Private quantum subsystems and quasiorthogonal operator algebras

Jeremy Levick\textsuperscript{1,2}, Tomas Joachym-O’Connor\textsuperscript{3}, David W Kribs\textsuperscript{1,3}, Raymond Laflamme\textsuperscript{3,4,5} and Rajesh Pereira\textsuperscript{1}

\textsuperscript{1}Department of Mathematics & Statistics, University of Guelph, Guelph, ON N1G 2W1, Canada
\textsuperscript{2}African Institute for Mathematical Sciences, Muizenberg, Cape Town, 7945, South Africa
\textsuperscript{3}Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada
\textsuperscript{4}Perimeter Institute for Theoretical Physics, Waterloo, ON N2L 2Y5, Canada
\textsuperscript{5}Canadian Institute for Advanced Research, Toronto, ON M5G 1Z8, Canada

Received 28 September 2015, revised 23 December 2015
Accepted for publication 8 January 2016
Published 9 February 2016

Abstract
We generalize a recently discovered example of a private quantum subsystem to find private subsystems for Abelian subgroups of the $n$-qubit Pauli group, which exist in the absence of private subspaces. In doing so, we also connect these quantum privacy investigations with the theory of quasiorthogonal operator algebras through the use of tools from group theory and operator theory.

Keywords: private quantum subsystem, private quantum channel, completely positive map, quasiorthogonal operator algebras, conditional expectations, $n$-qubit Pauli group

1. Introduction

A key goal of quantum information theory is to understand how concepts from classical information translate into the quantum setting. For example, in classical information theory, one finds the idea of the \textit{one-time pad}, a system that can be used to encode information sent through a channel, so long as the two parties share a private key between them. The generalization of this scheme to the quantum setting was established in \cite{1,6}; such a scheme was further generalized to what was initially called private quantum channels and now referred to as \textit{private quantum subsystems}. Developing a characterization of the special features of particular forms of completely positive maps is central to the study.
Subsequent developments on the subject over the past 15 years have included advances in the theory of private shared reference frames [4, 5], applications to quantum secret sharing [9, 10], bridges established with quantum error correction [15], and a first indication of connections with the theory of operator algebras [8]. More recently, a significant step was made toward a general theory for private quantum subsystems in [13, 14], including algebraic conditions that characterize such quantum privacy. In addition, that work included the first example of a private subsystem for a quantum channel that exists in the absence of any subspace that is privatized by the channel. The example in question was a simple two-qubit dephasing channel, and it was initially surprising to discover the underlying structure of a private subsystem for the channel.

This article began with an effort to generalize the example from [13, 14] more widely; in particular to obtain a large class of simple and easily implemented $n$-qubit quantum channels, which as a consequence of their simplicity would not privatize any subspace, but that nevertheless do privatize quantum information through more delicate subsystem encodings. In addition to building on previous work, one could imagine such a class of channels and encodings as being useful in quantum computing when deleting information swiftly is a desired outcome. As an outgrowth of our example-based effort, we also uncover an advance in the general theory of private quantum subsystems. Specifically, we show how finite-dimensional private quantum subsystems can be cast in the framework of quasiorthogonal operator algebras, which have been studied in quantum information for their intrinsic interest [18, 19, 22, 25] and specific connection with identifying maximal collections of mutually unbiased bases [3, 7, 23]. Combining the quasiorthogonal perspective with conditional expectation tools from operator algebra [21] and a group-theoretic analysis [24], we then show how quantum channels defined by operators forming an Abelian subgroup of the Pauli group can privatize quantum information encoded into subsystems of $n$-qubit Hilbert space, even though they can never privatize qubits directly encoded into subspaces of the Hilbert space. This gives a full picture of privatizing quantum information for such subgroups.

This paper is organized as follows. In the next section we present preliminary material on private quantum subsystems. This is followed by a discussion on quasiorthogonal operator algebras and conditional expectations, and we indicate how private subsystems fit into the framework. In the next section we turn our attention to the structure of Abelian subgroups of the Pauli group. We conclude by explicitly showing how such subgroups can be used to privatize quantum information.

2. Private quantum subsystems and subspaces

The motivating communication scenario for a private quantum code starts with two parties, Alice and Bob, who share a private classical key that Alice uses to inform Bob which of a set of unitary operators $\{U_i\}$ she has used to encode her quantum state (density operator) $\rho \mapsto U_i \rho U_i^\dagger$. Bob can then decode and recover the state $\rho$ without disturbing it. The set of unitaries $\{U_i\}$ and the probability distribution $\{p_i\}$ that makes up the random key which determines the encoding unitary are shared publicly. Hence an eavesdropper Eve’s description of the system is given by the random unitary channel $\Phi(\rho) = \sum_i p_i U_i \rho U_i^\dagger$. By carefully selecting the unitary operators and probabilities, the random unitary channel will provide Eve with no information about the input state. Notice that this generalizes the classical one-time pad, as Alice and Bob share a private key $k$, which determines the unitary $U_k$ that will be applied to $\rho$. With access to the private key, $\rho$ is easily recoverable, but from the perspective
of an eavesdropper without access to the key, the output of the channel contains no information about ρ.

More generally, quantum channels are given by completely positive trace-preserving maps Φ : M_n(ℂ) → M_n(ℂ), and motivated by the example above, one looks for sets S of density operators ρ that are mapped by Φ to the same state, Φ(ρ) = ρ_0 for all ρ ∈ S. Notice that in general, one might not be able to invert the action of the channel, even with extra private information. This more general version of the motivating example above is what we refer to as a private quantum channel. One may wish to impose conditions on the channel to ensure that with extra private information, the action of the channel can be reversed, preserving the analogy with the one-time pad; and indeed, all our examples below will be random unitary channels, which satisfy this condition (see appendix A). However, we will not impose this requirement in the definition of a private quantum channel.

Analogous to quantum error correction, we focus on sets of states that are associated with underlying Hilbert space structure and hence form a true quantum code in the sense that superpositions of privatized states are also private. We define a qubit to be a two-dimensional subspace of ℂ^n whose observables are given by the Pauli matrices in that fixed subspace

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\]

Thus the most basic choice for a set of private states is for S to be the set of density matrices whose non-zero action is entirely on a k-qubit, 2^k-dimensional subspace of the Hilbert space ℂ^n; i.e., there exists a subspace C such that the operators in S, when written in any basis containing C, has the block form

\[
\rho = \begin{pmatrix} \rho_C & 0 \\ 0 & 0 \end{pmatrix}.
\]

As a convenience we shall identify the full set of such operators with the set of operators \mathcal{L}(C) that act on C, which in this case is isomorphic to \mathcal{L}(ℂ^{2k}) and thus Φ privatizes k qubits of information. Two of the simplest examples in the single qubit case are given by the completely depolarizing channel, which satisfies Φ(ρ) = \frac{1}{4}I and I is the identity operator, and the spontaneous emission channel, which satisfies Φ(ρ) = |0⟩⟨0| for all single qubit ρ [17]. The complete depolarizing channel in particular is the random unitary channel implemented by the equally weighted Pauli operators I, X, Y, Z.

However, not all quantum channels admit a private subspace. In particular, as proved in [13, 14], any quantum channel Φ(ρ) = \sum_i A_i ρ A_i^* whose (normal) Kraus operators A_i are mutually commuting, cannot privatize a (multi-dimensional) subspace. Nevertheless, even in such instances it can still be possible to privatize quantum information. The following phase flip example was presented and discussed in detail in [13, 14]: let Φ : \mathcal{L}(ℂ^2 ⊗ ℂ^2) → \mathcal{L}(ℂ^2 ⊗ ℂ^2) be the completely positive map on two-qubit space whose Kraus operators are \{\frac{1}{2}I, \frac{1}{2}ZI, \frac{1}{2}IZ, \frac{1}{2}ZZ\}, where we have suppressed tensor symbols so that ZI is Z ⊗ I, etc. These operators are all diagonal in the computational basis \{|00⟩, |01⟩, |10⟩, |11⟩\}, and form an orthonormal basis for the diagonal subalgebra of M_4(ℂ) in the normalized trace (Hilbert–Schmidt) inner product. In particular they are mutually commuting and so the channel Φ has no private subspaces. However, the subalgebra spanned by I, IX, YY, YZ is privatized by Φ, and moreover, is isomorphic to the Pauli algebra on one qubit; thus the channel still privatizes a qubit:
This example relies on the more subtle notion of a quantum subsystem to privatize a qubit. A space \( A \) (or \( B \)) is a subsystem of a Hilbert space \( \mathcal{H} \) if there is a subspace \( \mathcal{C} \) of \( \mathcal{H} \) such that \( \mathcal{C} \) admits a tensor decomposition as \( \mathcal{C} = A \otimes B \).

**Definition 1.** Let \( \Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}) \) be a channel and let \( B \) be a subsystem of \( \mathcal{H} \). Then \( B \) is a private subsystem for \( \Phi \) if there is a \( \rho_0 \in \mathcal{L}(\mathcal{H}) \) and \( \sigma_A \in \mathcal{L}(A) \) such that
\[
\Phi(\sigma_A \otimes \sigma_B) = \rho_0 \quad \forall \sigma_B \in \mathcal{L}(B).
\]

As shown in [13, 14], the above example channel privatizes a qubit subsystem in the sense of equation (1), yet does not privatize a subspace. Moreover, the mapping is ‘non-operator’ in the language of [13, 14] in the sense that equation (1) holds for a particular state \( \sigma_A \in \mathcal{L}(A) \) but not for every state on \( A \). We seek to understand this example and generalize it, and we shall make use of conditional expectations and quasiorthogonality of two subalgebras, notions to which we now turn.

3. Quasiorthogonal subalgebras and conditional expectations

We begin this section by reviewing basic notions from operator algebras and then we indicate how private subsystems can be cast in the quasiorthogonal subalgebra framework and discuss examples.

A unital \( * \)-algebra of the \( N \times N \) complex matrices \( M_N(\mathbb{C}) \) is a subset \( \mathcal{A} \subseteq M_N(\mathbb{C}) \) that is closed under matrix addition, scalar multiplication, multiplication, and taking adjoints, and includes the identity matrix \( I_N \), which we denote by \( I \) when the dimension is clear. It follows from the representation theory of finite-dimensional \( \mathbb{C}^* \)-algebras [11], that any unital \( * \)-subalgebra \( \mathcal{A} \) of \( M_N(\mathbb{C}) \) is unitarily equivalent to an algebra of the form
\[
\bigoplus_{i=1}^m I_{k_i} \otimes M_{q_i}(\mathbb{C}),
\]
where \( \sum_i k_i q_i = N \).

**Definition 2.** Let \( \mathcal{A} \) be a unital \( * \)-subalgebra of \( M_N(\mathbb{C}) \). Then \( \Phi_{\mathcal{A}} : M_N(\mathbb{C}) \to M_N(\mathbb{C}) \) is called the trace-preserving conditional expectation onto \( \mathcal{A} \) when it is the unique completely positive trace-preserving map satisfying

1. \( \Phi_{\mathcal{A}}(a) = a \quad \forall a \in \mathcal{A} \),
2. \( \Phi_{\mathcal{A}}(a_1 a_2) = a_1 \Phi_{\mathcal{A}}(x) a_2 \quad \forall a_1, a_2 \in \mathcal{A}, \quad \forall x \in M_N(\mathbb{C}) \),
3. \( \Phi_{\mathcal{A}}(x) \geq 0 \quad \forall x \geq 0 \).

The trace-preserving conditional expectation onto a unital \( * \)-sub-algebra is unique as a linear map, and is always a completely positive map. Any unital \( * \)-subalgebra induces an inner product, the left-regular trace inner product, which is the Hilbert–Schmidt inner product in the induced left-regular trace given by the subalgebra \( \mathcal{A} \). More explicitly, let \( a \in \mathcal{A} \) and consider the left-regular representation of \( a \), \( L_a(x) = ax \) for \( x \in M_N(\mathbb{C}) \). The left-regular trace of \( a \) is the trace of the operator \( L_a \); \( \text{tr}_\mathcal{A}(a) = \text{tr}(L_a) \). This gives the left-regular trace inner product as \( \langle a, b \rangle_\mathcal{A} = \text{tr}_\mathcal{A}(a^* b) \).
Denote by \( \mathcal{A}^\prime \) the commutant of \( \mathcal{A} \): \( \mathcal{A}^\prime = \{ x \in M_N(\mathbb{C}) : xa = ax \ \forall a \in \mathcal{A} \} \). Importantly, the Kraus operators for \( \Phi_{\mathcal{A}} \) must be an orthonormal basis for \( \mathcal{A}^\prime \) in the left-regular inner product induced by \( \mathcal{A} \). In addition, recall that two different choices of Kraus operators must be related by a partial isometry conjugation. For more on conditional expectations onto matrix algebras, including for proofs and further references, see [21].

For the phase flip example discussed in the previous section, the map \( \Phi = \Phi_{\Delta_4} \) is the trace-preserving conditional expectation onto the \( 4 \times 4 \) diagonal subalgebra, \( \Delta_4 = \{ \sum_{i,j=0}^{3} a_{ij} |ij\rangle \langle ij| : a_{ij} \in \mathbb{C} \} \cong \mathbb{C} \otimes \mathbb{C} \otimes \mathbb{C} \otimes \mathbb{C} \). Since \( \Delta_4^\prime = \Delta_4 \), the Kraus operators for \( \Phi \) should be a basis for the diagonal matrices, and indeed they are.

From a geometric perspective, quasiorthogonal algebras arise through a natural broadening of the notion of orthogonality for algebras; namely, unital algebras \( \mathcal{A}, \mathcal{B} \) satisfy quasiorthogonality if \( \text{tr}(ab) = 0 \) whenever \( \text{tr}(a) = \text{tr}(b) = 0 \) and \( a \in \mathcal{A}, b \in \mathcal{B} \). The algebras are not orthogonal themselves as they both contain the identity operator, however the sets \( \mathcal{A} \otimes \mathcal{Cl} \) and \( \mathcal{B} \otimes \mathcal{Cl} \) are orthogonal in the Hilbert–Schmidt inner product \( \langle a, b \rangle = \text{tr}(b^\dagger a) \). We state equivalent forms of this definition in our current notation.

**Definition 3.** Two unital subalgebras \( \mathcal{A}, \mathcal{B} \subseteq M_N(\mathbb{C}) \) are said to be quasiorthogonal if any of the following equivalent conditions hold:

1. \( \text{tr} \left( \left( a - \frac{\text{tr}(a) I}{N} \right) \left( b - \frac{\text{tr}(b) I}{N} \right) \right) = 0 \ \forall a \in \mathcal{A}, \forall b \in \mathcal{B} \),
2. \( \frac{1}{N} \text{tr}(ab) = \frac{1}{N} \text{tr}(a) \frac{1}{N} \text{tr}(b) \ \forall a \in \mathcal{A}, \forall b \in \mathcal{B} \),
3. \( \Phi_{\mathcal{A}}(b) = \frac{\text{tr}(b) I}{N} \) and \( \Phi_{\mathcal{B}}(a) = \frac{\text{tr}(a) I}{N} \ \forall a \in \mathcal{A}, \forall b \in \mathcal{B} \),
4. \( \Phi_{\mathcal{A}} \circ \Phi_{\mathcal{B}}(\rho) = \Phi_{\mathcal{B}} \circ \Phi_{\mathcal{A}}(\rho) = \rho \frac{\text{tr}(\rho) I}{N} \) for all \( \rho \).

In particular, condition (3) says that the trace-preserving conditional expectation onto \( \mathcal{A} \) privatizes an element of \( \mathcal{B} \) (and vice-versa) precisely when the two subalgebras are quasiorthogonal to each other.

In the extremal case with \( \mathcal{A} = M_N(\mathbb{C}) \) and \( \mathcal{B} = \mathcal{Cl} = \mathcal{A}^\prime \), \( \Phi_{\mathcal{Cl}} \) is the complete depolarizing channel with Kraus operators given by a complete orthonormal set (in the Hilbert–Schmidt inner product) of operators, and \( \Phi_{\mathcal{Cl}}(a) = \frac{\text{tr}(a) I}{N} \) for all \( a \in \mathcal{A} \). As a simple subsystem example, consider the first qubit algebra \( \mathcal{A} \) in two-qubit space generated by \( \{ II, XI, YI, ZI \} \). The commutant \( \mathcal{A}^\prime = I_2 \otimes M_2(\mathbb{C}) \) is generated by the orthonormal set \( \{ II, IX, IY, IZ \} \), which also act as Kraus operators (after normalizing) for the map \( \Phi_{\mathcal{A}} \). Thus, \( \mathcal{A} \) and \( \mathcal{A}^\prime \) form a quasiorthogonal pair and in particular the second qubit is a private subsystem for the channel \( \Phi_{\mathcal{A}} \). Not all quasiorthogonal algebra pairs arise through the commutant in this way though; indeed, as an example note that the phase flip example above is determined by the algebra pairing \( \mathcal{A} = \Delta_4 \) and \( \mathcal{B} \) generated by \( \{ II, IX, YY, YZ \} \), which is unitarily equivalent to \( I_2 \otimes M_2(\mathbb{C}) \).

This behavior is not unique to qubit systems and can be generalized to multi-dimensional systems. The following example exhibits the behavior of privatized subalgebras for elementary systems composed of qutrits, we leave its proof for appendix \( B \).

**Example 1.** Let \( X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \) and \( Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \omega = e^{2\pi i/3} \), be the generalized Pauli operators for qutrits. Consider the channel on two qutrits given by
The Kraus operators for this channel are Abelian, and thus do not admit a private subspace. However, one may check that the subalgebra \( \mathcal{A} \) generated by \( X^2 \otimes X, XZ^2 \otimes Z \) is privatized by \( \Phi \), and moreover that \( \mathcal{A} \) is isomorphic as an algebra to the one-qutrit subalgebra generated by \( I \otimes X, I \otimes Z \).

As a next-step generalization of our motivating phase flip example, for the rest of the paper we consider conditional expectations onto algebras generated by Abelian subgroups of the \( n \)-qubit Pauli group. The subalgebras generated in this way will be Abelian, so by choosing a maximal Abelian subgroup of the \( n \)-qubit Pauli group that contains the initial subgroup, we obtain a maximal Abelian subalgebra generated by Pauli operators. The commutant of such an algebra will be itself, and so the Kraus operators for the trace-preserving conditional expectation will simply be the elements of the Abelian group, suitably weighted. Thus, having mutually commuting Kraus operators, there can be no private subspace for such a channel. However, if the Abelian subalgebra has a quasiorthogonal partner with a non-scalar component as in equation (2), the channel will still have a private sub-system. This motivates us to learn more about the structure of maximal Abelian subgroups of the \( n \)-qubit Pauli group, \( \mathcal{P}_n \), a topic to which we now turn.

4. Commutation relations of the pauli group

Given \( n \geq 1 \), let \( \mathcal{P}_n \) be the \( n \)-qubit Pauli group, which is the unitary subgroup of \( M_{2^n}(\mathbb{C}) \) generated by all \( n \)-fold tensor products of the Pauli matrices \( X, Y, Z \).

Note that the group-theoretic commutator \([\sigma, \tau] = \sigma \tau \sigma^{-1} \tau^{-1}\) (as opposed to the more typically considered Lie algebra commutator) of any two \( n \)-qubit Pauli matrices is equal to \( \pm I \). Also, \([\sigma, \tau] = [c_1 \sigma, c_2 \tau]\) for \( \sigma, \tau \in \mathcal{P}_n \) and \( c_1, c_2 \in \{ \pm 1, \pm i \} \). Hence, the function \( \chi : \mathcal{P}_n \times \mathcal{P}_n \rightarrow \mathbb{C} \) defined by \( \chi([\sigma], [\tau]) = [\sigma, \tau] \) is well-defined on the central quotient \( \mathcal{P}_n / [\pm I, \pm i] \). Notice that \( \mathcal{P}_1 \) is isomorphic to the Klein four-group \( V = \{ e, v_1, v_2, v_3 \} \) where \( e \) is the identity element, each \( v_i \) is its own inverse, and \( v_i v_j = v_k \). Similarly, \( \mathcal{P}_n \cong V^n \), where \( V^n \) is the (Abelian) direct product of \( n \) copies of the Klein four-group with itself.

We recall that a bicharacter on a group \( G \) is a function \( B(\cdot, \cdot) : G \times G \rightarrow \mathbb{C} \) satisfying the following:

1. \( B(e, g) = B(g, e) = 1 \) for all \( g \in G \),
2. \( B(g, hk) = B(g, h)B(k, g) \) and \( B(hk, g) = B(h, g)B(k, g) \) for all \( g, h, k \in G \).

Moreover, a bicharacter is non-degenerate if for all non-identity \( g \in G \) there exists some element \( h \in G \) such that \( B(g, h) \neq 1 \).

Notice that a bicharacter, when restricted in either argument to a fixed \( g \in G \) becomes a character on \( G \).

**Proposition 1.** The function \( \chi(\cdot, \cdot) \) defined above is a non-degenerate bicharacter on \( \mathcal{P}_n \).

**Proof.** Firstly, \( \chi([I], [\sigma]) = [I, \sigma] = I \), hence \( \chi([I], [\sigma]) = 1 \) and similarly \( \chi([\sigma], [I]) = 1 \). To prove the second condition holds, note that \( \sigma \rho = \chi([\sigma], [\rho]) \rho \sigma \) and \( \tau \rho = \chi([\tau], [\rho]) \tau \sigma \). Hence
\[ \sigma \tau \rho = \chi ([\sigma], [\rho]) \rho (\sigma \tau) \]
\[ = \chi ([\tau], [\rho]) \sigma \rho \tau \]
\[ = \chi ([\tau], [\rho]) \chi ([\sigma], [\rho]) \rho \sigma \tau \]
and the other identity is similarly proved. The claim that \( \chi (\cdot, \cdot) \) is non-degenerate is equivalent to the claim that for any non-identity \([\sigma] \in P_n\), there is some \([\tau] \in P_n\) that anti-commutes with \([\sigma]\), which is easily seen to be the case.

Consider the character matrix for \( P_1 \) given by
\[
H = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix},
\]
where the columns and rows index the Pauli matrices and the entries of \( H \) record whether elements of the Pauli basis commute or anti-commute. Then \( H \) is the so-called bicharacter matrix of \( \cdot, \cdot \) on \( P_1 \); this is \( H_{\sigma \tau} = \chi ([\sigma], [\tau]) \). Moreover, since the restriction of \( \chi ([\sigma], [\tau]) \) to any particular \( \sigma \) yields a character of the Abelian group \( P_1 \), \( H \) is a character matrix.

As noted above, the group \( P_1 \) is isomorphic to the Klein four-group, \( V = \{e, x, y, z\} \), an Abelian group defined by the relations \( x^2 = y^2 = z^2 = e \) and \( xy = z, xz = y, yz = x \). Thus, \( P_n \) is isomorphic to \( V^n \), the direct product of \( V \) with itself \( n \) times, and \( H_n \), a character matrix for the Abelian group \( P_n \), and records the commutation relations between basis elements for the \( n \)-qubit Pauli group. Lastly, we point out that a maximal Abelian subgroup of \( P_n \) corresponds to a maximal submatrix of \( H_n \) containing all 1s.

We recall another notion from group theory to continue. Let \( G \) be a group with dual group \( \hat{G} \) and \( K \) a subgroup of \( G \). Then the annihilator of \( K \) in \( G \), \( \text{Ann}_G(K) \) is the set of characters \( \hat{\chi} \in \hat{G} \) satisfying \( \hat{\chi}(k) = 1 \) for all \( k \in K \). The following is a well-known fact about the annihilator subgroup [24].

**Lemma 1.** Let \( G, K, \hat{G} \) be as above; then \( \text{Ann}_G(K) \) is isomorphically homeomorphic to the dual group of \( G/K \).

In particular, this implies that when \( G \) is finite and Abelian, that \( |\text{Ann}_G(K)| = |G/K| = |G|/|K| \). The following is a direct consequence of this statement.

**Corollary 1.** Let \( G = P_n \) and \( K \) be any subgroup of \( P_n \). Let \( I \) be column indices of \( H_n^{\otimes n} \) associated to the elements of \( K \). Let \( J = \chi^{-1}(\text{Ann}_G(K)) \) be the row indices associated to the annihilator of \( K \). Then we have \( |I||J| = 4^n \).

**Corollary 2.** Let \( K \) be an Abelian subgroup of \( P_n \) with \( |K| = 2^k < 2^n \). Then \( K \) can be extended to an Abelian subgroup of size \( 2^n \).

**Proof.** We will show that so long as \( k < n \), there exists a \( g \in P_n \setminus K \) such that \( g \) commutes with every element of \( K \); and so that \( <K, g> \), the group spanned by \( K \) and \( g \), must be Abelian. We use the previous corollary as follows: let \( I \) be the indices associated to the elements of \( K \); since \( K \) is Abelian the submatrix \( H_n[I] \) is an all 1 submatrix. Thus, by the previous result, there exist \( 4^n|I|^{-1} = 4^{n-2-k} \) rows whose intersection with each column in \( I \) contains only 1s. As \( k < n \), we have \( 2^k < \frac{4^n}{2^n} \) and so there is at least one row not already in \( I \) with this property. Call this row \( i \). By the symmetry of \( H_n \), the intersection of column \( i \) with
the rows of \( I \) is all 1s, and \( H_{\text{nn}=1} \), and so the submatrix indexed by \( I \cup \{i\} \) is an all one submatrix. Let \( g \) be the element of \( P_n \) associated with the \( i \)th column; then \( g \in P_n \) is an element of \( P_n \setminus K \) that commutes with every element of \( K \). Hence \( \langle K, g \rangle \) is an Abelian group of size at least \( 2^{k+1} \).

We can iterate the procedure until \( \frac{d^i}{2^i} = 2^k \), or \( k = n \).

We are now ready to prove the following theorem which will be useful in constructing examples that generalize our motivating phase flip example.

**Theorem 1.** Any maximal Abelian subalgebra \( \mathcal{A} \) of \( M_{2^n}(\mathbb{C}) \) generated by elements of \( P_n \) has dimension \( 2^n \).

**Proof.** To begin, we note that if \( \sigma \in P_n \) is an element of \( \mathcal{A} \), then so are \( -\sigma, \pm i\sigma \), and hence independent generators of \( \mathcal{A} \) must all come from different conjugacy classes. Thus, we may regard our generators as coming from \( P_n \), rather than \( P_n \). It follows that a generating set for a maximal Abelian subalgebra is simply a maximal Abelian subgroup \( K \subseteq P_n \), which by the previous corollary has size \( 2^n \). Since such a subgroup is already closed under matrix multiplication, it follows that \( \dim \langle K \rangle = 2^n \).

**Corollary 3.** Any subalgebra \( \mathcal{A} \) contained in the span of elements from \( P_n \) has the property that \( |\mathcal{A}| \cdot |\mathcal{A}| = 4^n \).

Now we may turn our attention to the private structure of quantum channels whose normalized Kraus operators form an Abelian subgroup of the Pauli group.

5. Privatizing qubits with Abelian subgroups

We begin by discussing the simplest case, the channel whose Kraus operators are a normalized basis for the diagonal algebra, on arbitrary \( n \)-qubit space and what algebras can be privatized.

Let \( \Delta_{2^n} \) be the diagonal algebra on \( 2^n \times 2^n \) complex matrices, with basis the group \( \Delta \) generated by \( \{Z_1, Z_2, \ldots, Z_n\} \), where \( Z_i = Z \otimes I \otimes \cdots \otimes I \), etc. Then \( \Delta_{2^n} = \Delta_{2^n} \), and thus the conditional expectation \( \Phi_{\Delta_{2^n}} \) onto \( \Delta_{2^n} \), has as its Kraus operators the elements of \( \Delta \), multiplied by \( \frac{1}{2^n} \).

Of course, we now know the answer is any algebra quasiothogonal to the diagonal algebra \( \Delta_{2^n} \). We can give an abstract description of such algebras, and also a concrete construction. The abstract result follows from the following result of [20] and provides an upper bound on the number of privatized qubits.

**Lemma 2.** Let \( \mathcal{A} \) be a subalgebra of \( M_N(\mathbb{C}) \) unitarily equivalent to \( \bigoplus_{k=1}^n I_k \otimes M_{j_k}(\mathbb{C}) \). Then the following conditions are equivalent:

1. \( \mathcal{A} \) is quasiothogonal to \( \Delta_N \);
2. \( i_k \geq j_k \) for all \( 1 \leq k \leq m \).

As \( k \)-qubits can be encoded into the unital algebra \( I_{2^{n-k}} \otimes M_{2^k}(\mathbb{C}) \), the conditional expectation onto \( \Delta_{2^n} \) can privatize \( k \) qubits if and only if \( n - k \geq k \). In other words, the conditional expectation onto \( \Delta_{2^n} \) can privatize at most \( \left\lfloor \frac{n}{2} \right\rfloor \) qubits.
One explicit construction of such a subalgebra is to make use of the private subalgebra from our motivating example. For \(1 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor\) let \(X_i = \otimes_{k=1}^{n} \sigma_k\), where
\[
\sigma_k = \begin{cases} 
X & \text{if } k = 2i, \\
I & \text{otherwise}
\end{cases}
\]
and let \(Y_i = \otimes_{k=1}^{n} \sigma_k\), where
\[
\sigma_k = \begin{cases} 
Y & \text{if } k = 2i - 1, 2i \\
I & \text{otherwise}
\end{cases}
\]
Then \(\mathcal{B} = \text{Alg} \{X_i, Y_i\} : 1 \leq i, j \leq \left\lfloor \frac{n}{2} \right\rfloor\), where \(\text{Alg} \{S\}\) is the unital algebra generated by operators in \(S\), is quasiorthogonal to \(\Delta_2^n\), precisely because \(X_i, Y_i\) and all their products are never diagonal, unless they are the identity. This algebra encodes \(\left\lfloor \frac{n}{2} \right\rfloor\) qubits in the obvious way, where \(X_i, Y_i\) act as the Pauli matrices \(X, Y\) on \(\left\lfloor \frac{n}{2} \right\rfloor\) qubits with an \(X\) or \(Y\) in the \(i\)th tensor spot respectively.

We may use this explicit construction to prove the following in the general maximal Abelian case.

**Theorem 2.** Let \(\Phi\) be a a completely positive trace-preserving map on \(M_2^n(C)\) whose Kraus operators are equally weighted elements of a maximal Abelian subgroup \(G \subseteq \mathcal{P}_n\). Then \(\Phi\) can privatize \(\left\lfloor \frac{n}{2} \right\rfloor\) qubits.

**Proof.** Let \(\mathcal{A} = \text{Alg} \{G\}\) be the algebra generated by \(G\). Then \(\mathcal{A}\) is a maximal Abelian subalgebra of \(M_n(C)\). Thus \(\mathcal{A}' = \mathcal{A}\). The elements of \(G\) are clearly a basis for \(\mathcal{A}\), and hence \(\Phi\) is the trace-preserving conditional expectation onto \(\mathcal{A}' = \mathcal{A}\). Moreover, since \(\mathcal{A}\) is maximal Abelian, by simultaneously diagonalizing, there is a change of basis such that \(U \mathcal{A} U^\dagger = \Delta_2^n\). Denote by \(\mathcal{B}\) the subalgebra generated by \(\{X_i, Y_i\}\), where \(X_i\) and \(Y_i\) are as above. Then \(U^\dagger \mathcal{B} U\) is privatized by \(\Phi\); and following the discussion above, we see that \(\mathcal{B}\) is sufficient to encode \(\left\lfloor \frac{n}{2} \right\rfloor\) qubits.

We now examine the case that \(\mathcal{A}\) is a non-maximal Abelian algebra generated by Pauli operators. Corollary 3 says that for any subalgebra \(\mathcal{A}\) generated by elements of \(\mathcal{P}_n\), \(\dim(\mathcal{A}) \dim(\mathcal{A}') = 4^n = \dim(\mathcal{H})^2\). The algebras for which this equality holds can be characterized as follows [20].

**Lemma 3.** Let \(\mathcal{A}\) be a unital subalgebra of \(M_n(C)\), then the following are equivalent:

1. \(\dim(\mathcal{A}) \dim(\mathcal{A}') = N^2\),
2. \(\mathcal{A} = U(\oplus_{i=1}^{m} I_{4^i} \otimes M_{4^i}) U^\dagger\) for some unitary matrix \(U\).

**Lemma 4.** Every commutative subalgebra \(\mathcal{A} \subseteq M_n(C)\) generated by Pauli operators is unitarily equivalent to an algebra of the form \(I_{2^s} \otimes \text{Alg} \{Z_{i=1}^{k}\}\) for some \(k \leq n\).

**Proof.** By lemma 3, any commutative subalgebra \(\mathcal{A}\) generated by commuting Pauli operators satisfies \(rk_i = 1\) for all \(i\), and hence for some \(s\), decomposes as
Theorem 3. Let $\Phi : M_N(C) \rightarrow M_N(C)$ be a quantum channel whose Kraus operators $\{K_i\}_{i=1}^m$ are equally weighted elements of an Abelian subgroup of $\mathcal{P}_n$. Then there is a $\frac{k}{2}$-qubit algebra privatized by $\Phi$.

Proof. By lemma 4, the algebra generated by the Kraus operators must be unitarily equivalent to $I_{2^{2-k}} \otimes \Delta_{2^k}$; hence after diagonalizing and restricting to the subalgebra spanned by only the last $k$ qubits, we obtain the maximal Abelian subalgebra on $k$ qubits; theorem 2 tells us how to privatize $k$ qubits in this scheme. Tensoring any private algebra encoding $\frac{k}{2}$ qubits for the $2^k \times 2^k$ maximal Abelian case with a $2^{n-k} \times 2^{n-k}$ identity yields an algebra encoding $\frac{k}{2}$ qubits that is private for $\Phi$.

Remark 1. In a sense the results in this section can be thought of as the subsystem analog of the results from [1], where it was shown that $k$ unitaries could be used to privatize a $\frac{k}{2}$-qubit subspace. Here, we have shown that we can privatize a $\frac{k}{2}$-qubit subsystem algebra using $k$ elements from an Abelian subgroup of $\mathcal{P}_n$.

Another application of the privatization of information using Abelian subgroups is in the setting of approximately private channels, as presented in [2, 12]. In such a setting, the idea is to approximate a random unitary channel using a smaller set Kraus operators, which are drawn uniformly at random from a generating set. That is, given a target error rate $\epsilon$, the approximate random channel $\tilde{F}$ must approximate a channel on a private quantum subsystem within $\epsilon$ under the operator norm, $\|\tilde{F}(\rho) - I_d\|_\infty \leq \epsilon / d$. By comparing our channel construction to that of [2], we can obtain an approximate random channel using only $2^{k/2}$ random operators rather than $2^k$ to privatize a $\frac{k}{2}$-qubit algebra, which is a quadratic improvement.

Corollary 4. Given a set of operators $\{A_i\}_{i=1}^m$ that form an Abelian subgroup of $\mathcal{P}_n$, let $\Phi : M_N(C) \rightarrow M_N(C)$ be a quantum channel whose Kraus operators $\{R_i\}_{i=1}^S$ are chosen as a random distribution of operators from the set $\{A_i\}_{i=1}^m$, that is

$$\hat{\Phi}(\rho) = \frac{1}{S} \sum_{i=1}^S R_i \rho R_i^\dagger.$$ 

Assume $0 < \epsilon < 1$ and $S \geq Cd (\log d)^6 / \epsilon^2$, where $d = 2^{k/2}$. Then there exists a $\frac{k}{2}$-qubit algebra of states $\rho$ that is approximately privatized by the channel $\tilde{\Phi}$—that is $\|\tilde{\Phi}(\rho) - I_d\|_\infty \leq \epsilon / d$, for $d = 2^{k/2}$.

Proof. The idea behind the proof is to reduce the case of operators selected uniformly at random from an Abelian subgroup to the case of Pauli operators by finding an appropriate unitary equivalence between the private quantum subsystem and the traditional $\frac{k}{2}$-qubit algebra that is privatized by Pauli operators. Without loss of generality, we can choose the operators $\{A_i\}_{i=1}^m$ to be the set of operators that are the Kraus operators for the channel $I_{2^{2-k}} \otimes \Delta_{2^k}$, by unitary equivalence due to lemma 4. Then, by the mapping from theorem 2, there must exist a unitary $U$ between a $\frac{k}{2}$-qubit subspace and a subsystem that is
privatized by $I_{2^{n-1}} \otimes \Delta_{2^k}$. That is, let $\rho_0$ be an arbitrary $\frac{k}{2}$-qubit state, then there exists a $U$ such that

$$\frac{1}{2^k} \sum_{i=1}^{2^k} A_i \rho A_i^\dagger = \frac{1}{2^k} \sum_{i=1}^{2^k} A_i U (I_{2^{n-1}} \otimes \rho_0) U^\dagger A_i^\dagger.$$ 

In fact, theorem 2 states an even stronger result about the unitary equivalence $U$: there is a one-to-one correspondence between the operators $A_i$ and the Pauli operators $P_i$ restricted to the $\frac{k}{2}$-qubit subspace. Therefore, choosing a set of $S$ random operators from the set $\{A_i\}$, we arrive at the following identity

$$\Phi(\rho) = \frac{1}{S} \sum_{i=1}^{S} R_i \rho R_i^\dagger$$

$$= \frac{1}{S} \sum_{i=1}^{S} R_i U \rho_0 (UR_i)^\dagger$$

$$= \frac{1}{S} \sum_{i=1}^{S} (P_i' \otimes P_i) (I_{2^{n-1}} \otimes \rho_0) (P_i' \otimes P_i)$$

$$= \frac{1}{S} \sum_{i=1}^{S} (I \otimes P_i) (I_{2^{n-1}} \otimes \rho_0) (I \otimes P_i).$$

We can now use the result in [2, 12], which states that applying a channel whose Kraus operators are a random selection of Pauli operators on a particular subspace will result in an approximate random channel given $S \geq Cd (\log d)^9 / \epsilon^2$, where $d = 2^{k/2}$.

### 6. Conclusion

In this work, we demonstrate the underlying mathematical principles behind private quantum subsystems. Namely, by using the theory of quasiorthogonal algebras and developing the set of tools therein, we can make definite statements on the dimension of the subsystems that can be privatized by commuting Kraus operators. We show that by taking elements of a maximal Abelian subgroup $G$ of the $n$-qubit Pauli group $P_n$, the elements of such a group can privatize $\left\lfloor \frac{n}{2} \right\rfloor$ qubits when used as equally weighted Kraus operators of the channel, and we give explicit constructions for such private subsystems. Moreover, we show that this result can be generalized to fewer qubits when the size of the Abelian subgroup is not taken to be maximal.

### Acknowledgments

JL was supported by an AIMS-University of Guelph Postdoctoral Fellowship. TJ-O was supported by the Vanier-Banting Secretariat and NSERC through the Vanier Canada Graduate Scholarship. DWK was supported by NSERC and a University Research Chair at Guelph. RL was supported by NSERC, CIFAR, and the Canadian and Ontario governments. RP was supported by NSERC.

### Appendix A. Comment on generalized one-time pads

Following the analogy of the one-time pad, one could envision a private quantum channel $\Phi$ composed of a probabilistic distribution of channels $\Phi_k$, chosen according to a probability
distribution \( \{ p_k \} \) governed by a shared private key, thus \( \Phi(\sigma_k \otimes \sigma_k) = \sum_k p_k \Phi_k(\sigma_k \otimes \sigma_k) \). Now in order for \( \Phi \) to be a private quantum channel for the subsystem \( B \), it would need to satisfy the general requirement of a private subsystem according to definition 1. Moreover, in order for Bob to be able to recover the original quantum information given the secret ket, that is having access to the outcome of one of the \( \Phi_k \) channels, one would have to further require that all \( \Phi_k \) be operator quantum error correctable [16].

**Appendix B. Proof of privatized qutrit subsystem**

In this Appendix, we prove the result stated in example 1. Namely, for the generalized Pauli \( X \) and \( Z \) operators on qutrits, the channel

\[
\Phi(\rho) = \frac{1}{9} \sum_{ij=0}^2 (X^iZ^j \otimes X^iZ^j)\rho(X^iZ^j \otimes X^iZ^j)^{\dagger}
\]

has no private subspace but can privatize the subalgebra \( \mathcal{A} \) generated by \( X^2 \otimes X, XZ^2 \otimes Z \), which is isomorphic to the one-qutrit subalgebra \( I \otimes X, I \otimes Z \).

**Proof.** Explicitly, \( X^3 = Z^3 = I \), and \( XZ = \omega ZX \), so the group generated by \( X, Z \) has a bicharacter given by \( [g, h] = \chi(g, h)I \), yielding the following character matrix:

\[
\begin{array}{cccccccc}
I & X & X^2 & Z & XZ & X^2Z & Z^2 & XZ^2 & X^2Z^2 \\
I & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
X & 1 & 1 & 1 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\
X^2 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega & \omega & \omega \\
Z & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 \\
XZ & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega \\
X^2Z & 1 & \omega^2 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 \\
XZ^2 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 \\
X^2Z^2 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 \\
\end{array}
\]

In two qutrit space, the matrix of commutation relations is \( F \otimes F \); any all-1s submatrix of \( F \otimes F \) yields an Abelian subalgebra. Our choice corresponds to the tensor product of the \( \{ 1, 6, 8 \} \) submatrix of \( F \) with itself union the tensor product of the \( \{ 1, 5, 9 \} \) submatrix of \( F \) with itself.

To find a quasiorthogonal algebra to this Abelian algebra, we take a quotient by the subalgebra to obtain the following equivalence classes:

| \( I \otimes I \) | \( I \otimes X \) | \( I \otimes X^2 \) | \( X \otimes I \) | \( X^2 \otimes I \) |
|---|---|---|---|---|
| \( I \otimes XZ \) | \( I \otimes X^2Z \) | \( I \otimes Z \) | \( X \otimes XZ \) | \( X^2 \otimes XZ \) |
| \( I \otimes X^2Z^2 \) | \( I \otimes Z^2 \) | \( I \otimes XZ^2 \) | \( X \otimes X^2Z^2 \) | \( X^2 \otimes X^2Z^2 \) |
| \( X^2Z \otimes I \) | \( X^2Z \otimes X \) | \( X^2Z \otimes X^2 \) | \( Z \otimes I \) | \( XZ \otimes I \) |
| \( X^2Z \otimes XZ \) | \( X^2Z \otimes X^2Z \) | \( X^2Z \otimes Z \) | \( Z \otimes XZ \) | \( XZ \otimes XZ \) |
| \( X^2Z \otimes XZ^2 \) | \( X^2Z \otimes Z^2 \) | \( X^2Z \otimes XZ^2 \) | \( Z \otimes XZ^2 \) | \( XZ \otimes XZ \) |
| \( XZ \otimes I \) | \( XZ \otimes XZ \) | \( XZ \otimes X^2 \) | \( XZ \otimes X^2 \) | \( Z \otimes XZ \) |
| \( XZ \otimes XZ \) | \( XZ \otimes XZ \) | \( XZ \otimes Z \) | \( XZ \otimes Z \) | \( Z \otimes XZ \) |
| \( XZ \otimes XZ \) | \( XZ \otimes XZ \) | \( XZ \otimes Z \) | \( XZ \otimes Z \) | \( Z \otimes XZ \) |
| \( XZ \otimes XZ \) | \( XZ \otimes XZ \) | \( XZ \otimes Z \) | \( XZ \otimes Z \) | \( Z \otimes XZ \) |

\[ J. \text{Phys. A: Math. Theor.} \textbf{49} (2016) 125302 \text{J Levick et al} \]
Notice that cosets 3, 5, 8 and 9 are obtained by squaring cosets 2, 4, 7 and 6 respectively, so a choice of two generators for a quasiorthogonal subalgebra should make sure to avoid these pairs. Our choice corresponds to choosing $X^2 \otimes X$ from coset 8 and $XZ^2 \otimes Z$ from coset 3.

To see that this choice of generators is isomorphic to a qutrit algebra, note that the block unitary

$$U = \begin{pmatrix}
I & X^2Z^2 & XZ \\
XZ^2 & Z & X^2 \\
X^2Z & X & Z
\end{pmatrix}$$

acts by on $I \otimes X$ and $I \otimes Z$ by

$$U(I \otimes X)U^\dagger = \omega^2XZ^2 \otimes Z,$$
$$U(I \otimes Z)U^\dagger = X^2 \otimes X.$$

References

[1] Ambainis A, Mosca M, Tapp A and de Wolf R 2000 Private quantum channels IEEE Symp. on Foundations of Computer Science (FOCS) (Washington, DC: IEEE Computer Society) pp 547–553

[2] Aubrun G 2009 On almost randomizing channels with a short Kraus decomposition Commun. Math. Phys. 288 1103–16

[3] Bandyopadhyay S, Oscar Boykin P, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases Algorithmica 34 512–28

[4] Bartlett S D, Hayden P and Spekkens R W 2005 Random subspaces for encryption based on a private shared Cartesian frame Phys. Rev. A 72 052309

[5] Bartlett S D, Rudolph T and Spekkens R W 2004 Decoherence-full subsystems and the cryptographic power of a private shared reference frame Phys. Rev. A 70 032307

[6] Oscar Boykin P and Roychowdhury V 2003 Optimal encryption of quantum bits Phys. Rev. A 67 042317

[7] Oscar Boykin P, Sitharam M, Huu Tiep P and Wojcan P 2007 Mutually unbiased bases and orthogonal decompositions of Lie algebras Quantum Inf. Comput. 7 371–82

[8] Church A, Kribs D W, Pereira R and Plosker S 2011 Private quantum channels, conditional expectations, and trace vectors Quantum Inf. Comput. 11 774–83

[9] Cleve R, Gottesman D and Lo H-K 1999 How to share a quantum secret Phys. Rev. Lett. 83 648

[10] Crepeau C, Gottesman D and Smith A 2002 Secure multi-party quantum computing 34th Annu. Symp. on Theory of Computing (Montreal: ACM) p 643

[11] Davidson K R 1996 $C^*$-Algebras by Example (Fields Institute Monograph Series) (Providence, RI: American Mathematical Society)
[12] Hayden P, Leung D, Shor P W and Winter A 2004 Randomizing quantum states: constructions and applications Commun. Math. Phys. 250 371–91
[13] Jochym-O’Connor T, Kribs D W, Laflamme R and Plosker S 2013 Private quantum subsystems Phys. Rev. Lett. 111 030502
[14] Jochym-O’Connor T, Kribs D W, Laflamme R and Plosker S 2014 Quantum subsystems: exploring the complementarity of quantum privacy and error correction Phys. Rev. A 90 032305
[15] Kretschmann D, Kribs D W and Spekkens R W 2008 Complementarity of private and correctable subsystems in quantum cryptography and error correction Phys. Rev. A 78 032330
[16] Kribs D W, Laflamme R, Poulin D and Lesosky M 2006 Operator quantum error correction Quantum Inf. Comput. 6 382–99
[17] Nielsen Michael A and Chuang Isaac L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[18] Ohno H 2008 Quasi-orthogonal subalgebras of matrix algebras Linear Algebr. Appl. 429 2146–58
[19] Ohno H and Petz D 2009 Generalizations of Pauli channels Acta Math. Hung. 124 165–77
[20] Pereira R 2003 Trace vectors in matrix analysis PhD Thesis University of Toronto
[21] Pereira R 2006 Representing conditional expectations as elementary operators Proc. Am. Math. Soc. 134 253–8
[22] Petz D and Kahn J 2007 Complementary reductions for two qubits J. Math. Phys. 48 012107
[23] Pittenger A O and Rubin M H 2004 Mutually unbiased bases, generalized spin matrices and separability Linear Algebr. Appl. 390 255–78
[24] Rudin W 1990 Fourier Analysis on Groups (Toronto: Wiley)
[25] Weiner M 2010 On orthogonal systems of matrix algebras Linear Algebr. Appl. 433 520–33