Then

$$\mathbf{A}^{(f')}_{\mathrm{S}} = \Big(\mathbf{K}_{11}\Big|\ \boldsymbol{\Gamma}^{(f)}\mathbf{K}^{-1}_{11}\Big), \quad \mathbf{A}^{(f')}_{\mathrm{F}} = \Big(\boldsymbol{\Gamma}^{(f)}\mathbf{K}_{21}\Big|\ -\mathbf{K}^{-1}_{21}\Big), \tag{69}$$

where $\mathbf{A}^{(f')}_{\mathrm{S}}$ and $\mathbf{A}^{(f')}_{\mathrm{F}}$ are matrices after transformations of types S and F, respectively.

Following equation (48), these transformations correspond to the new parametric curves

$$\boldsymbol{\Gamma}^{(\alpha')} = \mathbf{K}_{11}\mathbf{C}^{-1}, \quad \boldsymbol{\Gamma}^{(\beta')} = \boldsymbol{\Gamma}^{(f)}\mathbf{K}^{-1}_{11}, \quad \text{for S-type,} \tag{70}$$

and

$$\boldsymbol{\Gamma}^{(\alpha')} = \boldsymbol{\Gamma}^{(f)}\mathbf{K}_{21}\mathbf{C}^{-1}, \quad \boldsymbol{\Gamma}^{(\beta')} = -\mathbf{K}^{-1}_{21}, \quad \text{for F-type.} \tag{71}$$

The corresponding LS are obtained from the originals by permutations. Observing that $\mathbf{C}$ and $\mathbf{K}_{ij}$ commute, we must apply the permutations

$$\begin{aligned} &\text{no permutation of rows,} \\ &\text{column } i \to k \ \text{ with } k \text{ such that} \quad \mathbf{s}^k = \mathbf{s}^i\,\mathbf{K}^2_{11}, \\ &\text{symbol } k \to j \text{ with } k \text{ such that} \quad \mathbf{s}^k = \mathbf{s}^j\mathbf{K}^{-1}_{11} \end{aligned} \tag{72}$$

for type S transformations.

For type F transformations, we start from

$$\tilde{L}^{(f')}_{ij} = \Big(\mathbf{s}^j\boldsymbol{\Gamma}^{(f)}\mathbf{K}_{21}\mathbf{C}^{-1} - \mathbf{s}^i\mathbf{K}^{-1}_{21}\Big)\boldsymbol{\theta} \tag{73}$$

and we first interchange the rows and columns. Then, to this transformed square, we can apply the permutations

$$\begin{aligned} &\text{no permutation of rows,} \\ &\text{column } j \to k \ \text{ with } k \text{ such that} \quad \mathbf{s}^k = -\mathbf{s}^j\,\mathbf{K}^{-2}_{21}\,\mathbf{C}^2, \\ &\text{symbol } k \to j \ \text{ with } k \text{ such that} \quad \mathbf{s}^k = \mathbf{s}^j\,\mathbf{C}^{-1}\,\mathbf{K}_{21}. \end{aligned} \tag{74}$$

Although transposition is not an isotopy, the transformed and original squares are still main class equivalent. We note the interesting coincidence that a Fourier transformation will interchange two complementary variables, corresponding to an interchange in the phase-space axes, much like the transposition needed to bring $\tilde{L}_{ij}^{(f')}$ back to $L_{ij}^{(f)}$.

This set of local transformations has interesting composition relations with CNOT operations. If $\mathbf{U}^{\mathrm{S}}$ and $\mathbf{U}^{\mathrm{F}}$ are transformations of type S and F respectively

$$\begin{aligned}\mathbf{U}_p^{\mathrm{S}}(r)\mathbf{U}_q^{\mathrm{S}}(t)\mathbf{X}_{p,\,q}^{m} &\sim \mathbf{X}_{p,\,q}^{mtr^{-1}}\mathbf{U}_p^{\mathrm{S}}(r)\mathbf{U}_q^{\mathrm{S}}(t)\\ \mathbf{U}_p^{\mathrm{F}}(r)\mathbf{U}_q^{\mathrm{F}}(t)\mathbf{X}_{p,\,q}^{m} &\sim \mathbf{X}_{p,\,q}^{-mtr^{-1}}\mathbf{U}_p^{\mathrm{F}}(r)\mathbf{U}_q^{\mathrm{F}}(t),\end{aligned} \tag{75}$$

where $\sim$ indicates these hold to within an overall phase. On the other hand, the composition and commutation relations between $\mathbf{U}_j^{\mathrm{F}}$ and $\mathbf{U}_j^{\mathrm{S}}$ are as follows

$$\mathbf{U}_j^{\mathrm{S}}(k)\mathbf{U}_j^{\mathrm{S}}(r) = \mathbf{U}_j^{\mathrm{S}}(kr), \quad \mathbf{U}_j^{\mathrm{F}}(k)\mathbf{U}_j^{\mathrm{F}}(r) = \mathbf{U}_j^{\mathrm{S}}\left(-kr^{-1}\right), \tag{76}$$

$$\mathbf{U}_j^{\mathrm{S}}(k)\mathbf{U}_j^{\mathrm{F}}(t) = \mathbf{U}_j^{\mathrm{F}}\left(tk^{-1}\right), \quad \mathbf{U}_j^{\mathrm{F}}(t)\mathbf{U}_j^{\mathrm{S}}(k) = \mathbf{U}_j^{\mathrm{F}}(tk). \tag{77}$$

We conclude that unitary transformations on MUBs preserving the complete set of MOLS must be a combination of CNOT transformations, or type S/F transformations, where either type S transformations are applied to all qudits, or type F to all qudits.

This conclusion is important as it allows us to drastically simplify the possible sequence of transformations that map invertible curves to invertible curves. As a result, all non-local transformations can be done consecutively, followed by a sequence of local transformations.

7. Latin minisquares and commutative curves

Curves corresponding to Latin squares are permutation polynomials [33]; these curves are necessarily invertible, but may not be commutative. However, only curves which are both additive and commutative can correspond to MUBs of monomial type [24]. Given an arbitrary Latin square, we provide a method of quickly determining if its associated curve is commutative.

We define a minisquare $\ell^{(f)}$, a subsquare of its parent $L^{(f)}$, with entries computed from only the self-dual basis elements

$$\ell_{ij}^{(f)} = \theta_j + f\left(c_i^{-1}\theta_i\right), \quad i, j = 1, \ldots, n. \tag{78}$$

Writing $\theta_j = \sigma^{p(j)}$ and $c_i^{-1}\theta_i = \sigma^{q(i)}$ for some functions p and q, we have

$$\begin{aligned}\ell_{ij}^{(f)} &= L_{q(i)p(j)}^{(f)},\\ \mathrm{Tr}\left(\ell_{ij}^{(f)}c_j^{-1}\theta_j\right) &= 1 + \Gamma_{ji}^{(f)}.\end{aligned} \tag{79}$$

The minisquares thus contain information about $\Gamma_{ji}^{(f)}$. In addition, $\ell^{(f)}$ corresponds to a commutative curve if

$$\mathrm{Tr}\left(\ell_{ij}c_j^{-1}\theta_j\right) = \mathrm{Tr}\left(\ell_{ji}c_i^{-1}\theta_i\right). \tag{80}$$

One example of application is provided in Appendix A.1. Here, we consider instead a situation where LS from a set associated to the Hall projective plane in dimension 9 do not have associated MUBs of the monomial type. This is a two-qutrit problem; since the (almost) self-dual basis is $\{\sigma^4, \sigma^2\}$ we find $p(1) = 4$, $p(2) = 2$, $q(1) = 8$ and $q(2) = 2$ since $c_1 = 2$.

We start with a LS obtained from the Hall plane, with associated curve $f = \sigma^5\alpha^3$

$$L^{(\sigma^5\alpha^3)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 3 & 5 & 0 & 2 & 1 & 6 & 4 \\ 3 & 4 & 1 & 7 & 2 & 6 & 8 & 0 & 5 \\ 6 & 3 & 0 & 8 & 7 & 4 & 2 & 5 & 1 \\ 1 & 5 & 8 & 4 & 6 & 0 & 3 & 2 & 7 \\ 4 & 6 & 5 & 2 & 8 & 3 & 7 & 1 & 0 \\ 7 & 2 & 4 & 0 & 1 & 8 & 5 & 3 & 6 \\ 2 & 8 & 6 & 1 & 5 & 7 & 0 & 4 & 3 \\ 5 & 0 & 7 & 6 & 3 & 1 & 4 & 8 & 2 \end{pmatrix}. \tag{81}$$

The elements of the minisquare are then

$$\ell^{(\sigma^5\alpha^3)} = \begin{pmatrix} L_{84} & L_{82} \\ L_{24} & L_{22} \end{pmatrix} \to \begin{pmatrix} \sigma^3 & \sigma^7 \\ \sigma^2 & \sigma \end{pmatrix} = \begin{pmatrix} 2\theta_1 + \theta_2 & \theta_1 + 2\theta_2 \\ \theta_2 & 2\theta_1 + 2\theta_2 \end{pmatrix}. \tag{82}$$

The curve associated with this LS is not commutative, since $\mathrm{Tr}\,(\ell_{ij}c_j^{-1}\theta_j) \neq \mathrm{Tr}\,(\ell_{ji}c_i^{-1}\theta_i)$ for $i \neq j$. The resulting adjacency matrix, though invertible as required, is not symmetric

$$\boldsymbol{\Gamma}^{(f)} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \tag{83}$$

and so cannot describe a commuting curve.

8. Conclusions

We have shown that, in dimension p^n, one can associate a complete sets of MUBs with a set of $p^n - 1$ of invertible curves, and thus with a complete set of MOLS (excluding two 'faux' squares obtained from degenerate curves). There exist subsets of unitary transformations acting on the MUBs that induce isomorphisms at the level of the corresponding MOLS. These transformations comprise CNOT-type transformations, and local transformations denoted type S and type F, applied uniformly to all the particles. This analysis has also allowed us to unravel the isomorphism permutations between the MOLS associated with the original and transformed MUBs.

In particular, we explicitly provide the mappings between MUBs of the monomial type described by invertible curves and their associated MOLS so that, given these restrictions, the following diagram holds

$$\begin{array}{ccc} MUBs & \Leftrightarrow & MOLS \\ \text{Unitary transformation} \Updownarrow & & \Updownarrow \text{Isomorphism permutation} \\ MUBs' & \Leftrightarrow & MOLS' \end{array}$$

We have also shown that local transformations preserving mappings from MUBs to MOLS form a group with multiplication given in equations (76), (77). The composition relation with CNOT given in equation (75) always preserves the mapping. This relation allows us to separate permutations of LS elements of a given set of MOLS related by local and non-local transformations, thus simplifying the classification of permutations that preserve the relations between MOLS and MUBs.

Arbitrary Latin squares do not necessarily correspond to MUBs, as is evident in the example of the Hall square of section 7. Latin minisquares serve as an excellent means of

verifying commutativity of a curve. Conversely, not every set of MUBs leads to a set of MOLS, but only those that contain $p^n - 1$ invertible curves. Furthermore, arbitrary permutations on Latin squares that do correspond to MUBs do not necessarily preserve them, unless they conform to the types of transformations listed above.

Acknowledgments

We thank Prof K Hicks for his help in numerically testing some of the hypotheses in the early stages of this work. ODM was funded in part by NSERC of Canada. Part of this work was done while visiting the Fields Institute in Toronto, and this visit was supported in part by the Julian Schwinger Foundation. The work of ABK is supported by the Grant 106525 of CONACyT (Mexico). HdG acknowledges support from NSERC. ABK and HdG also acknowledge partial support from the Fields Institute.

Appendix A. Two examples

A.1. MOLS and CNOT for three qubits

The irreducible polynomial is $\sigma^3 + \sigma^2 + 1 = 0$; $\boldsymbol{\theta} = \{\sigma, \sigma^2, \sigma^4\}$, $\mathbf{C} = \mathbb{1}$.

The expansions in the self-dual basis are

$$\begin{aligned} &\mathbf{s}^0 = (0,\,0,\,0) \quad \mathbf{s}^1 = (1,\,0,\,0) \quad \mathbf{s}^2 = (0,\,1,\,0) \quad \mathbf{s}^3 = (1,\,0,\,1) \\ &\mathbf{s}^4 = (0,\,0,\,1) \quad \mathbf{s}^5 = (0,\,1,\,1) \quad \mathbf{s}^6 = (1,\,1,\,0) \quad \mathbf{s}^7 = (1,\,1,\,1). \end{aligned} \tag{A.1}$$

We choose the ray $f(\alpha) = \alpha$ so $f =$ Id and $\boldsymbol{\Gamma}^{(\alpha)} = \mathbb{1}$. Using (22)

$$L^{(\alpha)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 6 & 4 & 3 & 7 & 2 & 5 \\ 2 & 6 & 0 & 7 & 5 & 4 & 1 & 3 \\ 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \\ 4 & 3 & 5 & 1 & 0 & 2 & 7 & 6 \\ 5 & 7 & 4 & 6 & 2 & 0 & 3 & 1 \\ 6 & 2 & 1 & 5 & 7 & 3 & 0 & 4 \\ 7 & 5 & 3 & 2 & 6 & 1 & 4 & 0 \end{pmatrix}. \tag{A.2}$$

This Latin square is symmetric, as is always the case for the curve $\beta = \alpha$. A Latin square with both the first row and first column in standard order is said to be *reduced* [1].

Suppose we perform CNOT on the first and second qubits, $\mathbf{X}^1_{1,2}$. By (35) and (33)

$$\mathbf{X}^1_{1,\,2} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \boldsymbol{\Gamma}^{(g)} = \left(\mathbf{X}^1_{1,2}\right)^T \boldsymbol{\Gamma}^{(\alpha)} \mathbf{X}^1_{1,\,2} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{A.3}$$

where $\boldsymbol{\Gamma}^{(\alpha)} = \mathbb{1}$, as noted before. The resulting square is

$$\tilde{L}^{(g)} = \begin{pmatrix} 0 & 1 & 6 & 3 & 4 & 7 & 2 & 5 \\ 6 & 2 & 0 & 5 & 7 & 4 & 1 & 3 \\ 2 & 6 & 1 & 7 & 5 & 3 & 0 & 4 \\ 7 & 5 & 4 & 2 & 6 & 0 & 3 & 1 \\ 4 & 3 & 7 & 1 & 0 & 6 & 5 & 2 \\ 5 & 7 & 3 & 6 & 2 & 1 & 4 & 0 \\ 1 & 0 & 2 & 4 & 3 & 5 & 6 & 7 \\ 3 & 4 & 5 & 0 & 1 & 2 & 7 & 6 \end{pmatrix}. \tag{A.4}$$

Using equation (37), we can permute this square into standard form. These equations produce $\mathbf{s}^2 \leftrightarrow \mathbf{s}^6$ and $\mathbf{s}^5 \leftrightarrow \mathbf{s}^7$, indicating that rows 2 and 6, and rows 5 and 7 need to be interchanged, and likewise for the columns. This yields

$$L^{(g)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 5 & 7 & 3 & 0 & 4 \\ 1 & 0 & 6 & 4 & 3 & 7 & 2 & 5 \\ 7 & 5 & 3 & 2 & 6 & 1 & 4 & 0 \\ 4 & 3 & 5 & 1 & 0 & 2 & 7 & 6 \\ 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \\ 2 & 6 & 0 & 7 & 5 & 4 & 1 & 3 \\ 5 & 7 & 4 & 6 & 2 & 0 & 3 & 1 \end{pmatrix}. \tag{A.5}$$

This standard form square can also be found directly using $\boldsymbol{\Gamma}^{(g)}$ in equations (A.3) and (22).

To bring $L^{(g)}$ to $L^{(\alpha)}$, use equation (42). Since $\mathbf{C} = \mathbb{1}$, the symbol permutation is obtained from

$$\left(s_1^i, s_2^i, s_3^i\right)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} \theta_1 \\ \theta_2 \\ \theta_3 \end{pmatrix} \to \sigma^i, \tag{A.6}$$

so that, choosing $i = 7$ for instance

$$(1,\ 1,\ 1)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} \sigma \\ \sigma^2 \\ \sigma^4 \end{pmatrix} = \sigma + \sigma^4 = \sigma^3 \to \sigma^7. \tag{A.7}$$

Proceeding systematically in this way we find the additional symbol permutations $1 \leftrightarrow 6$, $7 \leftrightarrow 3$ with all others unchanged. In the same manner, using again equation (42) it is found that the row transformations are simply $2 \leftrightarrow 6$ and $5 \leftrightarrow 7$; the column permutations are $1 \leftrightarrow 6$ and $3 \leftrightarrow 7$.

Alternatively, $\tilde{L}^{(g)}$ can be transformed back to $L^{(f)}$ of equation (A.2) in a single shot, using equations (39) as a starting point. No row permutation is necessary. The matrix

$$\mathbf{W} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{A.8}$$

induces the column permutations

$$1 \to 6 \to 2 \to 1 \qquad 3 \to 7 \to 5 \to 3. \tag{A.9}$$

Finally, $\mathbf{X}^1_{1,2}$ induces the same symbol transformation $1 \leftrightarrow 6$, $7 \leftrightarrow 3$ as before.

Table A1. Two sets of curves, each corresponding to a different set of MUBs with different separability properties. Application of the same sequence of permutations to the MOLS obtained using the f curves yields MOLS obtained using the g curves.

Initial curve	New curve
$f = \alpha$	$g = \sigma^6\alpha + \sigma\alpha^2 + \sigma^4\alpha^4$
$f = \sigma\alpha$	$g = \sigma\alpha$
$f = \sigma^2\alpha$	$g = \sigma^5\alpha + \sigma^3\alpha^2 + \sigma^5\alpha^4$
$f = \sigma^3\alpha$	$g = \sigma^3\alpha + \sigma^4\alpha^2 + \sigma^2\alpha^4$
$f = \sigma^4\alpha$	$g = \sigma^4\alpha + \sigma^4\alpha^2 + \sigma^2\alpha^4$
$f = \sigma^5\alpha$	$g = \sigma^2\alpha + \sigma\alpha^2 + \sigma^4\alpha^4$
$f = \sigma^6\alpha$	$g = \alpha + \sigma^3\alpha^2 + \sigma^5\alpha^4$

To illustrate the composition of curves of section 5.3, and the idea of orbits introduced in this section, we consider the adjacency matrix corresponding to $f(\alpha) = \sigma\alpha$

$$\boldsymbol{\Gamma}^{(f)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \tag{A.10}$$

so that, using equation (51) with $g = f$ leads to the cyclic permutation of columns

$$7 \to 6 \to 5 \to 4 \to 3 \to 2 \to 1 \to 7, \tag{A.11}$$

which is nothing but the permutation of columns needed to take the LS corresponding to $f \circ f(\alpha) = \sigma^2\alpha$ to back to $L^{(f)}$.

For completeness we provide in table A1 the complete set of Desarguesian curves transformed under $\mathbf{X}^1_{1,2}$. The first column shows the original curves whereas the second column show the transformed curve. The new curves are calculated according to a transformation known from [29], valid for qubit curves

$$g(\alpha) = f(\alpha) + \mathrm{Tr}\,(\alpha\theta_q) f(\theta_p) + \mathrm{Tr}\left[f(\alpha)\theta_p\right]\theta_q + \mathrm{Tr}\,(\alpha\theta_q)\,\mathrm{Tr}\left[f(\theta_p)\theta_p\right]\theta_q. \tag{A.12}$$

To obtain the minisquare for $f(\alpha) = \sigma\alpha$ we first recall that $\boldsymbol{\theta} = \{\sigma, \sigma^2, \sigma^4\}$. Since $\mathbf{C} = \mathbb{1}$, $p(i) = q(i)$ and we find

$$p(1) = q(1) = 1, \qquad p(2) = q(2) = 2, \qquad p(3) = q(3) = 4. \tag{A.13}$$

The minisquare then has entries which are those at the intersections of lines and columns 1, 2 and 4 of (A.2) (recall the indexing starts with 0)

$$\ell^{(\alpha)} = \begin{pmatrix} 0 & 6 & 3 \\ 6 & 0 & 5 \\ 3 & 5 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & \sigma^6 & \sigma^3 \\ \sigma^6 & 0 & \sigma^5 \\ \sigma^3 & \sigma^5 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \theta_1+\theta_2 & \theta_1+\theta_3 \\ \theta_1+\theta_2 & 0 & \theta_2+\theta_3 \\ \theta_1+\theta_3 & \theta_2+\theta_3 & 0 \end{pmatrix}. \tag{A.14}$$

The matrix with entries $\mathrm{Tr}\,(\ell_{ij}\theta_j)$ is symmetric and corresponds to $\Gamma^{(\alpha)}$ given by

$$\mathrm{Tr}\left(\ell_{ij}\theta_j\right) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad \Rightarrow \qquad \Gamma^{(\alpha)} = \mathbb{1}, \tag{A.15}$$

which, being symmetric, means f is indeed commutative.

Finally, we mentioned in section 6.1 that the CNOT changes the separability properties of MUBs. In this example, the eigenstates of MUB operators constructed from the linear functions f have separability structure (3, 0, 6), meaning 3 fully separable sets of states, 6 non-separable sets of states and one biseparable set of states. Eigenstates of the transformed operators constructed from the functions g have a different structure: (2, 3, 4) (2 separable, 3 biseparable and 4 non-separable) [25]. Both sets however, are Desarguesian, illustrating how the factorization structure is not reflected at the geometrical level.

A.2. Two qutrits and a local transformation

The irreducible polynomial is $\sigma^2 + \sigma + 2 = 0$; the almost self-dual basis $\boldsymbol{\theta} = \{\sigma^4, \sigma^2\}$ produces

$$\mathbf{C} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}. \tag{A.16}$$

Thus $\sigma^i = 2s_1^i\sigma^4 + s_2^i\sigma^2$. Explicitly, we have the vectors

$$\begin{aligned} &\mathbf{s}^0 = (0,\,0) \quad \mathbf{s}^1 = (1,\,2) \quad \mathbf{s}^2 = (0,\,1) \quad \mathbf{s}^3 = (1,\,1) \quad \mathbf{s}^4 = (2,\,0) \\ &\mathbf{s}^5 = (2,\,1) \quad \mathbf{s}^6 = (0,\,2) \quad \mathbf{s}^7 = (2,\,2) \quad \mathbf{s}^8 = (1,\,0). \end{aligned} \tag{A.17}$$

We choose the curve $\beta = \sigma^3\alpha$, which can be represented in parametric form (α, β) with $\alpha(\sigma^i) = \sigma^2\sigma^i$ and $\beta(\sigma^i) = \sigma^5\sigma^i$, so

$$\boldsymbol{\Gamma}^{(\alpha)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \boldsymbol{\Gamma}^{(\beta)} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}. \tag{A.18}$$

The points are not in standard order; the corresponding non-standard LS is given by

$$\tilde{L}_{ij}^{(\sigma^3\alpha)} = \left[\mathbf{s}^j\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \mathbf{s}^i\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\right]\boldsymbol{\theta}, \tag{A.19}$$

which upon evaluation, gives the full square

$$\tilde{L}^{(\sigma^3\alpha)} = \begin{pmatrix} 0 & 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \\ 6 & 8 & 7 & 4 & 2 & 5 & 1 & 3 & 0 \\ 7 & 0 & 1 & 8 & 5 & 3 & 6 & 2 & 4 \\ 8 & 5 & 0 & 2 & 1 & 6 & 4 & 7 & 3 \\ 1 & 4 & 6 & 0 & 3 & 2 & 7 & 5 & 8 \\ 2 & 1 & 5 & 7 & 0 & 4 & 3 & 8 & 6 \\ 3 & 7 & 2 & 6 & 8 & 0 & 5 & 4 & 1 \\ 4 & 2 & 8 & 3 & 7 & 1 & 0 & 6 & 5 \\ 5 & 6 & 3 & 1 & 4 & 8 & 2 & 0 & 7 \end{pmatrix}. \tag{A.20}$$

The maps given by (26) and (28) produce the following permutations

$$0 \to 0 \qquad 1 \to 3 \to 5 \to 7 \to 1 \qquad 2 \to 4 \to 6 \to 8 \to 2. \tag{A.21}$$

Applying these permutations to the rows and the columns of (A.20) will return this square to standard form.

Next, let us find the LS obtained after application of $\mathbf{X}_{1,2}^2$ to the commuting set defined by $f(\alpha) = \sigma^3\alpha$. Given

$$\mathbf{X}_{1,2}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{X}_{1,2}^{-2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{A.22}$$

we obtain

$$\boldsymbol{\Gamma}^{(g)} = \left(\mathbf{X}^2_{1,2}\right)^T \boldsymbol{\Gamma}^{(f)} \mathbf{X}^2_{1,2} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \tag{A.23}$$

which corresponds to the non-standard LS

$$\tilde{L}^{(g)} = \begin{pmatrix} 0 & 6 & 3 & 5 & 4 & 2 & 7 & 1 & 8 \\ 7 & 5 & 0 & 8 & 1 & 4 & 3 & 2 & 6 \\ 4 & 7 & 2 & 3 & 8 & 5 & 1 & 6 & 0 \\ 6 & 2 & 8 & 4 & 7 & 0 & 5 & 3 & 1 \\ 5 & 4 & 6 & 1 & 3 & 7 & 8 & 0 & 2 \\ 3 & 8 & 7 & 6 & 2 & 1 & 0 & 4 & 5 \\ 8 & 1 & 5 & 2 & 0 & 3 & 6 & 7 & 4 \\ 2 & 0 & 1 & 7 & 5 & 6 & 4 & 8 & 3 \\ 1 & 3 & 4 & 0 & 6 & 8 & 2 & 5 & 7 \end{pmatrix}. \tag{A.24}$$

The series of permutations that bring (A.24) back to the standard form of the untransformed square, $L^{(\sigma^3\alpha)}$, can be once again found using equation (39). There is no row transformation. The column transformation yields

$$1 \to 6 \to 4 \to 5 \to 2 \to 8 \to 1 \qquad 3 \to 7 \to 3. \tag{A.25}$$

We must also determine the symbol transformations. Unlike in the three qubit example, $c_1 = 2$ and $c_2 = 1$ so we must take into account the matrix $\mathbf{C}$ in our expansion $\sigma^i = s_1^i c_1^{-1}\theta_1 + s_2^i c_2^{-1}\theta_2$.

Finally, using equation (39) produces the equation

$$\sigma^i \to \left(s_1^i,\, s_2^i\right)\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} \tag{A.26}$$

which leads to the symbol permutations

$$\sigma^1 \to \sigma^3 \to \sigma^8 \to \sigma^1 \qquad \sigma^4 \to \sigma^5 \to \sigma^7 \to \sigma^4 \tag{A.27}$$

meaning we must perform the symbol swaps $1 \to 3 \to 8 \to 1$ and $4 \to 5 \to 7 \to 4$.

For a single qutrit, there are eight generalized Paulis: $\mathcal{Z}$, $\mathcal{X}$, $\mathcal{Z}\mathcal{X}$, $\mathcal{Z}^2\mathcal{X}$, and their squares. Under the local transformation

$$\mathbf{U}_1^{\mathrm{S}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{A.28}$$

they are mapped (up to a phase) to

$$\mathcal{Z} \leftrightarrow \mathcal{Z}^2, \quad \mathcal{X} \leftrightarrow \mathcal{X}^2, \quad \mathcal{Z}\mathcal{X} \leftrightarrow (\mathcal{Z}\mathcal{X})^2, \quad (\mathcal{Z}^2\mathcal{X}) \leftrightarrow (\mathcal{Z}^2\mathcal{X})^2. \tag{A.29}$$

Choose the generating set $G = \{2\sigma^4, \sigma^2\} = \{\sigma^8, \sigma^2\}$, and the curve $f(\alpha) = \sigma^4\alpha$. Then

$$\mathbf{A}^{(\sigma^4\alpha)} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{array}\right). \tag{A.30}$$

The monomials corresponding to each generator are

Generator	Monomial	Pauli representation
$g_1 = \sigma^8$	$Z_{\sigma^8} X_{\sigma^4}$	$\mathcal{Z}\mathcal{X} \otimes \mathbb{1}$
$g_2 = \sigma^2$	$Z_{\sigma^2} X_{\sigma^6}$	$\mathbb{1} \otimes (\mathcal{Z}\mathcal{X}^2)$

The transformation $\mathbf{U}_1^S$ corresponds to the 2×2 map

$$T\left(\mathbf{U}_1^S\right) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \tag{A.31}$$

shuffling the powers a_1, b_1 in the initial monomials. Now, $\mathbf{U} = \mathbf{U}_1^S \otimes \mathbb{1}$. Given $T(\mathbb{1}) = \mathbb{1}$, we readily obtain $\mathbf{K}_s$

$$\begin{aligned} \mathbf{K}_{11} &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{K}_{12} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \\ \mathbf{K}_{21} &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{K}_{22} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned} \tag{A.32}$$

so that

$$\tilde{\mathbf{A}}^{(f')} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{array}\right) \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \left(\begin{array}{cc|cc} 2 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{array}\right) \tag{A.33}$$

It follows from equation (A.29) that the new generating elements are

Pauli representation	Monomial	Generator
$(\mathcal{Z}\mathcal{X})^2 \otimes \mathbb{1}$	$Z_{\sigma^4} X_{\sigma^8}$	$g_1' = \sigma^4$
$\mathbb{1} \otimes (\mathcal{Z}\mathcal{X}^2)$	$Z_{\sigma^2} X_{\sigma^6}$	$g_2' = \sigma^2$

Using equations (23) and (48), we can transform this to the standard form $(\mathbb{1} \mid \boldsymbol{\Gamma}^{(f')})$

$$\mathbf{A}^{(f')} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{array}\right), \tag{A.34}$$

and we can see that the resultant curve is both invertible and commutative, as the adjacency matrix is symmetric and $\det[\boldsymbol{\Gamma}^{(f')}] \neq 0$. In this case, it just so happens that the curve is not changed under transformation; this is not always the case.

References

[1] Laywine C F and Mullen G L 1998 *Discrete Mathematics using Latin Squares* (New York: Wiley)
[2] Denes J and Keedwell A D 1974 *Latin Squares and their Applications* (New York: Academic)
Denes J and Keedwell A D 1991 *Latin Squares: New Developments in the Theory and Applications* (Amsterdam: Elsevier)
[3] Wocjan P and Beth T 2005 *Quantum Inf. Comput.* **5** 93–101
[4] Klappenecker A and Röttler M 2004 *Finite Fields and its Applications* (Berlin: Springer) pp 137–44
[5] Wootters W K 2006 *Found. Phys.* **36** 112–26
[6] Zauner G 2011 *Int. J. Quantum Inf.* **9** 445–507
[7] Paterek T *et al* 2010 *Phys. Scr.* **T140** 014031
[8] Rao A, Donovan D and Hall J L 2010 *Cryptogr. Commun.* **2** 221–31

[9] Hall J L and Rao A 2010 *J. Phys. A: Math. Theor.* **43** 135302
[10] Paterek T, Dakić B and Brukner Č 2009 *Phys. Rev.* A **79** 012109
[11] Ghiu I and Ghiu C 2014 *Rep. Math. Phys.* **73** 49
Ghiu I 2013 *Phys. Scr.* **T153** 014027
[12] Fischer R A 1960 *The Design of Experiments* 7th edn (New York: Hafner Publishing)
[13] Herman M A and Strohmer T 2009 *IEEE Trans. Signal Process.* **57** 2275–84
[14] Gross D *et al* 2010 *Phys. Rev. Lett.* **105** 150401
Flammia S *et al* 2012 *New J. Phys.* **14** 095022
[15] Colbourn C J, Klove T and Ling A C 2004 *IEEE Trans. Inf. Theor.* **50** 1289–91
Huczynska S 2006 *Phil. Trans. R. Soc.* A **364** 3199–214
[16] Wootters W K and Fields B D 1989 *Ann. Phys., NY* **191** 363
[17] Dürt T, Englert B-G, Bengtsson I and Zyczkowski K 2010 *Int. J. Quantum Inf.* **8** 535–640
[18] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan V 2002 *Algorithmica* **34** 512
Pittenger A O and Rubin M H 2005 *J. Phys. A: Math. Gen.* **38** 6005
[19] Lawrence J 2011 *Phys. Rev.* A **84** 022338
[20] Klimov A B, Sánchez-Soto L L and De Guise H 2005 *J. Phys. A: Math. Gen.* **38** 2747
[21] Calderbank A R, Cameron P J, Kantor W M and Seidel J J 1997 *Proc. London Math. Soc.* **75** 436–80
[22] Kantor W M 2003 *J. Algebra* **270** 96–114
Kantor W M 2012 *J. Math. Phys.* **53** 032204
[23] Roy A and Scott A J 2007 *J. Math. Phys.* **48** 072110
Godsil C and Roy A 2009 *Eur. J. Comb.* **30** 246–62
Schmidt K-U and Zhou Y 2014 *J. Algebra Comb.* **40** 503–26
[24] Klimov A B, Romero J L, Björk G and Sánchez-Soto L L 2009 *Ann. Phys., NY* **324** 53–72
[25] Romero J L, Björk G, Klimov A B and Sánchez-Soto L L 2005 *Phys. Rev.* A **72** 062310
[26] Gibbons K S, Hoffman M J and Wootters W K 2004 *Phys. Rev.* A **70** 062101
[27] Vourdas A 2007 *J. Phys.* A **40** R285–331(R)
[28] Lidl R and Niederreiter H 1986 *Introduction to Finite Fields and their Applications Cambridge* (Cambridge: Cambridge University Press)
[29] Klimov A B, Muñoz C and Sánchez-Soto L L 2012 *J. Phys. A: Math. Theor.* **45** 215303
[30] Barenco A *et al* 1995 *Phys. Rev.* **A52** 3457
[31] Bahramgiri M and Beigi S 2007 arXiv:0610267v2 [quant-ph]
[32] Garcia A, Romero J L and Klimov A B 2010 *J. Phys. A: Math. Theor.* **43** 385301
[33] Wan D, Mullen G L and Shiue P J-S 1995 *Proc. Edinburgh Math. Soc.* **38** 133