All teleportation and dense coding schemes

2001 J. Phys. A: Math. Gen. 34 7081

(http://iopscience.iop.org/0305-4470/34/35/332)

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

J. Phys. A: Math. Gen. **34** (2001) 7081–7094 PII: S0305-4470(01)19278-4

All teleportation and dense coding schemes

R F Werner

Institut für Mathematische Physik, TU Braunschweig, Mendelssohnstr. 3, 38106 Braunschweig, Germany

E-mail: r.werner@tu-bs.de

Received 20 November 2000
Published 24 August 2001
Online at stacks.iop.org/JPhysA/34/7081

Abstract

We establish a one-to-one correspondence between (1) quantum teleportation schemes, (2) dense coding schemes, (3) orthonormal bases of maximally entangled vectors, (4) orthonormal bases of unitary operators with respect to the Hilbert–Schmidt scalar product and (5) depolarizing operations, whose Kraus operators can be chosen to be unitary. The teleportation and dense coding schemes are assumed to be 'tight' in the sense that all Hilbert spaces involved have the same finite dimension d, and the classical channel involved distinguishes d^2 signals. A general construction procedure for orthonormal bases of unitaries, involving Latin squares and complex Hadamard matrices is also presented.

PACS number: 03.67.−a

1. Introduction

Teleportation and dense coding are two processes, which stood at the beginning of modern quantum information theory. They both demonstrated radically new features of quantum information as opposed to classical information, in that both would be impossible without the assistance of entangled states. Indeed, the attempt of using the properties of a classically correlated system shared by sender and receiver to improve the transmission rate of a classical channel can easily be seen to be hopeless. But this is precisely what happens in teleportation and dense coding, and dramatically so, because without entanglement assistance, teleportation, i.e., the transmission of quantum information on a classical channel, would not only be less efficient, but virtually impossible.

In the original papers [BW, BB] the new possibilities were demonstrated by giving an explicit example, based on qubits. It was clear early on that extensions to systems with higher-dimensional Hilbert spaces were possible, not only to powers of 2, by running the process several times, but to any dimension $2 \leqslant d < \infty$ [BB].

The task set in this paper is to do this systematically, and to classify *all* schemes for teleportation and dense coding. There are several reasons for doing this. The first is, of course,

to take these miracle machines apart and to analyse what makes them work: what is the mathematical structure one really needs to set up such a scheme? For the present author one motivation of this kind was to understand the surprising observation that each of the published teleportation schemes also works as a dense coding scheme, and conversely: sender Alice and receiver Bob merely have to swap the equipment they use. An attempt at a direct proof of this failed, and indeed, as discussed below, the statement fails in general, but is true in the special case of 'tight' schemes.

The second reason for attempting a complete classification of teleportation schemes is more practical. In spite of amazing progress in recent years, experiments in quantum information processing are still quite difficult. Hence, for realizing a teleportation scheme it is useful to have a systematic overview of the options, before going on to find the one which is the easiest to implement. This also goes for approximate realizations. And in order to find feasible approximate teleportation schemes it is probably once again necessary to understand the manifold of exact realizations.

The aim of determining all schemes is not quite achieved in this paper, in two respects. Firstly, we will only look at the case when dense coding and teleportation are realized optimally with minimal resources, in the sense of Hilbert space dimensions and number of distinguishable classical signals. As in the well-known qubit case, this means that an entangled state between systems of the same dimension d as the input systems is used, and the classical channel distinguishes d^2 signals. That is, the classical capacity of the quantum channel is exactly doubled by dense coding, and teleportation requires twice as much classical channel capacity as the quantum capacity of the channel set up by this scheme. We will call schemes with these dimension parameters *tight*. As mentioned above, for these dimensions the symmetry between teleportation and dense coding holds perfectly. Classifying all schemes beyond the tight case appears to be more difficult because there is too much freedom, which cannot be parametrized in a simple way (see, however, [BD]).

The second respect in which this paper falls short of a complete classification is that we can only reduce it to another 'standard' problem, namely the construction of orthonormal bases of unitary operators with respect to the scalar product $(A, B) \mapsto d^{-1}\mathrm{tr}(A^*B)$. In the final section we provide a fairly general construction for such bases. However, even this construction has to rely on other well-known but not completely classified combinatorial designs, namely Latin squares, and complex Hadamard matrices. This suggests that a complete construction procedure for all unitary bases would be at least as difficult as a complete classification of Latin squares or Hadamard matrices, and hence hardly a promising task.

The paper is organized as follows. In section 2 the main theorem is stated: an equivalence in the tight case between teleportation schemes, dense coding schemes, orthonormal unitary bases, bases of maximally entangled vectors, and so-called unitary depolarizers. Basic consequences of the theorem are discussed. Section 3 contains the proof, divided into subsections, each devoted to some implication in the big equivalence. In writing the proof an attempt was made to include also simple steps explicitly, and to make as transparent as possible why the tightness condition is crucial. Finally, in section 4 we present the 'shift and multiply' construction of unitary bases, which are then classified in terms of Latin squares and Hadamard matrices.

2. Main result

In order to state our result we use the following notation and terminology: When $\mathcal{H}$ is a Hilbert space, we denote by $\mathcal{B}(\mathcal{H})$ the space of bounded linear operators on $\mathcal{H}$. A *channel* converting quantum systems with Hilbert space $\mathcal{H}_{\mathrm{in}}$ into systems with Hilbert space $\mathcal{H}_{\mathrm{out}}$ is a

linear operator $T : \mathcal{B}(\mathcal{H}_{\text{out}}) \to \mathcal{B}(\mathcal{H}_{\text{in}})$, which is completely positive [Da, Pa] and normalized as $T(\mathbb{1}) = \mathbb{1}$. A (discrete) *observable* F on $\mathcal{H}$ over an output parameter space X is a collection of positive operators $F_x \in \mathcal{B}(\mathcal{H})$ such that $\sum_x F_x = \mathbb{1}$. A *density operator* on $\mathcal{H}$ is a positive operator with trace 1. The basic *probabilistic interpretation* of these objects is fixed by the prescription that $\text{tr}(\omega T(F_x))$ is the probability to get the measuring result 'x' on systems prepared according to ω, before passing through the channel T. Finally, we call a vector $\Psi \in \mathcal{H} \otimes \mathcal{H}$ *maximally entangled*, if it is normalized, and its reduced density operator is maximally mixed, i.e., a multiple of $\mathbb{1}$:

$$\langle \Psi | (A \otimes \mathbb{1})\Psi \rangle = (\dim \mathcal{H})^{-1} \text{tr}(A). \tag{1}$$

Let us set up the equations describing dense coding and teleportation in this language. In both cases, the beginning of each transmission is to distribute the parts of an entangled state ω between sender Alice and receiver Bob. Only then Alice is given the message she is supposed to send, which is a quantum state in the case of teleportation and a classical value in case of dense coding. She codes this in a suitable way, and Bob reconstructs the original message by evaluating Alice's signal jointly with his entangled subsystem. For *dense coding*, assume that $x \in X$ is the message given to Alice. She encodes it by transforming her entangled system by a channel T_x, and sending the resulting quantum system to Bob, who measures an observable F jointly on Alice's particle and his. The probability for getting y as a result is then $\text{tr}(\omega(T_x \otimes \text{id})(F_y))$, where the '$\otimes$id' expresses the fact that no transformation is done to Bob's particle while Alice applies T_x to hers. If everything works correctly, this expression has to be 1 for $x = y$, and 0 otherwise (see equation (3)).

Let us take a similar look at *teleportation*. Here three quantum systems are involved: the entangled pair in state ω, and the input system given to Alice, in state ρ. Thus the overall initial state is $\rho \otimes \omega$. Alice measures an observable F on the first two factors, obtaining a result x sent to Bob. Bob applies a transformation T_x to his particle, and makes a final measurement of an observable A of his choice. Thus the probability for Alice measuring x and for Bob getting a result 'yes' on A, is $\text{tr}(\rho \otimes \omega)(F_x \otimes T_x(A))$. Note that the tensor symbols in this equation refer to different splittings of the system ($1 \otimes 23$ and $12 \otimes 3$, respectively). Teleportation is successful if the overall probability for getting A, computed by summing over all possibilities x, is the same as for an ideal channel, i.e. $\text{tr}(\rho A)$, as in equation (2).

The only relationship between the Hilbert spaces involved, which this description requires, is that the input and output spaces of the teleportation line are the same, since the whole teleportation process is equivalent to the identity. In some sense the best results (minimal dimension for the Hilbert spaces carrying the entangled state, best ratio of achieved capacity to capacity used) are obtained in the special case, where all Hilbert spaces have the same dimension d, and exactly $|X| = d^2$ signals are distinguished. We call this the *tight* case, and the main theorem refers only to this case.

Theorem 1. *Let $\mathcal{H}$ be a d-dimensional Hilbert space ($d < \infty$), and X a set of d^2 elements. Consider the following types of objects:*

(1) ***Teleportation schemes**, consisting of*

- *a density operator ω on $\mathcal{H} \otimes \mathcal{H}$*
- *a collection of channels $T_x : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, $x \in X$*
- *an observable F_x, $x \in X$ on $\mathcal{H} \otimes \mathcal{H}$ such that, for all density operators ρ on $\mathcal{H}$, and $A \in \mathcal{B}(\mathcal{H})$:*

$$\sum_{x \in X} \text{tr}(\rho \otimes \omega)(F_x \otimes T_x(A)) = \text{tr}\rho A. \tag{2}$$

(2) ***Dense coding schemes***, *consisting of the same objects as a teleportation scheme, but satisfying, instead of (2), the equation*

$$\mathrm{tr}(\omega(T_x \otimes \mathrm{id})(F_y)) = \delta_{xy}. \tag{3}$$

(3) ***Bases of maximally entangled vectors***, *i.e., families of maximally entangled vectors* $\Phi_x \in \mathcal{H} \otimes \mathcal{H}$, $x \in X$ *such that*

$$\langle \Phi_x | \Phi_y \rangle = \delta_{xy}. \tag{4}$$

(4) ***Bases of unitary operators***, *i.e., collections of unitary operators* $U_x \in \mathcal{B}(\mathcal{H})$, $x \in X$ *such that*

$$\mathrm{tr}(U_x^* U_y) = d\delta_{xy}. \tag{5}$$

(5) ***Unitary depolarizers***, *i.e., collections of unitary operators* $U_x \in \mathcal{B}(\mathcal{H})$, $x \in X$ *such that for any* $A \in \mathcal{B}(\mathcal{H})$*:*

$$\sum_x U_x^* A U_x = d\,\mathrm{tr}(A)\mathbb{1}. \tag{6}$$

Then, given any object of any one of these types, one can construct an object of each of the types, using the following equations:

$$\omega = |\Omega\rangle\langle\Omega| \qquad \textit{with } \Omega \textit{ maximally entangled.} \tag{7}$$

$$F_x = |\Phi_x\rangle\langle\Phi_x| \tag{8}$$

$$T_x(A) = U_x^* A U_x \tag{9}$$

$$\Phi_x = (U_x \otimes \mathbb{1})\Omega. \tag{10}$$

The logical structure of this result is maybe slightly unusual, so we begin by giving some examples of how it is used. We can use it, for example, as a construction procedure: once we are given a unitary basis, we can obtain from equations (7)–(10) a teleportation scheme and a dense coding scheme. Moreover, since we could also start with these schemes, ending up with the unitary basis we are assured that *every* teleportation or dense coding scheme is obtained in this way, i.e., this construction is exhaustive. In particular, we learn that any tight teleportation scheme is necessarily of a very special form: the entangled state ω must be pure and maximally entangled, the channels T_x must be unitarily implemented, and the observable F must be a complete von Neumann measurement.

Another result contained in this theorem is the amazing equivalence between (1) and (2): any teleportation scheme works as a dense coding scheme, and conversely. Alice and Bob merely have to swap their equipment to convert one into the other. We must emphasize, however, that the tightness condition is absolutely crucial for this equivalence. For simplicity, we will discuss this only in the case that $|X| = n$ is not fixed to be d^2, leaving aside the more difficult question what kind of trade-off between resources becomes possible when ω lives on $\mathcal{H}_1 \otimes \mathcal{H}_2$, with dimensions other than $d \otimes d$.

The basic difference between teleportation and dense coding is that the parameters d and n have opposite roles: for teleportation, d describes the size of the signal to be sent, and n describes a resource, so the problem becomes more difficult when we increase d and decrease n. For dense coding, it is exactly the opposite. Therefore, it is easy to show that teleportation (resp. dense coding) schemes exist whenever $n \geqslant d^2$ (resp. $n \leqslant d^2$). In fact, for teleportation one can take X to be a continuum, and replace the sum in the teleportation equation by an integral [BD], but the dense coding equation would make no sense then. The optimality of these dimension inequalities, i.e., that no teleportation (resp. dense coding) scheme exists with $n < d^2$ (resp. $n > d^2$), is also a corollary of theorem 1. To prove it, suppose we had

a teleportation scheme with $n < d^2$. Then we could add $(d^2 - n)$ irrelevant classical signals happening with probability zero ($F_x = 0$), and apply the theorem, which says that all F_x must be non-zero after all. The same reasoning works for dense coding with the operation of throwing in a few unused Hilbert space dimensions.

Of course, our theorem is efficient as a construction procedure for dense coding and teleportation schemes only to the extent that unitary bases can be generated. After giving the proof of the theorem, we will therefore describe the most general construction for such bases known to us.

3. Proof of theorem 1

3.1. Proof of the implications '3 $\Longleftrightarrow$ 4'

Implicit in the formulation of the theorem is the claim that equation (10) $\Phi_x = (U_x \otimes \mathbb{1})\Omega$ not only determines Φ_x in terms of U_x but also, conversely, determines U_x in terms of Φ_x. This connection is based on a general construction, by which the d^2 matrix elements of an operator $A : \mathcal{H} \to \mathcal{H}$ are identified with the d^2 components of a vector Ψ. This identification depends on the choice of a maximally entangled vector Ω. By choosing appropriate orthonormal bases e_k, $k = 1, \ldots, d$, in the first and second tensor factor, such a vector can be written in 'Schmidt form' as

$$\Omega = \frac{1}{\sqrt{d}} \sum_k e_k \otimes e_k. \tag{11}$$

Then a one-to-one correspondence between operators $A \in \mathcal{B}(\mathcal{H})$ and $\Psi \in \mathcal{H} \otimes \mathcal{H}$ is given by the equation $\langle e_k | A e_\ell \rangle = \sqrt{d} \langle e_k \otimes e_\ell | \Psi \rangle$. We will use this in the form

$$\Psi = (A \otimes \mathbb{1})\Omega = (\mathbb{1} \otimes A^{\mathrm{T}})\Omega \tag{12}$$

where the transpose operation $A \mapsto A^{\mathrm{T}}$ is defined in the basis e_k. Then if A and Ψ and, similarly, A' and Ψ' are related in this way,

$$\langle \Psi | (B \otimes \mathbb{1}) \Psi' \rangle = \frac{1}{d} \mathrm{tr}(A^* B A') \tag{13}$$

for arbitrary $B \in \mathcal{B}(\mathcal{H})$. Thus Ψ is maximally entangled iff this expression (for $A = A'$) is equal to d^{-1} tr(B), i.e., iff A is unitary. Moreover, setting $B = \mathbb{1}$, the scalar product of vectors Ψ, Ψ' is translated to $d^{-1}\mathrm{tr}(A^* A')$ in terms of A, A'. Taking all this together, we get the one-to one correspondence between unitary bases and bases of maximally entangled vectors, as claimed. Note, however, that this correspondence depends on the choice of the reference maximally entangled vector Ω.

3.2. Proof of the implications '4 $\Longleftrightarrow$ 5'

This proof is relatively straightforward, since we are talking about only one type of objects, collections of d^2 unitaries $U_x \in \mathcal{B}(\mathcal{H})$. It is, however, also a crucial step for the entire proof, since it is here that the consequences of the tightness condition are seen. We will prove this in a form which is also needed later to establish that the state ω in teleportation and dense coding schemes is necessarily maximally entangled.

The basic observation concerning matching dimensions is the following.

Lemma 2. *D vectors $\phi_1, \ldots, \phi_D$ in a D-dimensional Hilbert space form an orthonormal basis if and only if*

$$\sum_{k=1}^{D} |\phi_k\rangle\langle\phi_k| = \mathbb{1}. \tag{14}$$

Of course, this is false when there are more vectors than the dimension of the Hilbert space. Such families of vectors are called 'over-complete'. They exist and are an interesting mathematical structure of their own. On the other hand, fewer vectors than the dimension can never satisfy (14), because the rank (dimension of the range) of the operator on the left-hand side is at most the number of vectors.

Proof. It is a well-known fact that (14) holds for any orthonormal basis. Conversely, we find from (14) that, for each k, $|\phi_k\rangle\langle\phi_k| \leqslant \mathbb{1}$, which is the same as $||\phi_k||^2 \leqslant 1$. On the other hand, taking the trace of (14), we get $\sum_k ||\phi_k||^2 = \mathrm{tr}(\mathbb{1}) = D$. This is only possible when $||\phi_k||^2 = 1$ for all k. Hence the operators $|\phi_k\rangle\langle\phi_k|$ are Hermitian projections, and we can invoke the observation that Hermitian projections p_1, p_2 with $p_1 + p_2 \leqslant \mathbb{1}$ are necessarily orthogonal. (For a quick proof, sandwich the inequality between factors p_1, finding $p_1 + p_1 p_2 p_1 \leqslant p_1$, i.e., $p_1 p_2 p_1 = (p_2 p_1)^*(p_2 p_1) \leqslant 0$, and hence $p_2 p_1 = 0$.) □

We now apply this lemma to a collection of $D = d^2$ operators in $\mathcal{B}(\mathcal{H})$, where this space is considered as a Hilbert space with a suitable scalar product.

Proposition 3. *Consider d^2 operators $K_1, \ldots, K_{d^2}$ on a d-dimensional Hilbert space $\mathcal{H}$, and let $R > 0$ be an invertible operator on $\mathcal{H}$.*

Then the following conditions are equivalent

(1) $\mathrm{tr}(K_x^* R^{-1} K_y) = \delta_{xy}$, *for* $x, y = 1, \ldots, d^2$
(2) $\sum_x K_x^* C K_x = \mathrm{tr}(RC)\mathbb{1}$ *for all* $C \in \mathcal{B}(\mathcal{H})$.

Proof. Let us define a scalar product $\langle\cdot|\cdot\rangle_R$ on $\mathcal{B}(\mathcal{H})$ by

$$\langle A|B\rangle_R = \mathrm{tr}(A^* R^{-1} B). \tag{15}$$

Since R is positive and invertible, this is indeed a scalar product, satisfying $\langle A|A\rangle_R = 0$ only for $A = 0$. Condition 1 then simply says that the K_x are an orthonormal basis. By the previous lemma this is equivalent to the completeness relation (14), so all we have to do is to show that this relation, adapted to the special scalar product at hand, is equivalent to condition 2 of the present lemma. The completeness relation is that, for any $A, B \in \mathcal{B}(\mathcal{H})$,

$$\langle A|B\rangle_R = \sum_x \langle A|K_x\rangle_R \langle K_x|B\rangle_R. \tag{$*$}$$

It suffices to evaluate this on rank one operators $A, B \in \mathcal{B}(\mathcal{H})$, since these span the whole space. We take $A = |\phi_1\rangle\langle\phi_2|$ and $B = |\psi_1\rangle\langle\psi_2|$. Then the left-hand side of equation ($*$) becomes

$$\langle\phi_1|R^{-1}\psi_1\rangle\langle\psi_2|\phi_2\rangle \tag{$*$LHS}$$

whereas the right-hand side is

$$\sum_x \langle\phi_1|R^{-1}K_x\phi_2\rangle\langle\psi_2|K_x^* R^{-1}\psi_1\rangle = \langle\psi_2|M\phi_2\rangle \tag{$*$RHS}$$

with

$$M = \sum_x K_x^* R^{-1}|\psi_1\rangle\langle\phi_1|R^{-1}K_x \equiv \sum_x K_x^* C K_x$$

where we have interchanged the two factors in each term, and introduced the abbreviation C. Since ($*$LHS)=($*$RHS) for every ψ_2, ϕ_2, we find $M = \langle\phi_1|R^{-1}\psi_1\rangle\mathbb{1}$. The factor is readily identified as $\langle\phi_1|R^{-1}\psi_1\rangle = \mathrm{tr}(RC)$. Since operators of the form C span $\mathcal{B}(\mathcal{H})$, the completeness relation thus becomes equivalent to $\sum_x K_x^* C K_x = \mathrm{tr}(RC)\mathbb{1}$ for all C, which completes the proof. □

The special case of this proposition, where each K_x is unitary and $R = \frac{1}{d}\mathbb{1}$, is exactly the relationship between items 4 and 5 of theorem 1. However, there is another consequence needed later on:

Corollary 4. *Let $U_1, \ldots, U_{d^2} \in \mathcal{B}(\mathcal{H})$ be unitaries in a d-dimensional Hilbert space $\mathcal{H}$, and ρ a density operator such that* $\operatorname{tr}(U_x^* \rho U_y) = \delta_{xy}$. *Then* $\rho = d^{-1}\mathbb{1}$.

Proof. Since the U_x are an orthonormal set whose cardinality is the dimension, there can be no null vectors of this scalar product, i.e., $\operatorname{tr}(A^*\rho A) = 0$ implies $A = 0$. Hence ρ is invertible, and we can apply the previous proposition with $R = \rho^{-1}$, finding that $\sum_x U_x^* A U_x = \operatorname{tr}(\rho^{-1}A)\mathbb{1}$. The trace of this equation is $d^2 \operatorname{tr}(A) = d \operatorname{tr}(\rho^{-1}A)$. This holds for all A, i.e., $\rho^{-1} = d\mathbb{1}$. □

3.3. Proof of '(3 or 4) $\Longrightarrow$ (1 and 2)'

Suppose now we are given either a basis of unitary operators or of maximally entangled vectors. Then we can choose a maximally entangled vector Ω and use equation (10) as in the proof of '3 $\Longrightarrow$ 4' to define the other kind of basis. Equations (8) and (9) then become explicit definitions of the observable F_x and the transformations T_x, respectively, so all the objects needed for a teleportation or dense coding scheme are defined, and we only need to verify that equations (2) and (3) are indeed satisfied.

In the teleportation equation an expectation value is generated between a state on the first and an observable on the third factor of a triple tensor product. This is a consequence of a similar 'teleportation equation' on the level of vectors, which we now state. For later use we prove a certain converse at the same time.

Lemma 5. *Let $\Omega \in \mathbb{C}^d \otimes \mathbb{C}^d$ be the maximally entangled vector $\Omega = d^{-1/2}\sum_k e_k \otimes e_k$, where $e_k, k = 1, \ldots, d$ is the standard basis of $\mathbb{C}^d$. Let $M \in \mathcal{B}(\mathbb{C}^d)$, and $\mu \in \mathbb{C}$. Then the equation*

$$\langle \phi \otimes \Omega | (\mathbb{1} \otimes M \otimes \mathbb{1})\Omega \otimes \psi \rangle = \mu \langle \phi | \psi \rangle$$

holds for all $\phi, \psi \in \mathbb{C}^d$, if and only if $M = d\mu\mathbb{1}$.

Proof. Inserting the sum defining Ω we get

$$\langle \phi \otimes \Omega(\mathbb{1} \otimes M \otimes \mathbb{1})\Omega \otimes \psi \rangle = \frac{1}{d}\sum_{k\ell} \langle \phi \otimes e_\kappa \otimes e_\kappa | (\mathbb{1} \otimes M \otimes \mathbb{1}) e_\ell \otimes e_\ell \otimes \psi \rangle$$

$$= \frac{1}{d}\sum_{\kappa\ell} \langle \phi | e_\ell \rangle \langle e_k | M e_\ell \rangle \langle e_k | \psi \rangle = \frac{1}{d}\langle \phi | M^T \psi \rangle$$

which is equal to $\mu\langle\phi|\psi\rangle$ for all ϕ, ψ iff $M^T = d\mu\mathbb{1}$. □

Consider now the term with index $x \in X$ in the *teleportation* equation (2), with F_x and T_x defined via equations (8), (9), and (10). Without loss of generality we set $\rho = |\phi_1\rangle\langle\phi_2|$, $A = |\psi_1\rangle\langle\psi_2|$. Then

$$\text{term}_x = \langle \phi_2 \otimes \Omega | \Phi_x \otimes U_x^* \psi_1 \rangle \langle \Phi_x \otimes U_x^* \psi_2 | \phi_1 \otimes \Omega \rangle.$$

The first scalar product can be rewritten by substituting Φ_x from equation (10), using equation (12):

$$\begin{aligned}
\langle \phi_2 \otimes \Omega | \Phi_x \otimes U_x^* \psi_1 \rangle &= \langle \phi_2 \otimes ((\mathbb{1} \otimes U_x)\Omega) | ((U_x \otimes \mathbb{I})\Omega) \otimes \psi_1 \rangle \\
&= \langle \phi_2 \otimes ((U_x^T \otimes \mathbb{1})\Omega) | ((\mathbb{1} \otimes U_x^T)\Omega) \otimes \psi_1 \rangle \\
&= \langle (\mathbb{1} \otimes U_x^T \otimes \mathbb{I})\phi_2 \otimes \Omega | (\mathbb{1} \otimes U_x^T \otimes \mathbb{1})\Omega \otimes \psi_1 \rangle \\
&= \langle \phi_2 \otimes \Omega | \Omega \otimes \psi_1 = \frac{1}{d}\langle \phi_2 | \psi_1 \rangle,
\end{aligned}$$

where in the last equation we used lemma 5 with $\mu = 1/d$. Together with a similar computation for the second scalar product, we get $\text{term}_x = d^{-2}\langle\phi_2|\psi_1\rangle\langle\psi_2|\phi_1\rangle = d^{-2}\,\text{tr}(\rho A)$, and equation (2) follows by summing over d^2 equal terms.

Similarly, for the *dense coding* equation (3) we get

$$\text{tr}(\omega(T_x \otimes \text{id})(F_y)) = \langle\Omega|(U_x^* \otimes \mathbb{I})\Phi_y\rangle\langle\Phi_y|(U_x \otimes \mathbb{1})\Omega\rangle,$$

i.e., the absolute square of the scalar product

$$\langle\Omega|(U_x^* \otimes \mathbb{1})\Phi_y\rangle = \langle\Omega|(U_x^* U_y \otimes \mathbb{1})\Omega\rangle = \frac{1}{d}\text{tr}(U_x^* U_y) = \delta_{xy},$$

where we have used in turn equation (10), the maximal entangledness of Ω (see equation (1)), and the orthogonality of the U_x. This completes the proof of the dense coding property.

3.4. Proof of the implications '2 $\Longrightarrow$ rest'

Let us now assume that a dense coding scheme is given. We have to conclude that it is of the special form given in equations (7)–(10).

Note first that if $\omega = \sum_\alpha \lambda_\alpha \omega_\alpha$ ($\lambda_\alpha > 0$) is a mixture of states satisfying the teleportation equation, then every ω_α also satisfies it. Hence the assumption is also satisfied for each pure component ω_α, and we can first analyse the problem assuming ω to be pure. In order to show that ω indeed is pure, we only have to verify that the given *F, T* are consistent only with one pure state. So for the moment we will assume that $\omega = |\Omega\rangle\langle\Omega|$ is pure.

The next step is a simple general observation on the coding of classical information on quantum channels, which we isolate in a lemma.

Lemma 6. *Let $\mathcal{K}$ be a D-dimensional Hilbert space, and $\sigma_x, F_x \in \mathcal{B}(\mathcal{K})$, for $x \in X$, a set with D elements. Suppose that each σ_x is a density operator, F is an observable, and $\text{tr}(\sigma_x F_y) = \delta_{xy}$, for $x, y = 1, \ldots, D$. Then there is an orthonormal basis $\Phi_x \in \mathcal{H}$ such that*

$$\sigma_x = F_x = |\Phi_x\rangle\langle\Phi_x|.$$

Proof. Let Φ_x be one of the normalized eigenvectors of σ_x with non-zero eigenvalue. Then since $F_x \leqslant \mathbb{1}$, and $\langle\Phi_x|F_x\Phi_x\rangle = 1$, Φ_x must also be an eigenvector of F_x with eigenvalue 1. Similarly, for any $y \neq x$ the $F_x \geqslant 0$, and the normalization $\sum_x F_x = \mathbb{1}$ forces $F_y\Phi_x = 0$. Hence the Φ_x are orthonormal, and since their number is the dimension of the space, they must be a basis. Consequently we have jointly diagonalized the F_x and the σ_x, with eigenvalues either 0 or 1. □

We apply this lemma with $D = d^2$ and σ_x the state after application of T_x to the first factor, i.e., $\text{tr}(\sigma_x A) = \text{tr}(\omega(T_x \otimes \text{id})(A))$. This proves equation (8), although it remains to be seen that each Φ_x is maximally entangled.

Since the σ_x form a maximal set of pure states, there cannot be a non-zero projection P such that, for all $x \in X$,

$$\begin{aligned} 0 &= \text{tr}(\sigma_x(\mathbb{1} \otimes P)) = \text{tr}(\omega(T_x \otimes \text{id})(\mathbb{1} \otimes P)) \\ &= \text{tr}(\omega(\mathbb{1} \otimes P)) = \langle\Omega|(\mathbb{1} \otimes P)\Omega\rangle. \end{aligned}$$

Hence Ω must have *full Schmidt rank*. We will need the consequence that the equation $(A \otimes \mathbb{1})\Omega = (A' \otimes \mathbb{1})\Omega$ implies $A = A'$.

Let $T_x(A) = \sum_\alpha K_{x,\alpha}^* A K_{x,\alpha}$ be the Kraus decomposition of T_x. Then the teleportation equation is

$$\sum_\alpha |\langle\Omega|(K_{x,\alpha}^* \otimes \mathbb{I})\Phi_y\rangle|^2 = \delta_{xy}.$$

Therefore, $\langle (K_{x,\alpha} \otimes \mathbb{1})\Omega | \Phi_y \rangle = 0$ for all $y \neq x$, and for every x there must be constants c_α such that

$$(K_{x,\alpha} \otimes \mathbb{1})\Omega = c_\alpha \Phi_x \ . \tag{16}$$

Since Ω has full Schmidt rank, this implies that all $K_{x,\alpha}$ are proportional to each other, i.e., that T_x can be written with a single Kraus summand. Of course, the corresponding $K_x \equiv U_x$ must be unitary, and since both sides are normalized, equation (16) $\Phi_x = (U_x \otimes \mathbb{1})\Omega$, possibly after fixing suitable phase factors (which influence neither T_x nor F_x).

The orthonormality of the Φ_x translates into $\mathrm{tr}(\rho U_x^* U_y) = \delta_{xy}$, where ρ is the reduced density operator of ω. But then corollary 4 shows that ρ must be a multiple of the identity, i.e., Ω, and each Φ_x is maximally entangled.

Finally, we have to complete the argument for the purity of ω by showing that only one pure state is consistent with the other data *T, F*, encoded in U_x. But this is obvious from the explicit expression $\Omega = (U_x^* \otimes \mathbb{1})\Phi_x$.

3.5. Proof of the implications '1 $\Longrightarrow$ rest'

Let us now assume that a teleportation scheme is given. We have to conclude that it is of the special form given in equations (7)–(10).

The crucial input for this proof is the principle that in quantum mechanics there is no measurement without perturbation. It enters in the following form, a corollary of the so-called Radon–Nikodym theorem for completely positive maps. We state it here as a lemma.

Lemma 7. *Let $\mathcal{H}$ be a finite dimensional Hilbert space, and let $T_\alpha : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be completely positive maps such that $\sum_\alpha T_\alpha = \mathrm{id}$. Then there are positive numbers t_α such that $T_\alpha = t_\alpha \mathrm{id}$.*

Proof. For readers less familiar with dilation theory of cp-maps we include a quick proof based on the Kraus decomposition $T(A) = \sum_\beta K_\beta^* A K_\beta$, which exists for every completely positive map. Note that by decomposing each T_α in Kraus form, we get a finer decomposition of id, so we may as well prove the lemma for the case that each T_α is of the form $T_\alpha(A) = K_\alpha^* A K_\alpha$. With $A = |\psi\rangle\langle\psi|$,

$$|K_\alpha^*\psi\rangle\langle K_\alpha^*\psi| \leqslant \sum_\alpha |K_\alpha^*\psi\rangle\langle\psi|K_\alpha = |\psi\rangle\langle\psi| \ .$$

Hence $K_\alpha^*\psi = \lambda(\psi)\psi$, with a factor $\lambda(\psi) \in \mathbb{C}$. But then *every* vector ψ is an eigenvector of the linear operator K_α^*, which is only possible if K_α^* is a multiple of the identity. □

A collection of completely positive maps adding up to a normalized one should be understood as an 'instrument' in the terminology of Davies [Da], i.e., a device which produces classical measurement results '*k*', such that the probability for obtaining this result *and* a response to a subsequent measurement F on an input state ρ is $\mathrm{tr}(\rho T_k(F))$). The channel $\sum_k T_k$ then describes the overall state change, when the measuring results are ignored. In this language the hypothesis of the lemma says that there is no overall state change through the device, i.e., 'no perturbation' of the system. The conclusion is that in that case the output probabilities are t_k, and independent of the input state, i.e., no information about the system is obtained.

As a first application, we conclude exactly as in the previous subsection that each convex component of the state ω again satisfies the teleportation equation. Hence we can once more assume that $\omega = |\Omega\rangle\langle\Omega|$ is a pure state. The argument that Ω is then uniquely determined by the other data, and hence that ω is pure is the same as in the dense coding case.

Clearly, this kind of argument is also useful for decompositions of T_x or F_x into sums of (completely) positive terms. To do this systematically, fix a maximally entangled unit vector Ξ, so that vectors in $\mathcal{H}\otimes\mathcal{H}$ become expressed as $\Phi = (A\otimes\mathbb{1})\Xi$ for a uniquely determined operator A (see equation (12)). In particular, we can write $\Omega = (W\otimes\mathbb{1})\Xi$, and the Kraus decomposition and spectral decomposition of each F_x in the form

$$T_x(A) = \sum_\alpha K_{x,\alpha}^* A K_{x,\alpha} \tag{17}$$

$$F_x = \sum_\beta (A_{x,\beta}\otimes\mathbb{1})|\Xi\rangle\langle\Xi|(A_{x,\beta}\otimes\mathbb{1})^*. \tag{18}$$

Inserting this into the teleportation equation (2) we find a sum over x, α, β, in which each term represents a completely positive operator, and which sum up to the identity. Hence by lemma 7, each term has to be multiple of the identity, $\tilde{\mu}_{x,\alpha,\beta}\mathrm{id}$, say. This can be written in terms of scalar products, if we take $\rho = |\phi_1\rangle\langle\phi_2|$ and $A = |\psi_1\rangle\langle\psi_2|$:

$$\begin{aligned}\tilde{\mu}_{x,\alpha,\beta}\,\mathrm{tr}(\rho A) &= \tilde{\mu}_{x,\alpha,\beta}\langle\phi_2,\psi_1\rangle\langle\psi_2,\phi_1\rangle\\ &= \langle\phi_2\otimes\Omega, (A_{x,\beta}\otimes\mathbb{1}\otimes K_{x,\alpha}^*)\Xi\otimes\psi_1\rangle\langle\Xi\otimes\psi_2, (A_{x,\beta}^*\otimes\mathbb{1}\otimes K_{x,\alpha})\phi_1\otimes\Omega\rangle.\end{aligned}$$

Note that the two scalar products on the right-hand side are complex conjugates of each other apart from a swapping of the arguments (ϕ_2,ψ_1) and (ψ_2,ϕ_1), which exactly matches the variable pairing on the left-hand side. Since the equation is to hold for arbitrary vectors $\phi_1, \phi_2, \psi_1, \psi_2$, we can hold one pair fixed and find that

$$\langle\phi_2\otimes\Omega, (A_{x,\beta}\otimes\mathbb{1}\otimes K_{x,\alpha}^*)\Xi\otimes\psi_1\rangle = \mu_{x,\alpha,\beta}\,\langle\phi_2,\psi_1\rangle, \tag{19}$$

where $\mu_{x,\alpha,\beta}$ is a factor determined in terms of $\tilde{\mu}$, and the scalar products involving (ψ_2,ϕ_1). With $\Omega = (W\otimes\mathbb{1})\Xi$, and equation (12) we get

$$\begin{aligned}&\langle\phi_2\otimes\Omega, (A_{x,\beta}\otimes\mathbb{1}\otimes K_{x,\alpha}^*)\Xi\otimes\psi_1\rangle\\ &\quad= \langle\phi_2\otimes(\mathbb{1}\otimes K_{x,\alpha})\Xi, (\mathbb{I}\otimes W^*\otimes\mathbb{1})((A_{x,\beta}\otimes\mathbb{1})\Xi\otimes\psi_1)\rangle\\ &\quad= \langle\phi_2\otimes(K_{x,\alpha}^T\otimes\mathbb{1})\Xi, (\mathbb{1}\otimes W^*\otimes\mathbb{1})((\mathbb{1}\otimes A_{x,\beta}^T)\Xi\otimes\psi_1)\rangle\\ &\quad= \langle\phi_2\otimes\Xi, (\mathbb{1}\otimes\overline{K_{x,\alpha}}W^*A_{x,\beta}^T\otimes\mathbb{1})\Xi\otimes\psi_1\rangle\\ &\quad\equiv \mu_{x,\alpha,\beta}\langle\phi_2,\psi_1\rangle\end{aligned}$$

where we have used the notation $\bar{K} = (K^*)^T$ for the matrix elementwise complex conjugation in the Schmidt basis belonging to the maximally entangled state Ξ. Since the above equation holds for all ϕ_2 and ψ_1, lemma 5 implies that

$$\overline{K_{x,\alpha}}W^*A_{x,\beta}^T = d\mu_{x,\alpha,\beta}\mathbb{1}, \tag{20}$$

for all x, α, β.

Let us say that a label $x\in X$ *contributes* to teleportation, if the corresponding term in the teleportation equation does not vanish for all ρ and A. This is equivalent to saying that for some α,β the factor $\mu_{x,\alpha,\beta}$ is non-zero. For such triples (x,α,β) all three operators on the left-hand side of equation (20) have to be invertible.

Now since there has to be at least one contributing label, W has to be non-singular, which means that Ω has *full Schmidt rank*. Equivalently, the reduced density operator ω_1 for the first factor has no zero eigenvalues. From this we conclude that the non-contributing labels are precisely those for which $F_x = 0$. Indeed, we may set $A = \rho = \mathbb{1}$, and use the normalization of T_x to find

$$0 = \mathrm{tr}((\mathbb{1}\otimes\omega)(F_x\otimes\mathbb{1})) = \mathrm{tr}((\mathbb{1}\otimes\omega_1)F_x)$$

Since $F_x \geqslant 0$, and $\mathbb{1}\otimes\omega_1$ has only strictly positive eigenvalues, this implies $F_x = 0$.

Now let x be a contributing index, and choose some triple (x, α, β) with $\mu_{x,\alpha,\beta} \neq 0$. If we now look at equation (20) for triples (x, α', β) with arbitrary α', we get $\overline{K_{x,\alpha'}} = (\mu_{x,\alpha',\beta}/\mu_{x,\alpha,\beta})\overline{K_{x,\alpha}}$, i.e., all Kraus operators of T_x are proportional, and hence T_x can be written with a single Kraus summand, $T_x(A) = U_x^* A U_x$, with a unitary U_x.

Similarly, we find that all $A_{x,\beta'}$ are proportional, which means that $F_x = |\Phi_x\rangle\langle\Phi_x|$ with $\Phi_x = (A_x \otimes \mathbb{1})\Xi$.

We can now apply lemma 2 to these vectors Φ_x, setting $\Phi_x = 0$ for non-contributing labels. The conclusion is that the Φ_x are an orthonormal basis. In particular, all indices do contribute after all.

Equation (20) and the unitarity of U_x allow us to express A_x in terms of U_x:

$$A_x = d\mu_x \, U_x \overline{W}^{-1} \, . \tag{21}$$

Orthonormality of the Φ_x becomes

$$\delta_{xy} = \frac{1}{d}\mathrm{tr}(A_x^* A_y) = d\overline{\mu_x}\mu_y \, \mathrm{tr}(U_y \overline{W}^{-1} (\overline{W}^{-1})^* \, U_x^*). \tag{22}$$

For $x = y$ we find that $|{\mu_x}^2|$ is independent of x, hence the operators $(\overline{\mu_x}/|\mu_x|)U_x^*$ are unitary, and satisfy the hypothesis of corollary 4 with ρ a positive multiple of $\overline{W}^{-1}(\overline{W}^{-1})^*$. Hence this operator is a multiple of the identity, W is unitary up to a factor, and $\Omega = (W \otimes \mathbb{1})\Xi$ is maximally entangled. Moreover, we see from equation (22) that the U_x form a unitary basis.

Since Ξ was an arbitrary maximally entangled vector, we may just as well take $\Xi = \Omega$, so equation (21) holds with $W = \mathbb{1}$. Hence, $\Phi_x = c \, (U_x \otimes \mathbb{1})\Omega$, where c is a factor which has to be of modulus 1, because Ω and Φ_x are normalized, and U_x is unitary, and which can be chosen to be 1 by adjusting the phase of Φ_x. This completes the proof.

4. Constructing bases of unitaries

It is not *a priori* clear that bases of unitary operators should exist in any dimension. Indeed, the system equation (5) of equations is formally overdetermined, according to the following rough dimension count. The variables in this system are the unitaries U_x, each of which we can take in the $(d^2 - 1)$-dimensional manifold SU_d, i.e., with $\det(U_x) = 1$, by fixing a phase factor. Since the transformations $U_x \mapsto V_1 U_x V_2$, for arbitrary $V_1, V_2 \in SU_d$ leave the set of solutions invariant, we may fix $U_1 = \mathbb{1}$, and take U_2 diagonal without loss of generality. This reduces the number of variables to $(d-1)+(d^2-2)(d^2-1)$. On the other hand, orthogonality introduces one complex constraint for every pair $x \neq y$. None of these is trivially satisfied due to the special choices we made, so we have to take $d^2(d^2 - 1)$ constraints into account. This leaves, formally,

$$\text{no of variables} - \text{no of equations} = -(d-1)(2d+1) < 0.$$

Of course, we know that this count is somehow too crude, because, after all, many inequivalent unitary bases are constructed below. But it is not so easy to spot the dependences among the constraints. Note also that the dimension count is essentially the same for bases orthogonal with respect to a weight $\rho \neq d^{-1}\mathbb{1}$, but in that case corollary 4 shows that there is no solution at all.

In order to describe the best known construction for unitary bases [VW], let us introduce some terminology. We say that a (single) unitary matrix is of *shift and multiply* type, if it is the product of a permutation operator and a diagonal unitary. In other words, every row or column contains $(d-1)$ zero entries, and one entry of modulus 1. The bases we will construct not only have the property that each element is of this type, but also that the d^2 values for x can be split into d options for 'shift' and d options for 'multiply'.

Definition 8. *A **shift and multiply basis** of unitary matrices in $\mathbb{C}^d$ is a collection of d^2 unitary operators $U_{ij}, i, j \in I_d \equiv \{1, \ldots, d\}$, satisfying the orthogonality relation $\mathrm{tr}(U_{ij}^* U_{k\ell}) = d\ \delta_{ik}\delta_{j\ell}$, and acting on the basis vectors $|k\rangle$ as*

$$U_{ij}|k\rangle = H_{ik}^j |\lambda(j,k)\rangle \tag{23}$$

where these H_{ik}^j are complex numbers, and $\lambda : I_d \times I_d \to I_d$.

Proposition 9. *The parameters and $\lambda : I_d \times I_d \to I_d$ define a shift and multiply basis of unitary matrices if and only if the following two conditions are satisfied:*

(1) *Each H^j is a **Hadamard matrix**, i.e. $|H_{ik}^j| = 1$ for all i, k, and $H^j (H^j)^* = d\mathbb{1}$.*
(2) *λ is a **Latin square**, i.e., the maps $k \mapsto \lambda(k, \ell)$ and $k \mapsto \lambda(\ell, k)$ are injective for every ℓ.*

Proof. For U_{ij} to be unitary, it is necessary and sufficient that the H_{ik}^j are phases, and that $k \mapsto \lambda(j, k)$ is injective (hence bijective) for every j. For the orthogonality we have to evaluate

$$\mathrm{tr}(U_{ij}^* U_{i'j'}) = \sum_k \overline{H_{ik}^j} H_{i'k}^{j'} \langle \lambda(j,k)|\lambda(j',k)\rangle.$$

We consider first the case $j = j'$. Then the scalar products in the sum are all equal to 1, and equating this expression to $\delta_{ii'}$ we find that H^j is Hadamard.

Now let $j \neq j'$, and consider the 'coincidence set' $C = \{k|\lambda(j,k) = \lambda(j',k)\}$. Then orthogonality requires, for every i, i', that

$$0 = \sum_{k\in C} \overline{H_{ik}^j} H_{i'k}^{j'} = \sum_{k=1}^{d} H_{i'k}^{j'}\ \chi_C(k)\ (H^{j*})_{ki} = (H^{j'} \chi_C H^{j*})_{i'i}, \tag{24}$$

where $\chi_C(k) = 1$ for $k \in C$, and zero otherwise, and in the last line χ_C denotes the projection $\chi_C|k\rangle = \chi_C(k)|k\rangle$. But since $H^{j'}$ and H^j are Hadamard, and in particular invertible, this implies $\chi_C = 0$. Hence C is empty, and the second injectivity of λ is proved. □

In order to construct unitary bases of this form, we must now construct Hadamard matrices and Latin squares of the appropriate dimension. For both of these tasks there is a rich literature, and below we will give a brief summary on what is known for each.

It is useful to note that each of the structures 'unitary bases', 'Hadamard matrices' and 'Latin squares' has a natural notion of *equivalence*, and to some extent these equivalences are related. We call two unitary bases U, U' equivalent, if $U'_x = V_1 U_{x'} V_2$, for some unitaries V_1, V_2, and a relabelling $x \mapsto x'$. Hadamard matrices are called equivalent, if one is obtained from the other by permuting rows or columns, or multiplying rows or columns with phases. Finally, a Latin square $\lambda : I_d \times I_d \to I_d$ is equivalent to any other obtained by applying a permutation on each of the three copies of I_d involved. In each case there are also discrete transformations, such as transposition or complex conjugation (where applicable). It should be noted that replacing each H^j by an equivalent one, typically only leads to an equivalent unitary basis, if the equivalence operation is the same for each j. With j-dependent equivalence transformations it is possible to construct inequivalent unitary bases in $d = 3$, although in this dimension there is only one Hadamard matrix and only one Latin square—up to equivalence. Of course, in $d = 2$ all three structures, including the unitary bases, are unique up to equivalence [VW]. The unique unitary basis is then given by the three Pauli matrices and the identity and, of course generates, via theorem 1, the usual two qubit examples of teleportation and dense coding.

For each of the three structures we furthermore have an obvious notion of *tensor product*, allowing the construction of a unitary basis (resp. a Hadamard matrix or Latin square) in dimension $d = d_1 d_2$, if counterparts in dimension d_1 and dimension d_2 are given.

In order to show that unitary bases exist in any dimension it is easiest to use group-theory-based constructions: the Latin square can be taken as the multiplication table of any group of order d, for example the cyclic group. The Hadamard matrix can be taken as the matrix implementing the Fourier transform on an Abelian group of order d, the standard example being given once again by the cyclic group of order d. Thus $H_{k\ell} = \exp(\frac{2\pi \mathrm{i}}{d} k\ell)$, where k and ℓ are taken modulo d. If we combine these data into a unitary basis we get an instance of what we propose to call a *unitary basis of group type* ('nice error basis' in [Kn]). These are orthonormal unitary bases with the additional property that the operator product of any two elements is a third, up to a phase. That is to say, the index set X is a group, and

$$U_x U_y = \mu(x, y) U_{xy} \tag{25}$$

with $|\mu(x, y)| = 1$. In the special case of an Abelian group X this is a discrete version of *Weyl systems* of unitary operators, named after their continuous variable counterpart, well-known from quantum optics and non-relativistic 'phase space' quantum mechanics.

Latin squares are not completely classified, nor does there seem to be a realistic hope to do so. A standard work on the subject is [DK], a useful net resource is [Ri]. Counts of squares are usually done for 'normalized squares', in which the first row and column are in natural order, thus eliminating some trivial freedom. In $d = 5$ Euler counted 56 of these, but only 2 are inequivalent, because the symbols themselves can also be permuted. Counts of normalized squares have now gone all the way up to $d = 10$, but are no longer done by hand (there are roughly 7.5×10^{24} [MR]. It is also clear from these numbers that group based constructions exhaust only a tiny fraction of the possible unitary bases.

Hadamard matrices are also a standard subject in coding theory. However, usually only the real case (orthogonal matrices with entries ± 1) is considered. It is easy to see that real Hadamard matrices exist only in dimension two and multiples of four. Again, the possibilities for such designs by far exceed the group based possibilities (the characters of an Abelian group are real only if $d = 2^n$). A standard reference is [Ag].

For complex Hadamard matrices the Fourier matrices show that there is no constraint on dimension. The uniqueness in $d = 3$ is easy to get. The general form in $d = 4$ is, up to equivalence

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & u & -u \\ 1 & -1 & -u & u \end{pmatrix} \tag{26}$$

where u is an arbitrary phase. For $u = 1$ this is equivalent to the Fourier matrix of 'Klein's Four Group', the product of two copies of the two-element group, and for $u = i$ it is equivalent to the Fourier matrix of the cyclic group. The possibility of embedding the cyclic group Fourier matrix into a higher dimensional manifold can be generalized to arbitrary composite numbers $d = pq$: whenever $V_{k\ell}$ is a matrix of phases satisfying the periodicity conditions $V_{k,\ell} = V_{k+p,\ell} = V_{k,\ell+q}$, we get a Hadamard matrix as

$$H_{k\ell} = V_{k\ell} \exp\left(\frac{2\pi \mathrm{i}}{d}\, k\ell\right). \tag{27}$$

One might conjecture from this that for prime orders d the Hadamard matrix is unique. This problem was discussed by Haagerup [Ha] on the basis of a completely different motivation (theory of von Neumann algebras). There it is shown that for $d = 5$ there is uniqueness, but for $d = 7$ there are at least five solutions. For some primes, uncountably many inequivalent Hadamard matrices are known.

References

[Ag] Agaian S S *Hadamard Matrices and Applications* (*Lecture Notes in Mathematics 1168*) (Berlin: Springer)

[BB] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9

[BW] Bennett C H and Wiesner S J 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states *Phys. Rev. Lett.* **69** 2881–4

[BD] Braunstein S L, D'Ariano G M, Milburn G J and Sacchi M F 2000 Universal teleportation with a twist *Phys. Rev. Lett.* **84** 3486
(Braunstein S L, D'Ariano G M, Milburn G J and Sacchi M F 1999 *Preprint* quant-ph/9908036)

[Cr] Craigen R 1991 Equivalence classes of inverse orthogonal and unit Hadamard matrices *Bull. Aust. Math. Soc.* **44** 109–15

[Da] Davies E B 1976 *Quantum Theory of Open Systems* (New York: Academic)

[DK] Dénes J and Keedwell A D 1991 *Latin Squares—New Developments in the Theory and Applications* (Amsterdam: North-Holland)

[Ha] Haagerup U 1997 Orthogonal maximal abelian*-subalgebras of the $n \times n$-matrices and cyclic n-roots *Operator Algebras and Quantum Field Theory (Rome, 1996)* (International Press) pp 296–322

[Kn] Knill E 1996 Group representations, error bases and quantum codes (preliminary report) *Preprint* quant-ph/9608049

[Pa] Paulsen V I 1986 *Completely Bounded Maps and Dilations* (London: Longman Scientific and Technical)

[Ri] Ritter T Latin Squares, a literature survey http://www.io.com/˜ritte/RES/LATSQ.HTM

[MR] McKay B and Rogoyski E 1995 Latin squares of order 10 *El. J. Combinatorics* **2** 1–4

[VW] Vollbrecht K G H and Werner R F 2000 Why two qubits are special *J. Math. Phys.* **41** 6772
(Vollbrecht K G H and Werner R F 1999 *Preprint* quant-ph/9910064)

[Wa] Wallis J 1973 Complex Hadamard matrices *Lin. Multilin. Algebra* **1** 257–72