Designs, Codes and Cryptography, 29, 51–70, 2003
© 2003 Kluwer Academic Publishers. Manufactured in The Netherlands.

A New Class of Designs Which Protect against Quantum Jumps

THOMAS BETH
Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany

CHRISTOPHER CHARNES
Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany
Department of Computer Science & Software Engineering, University of Melbourne, Parkville, Vic 3052, Australia

MARKUS GRASSL
Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany

GERNOT ALBER
Abteilung für Quantenphysik, Universität Ulm, 89069 Ulm, Germany

ALDO DELGADO
Abteilung für Quantenphysik, Universität Ulm, 89069 Ulm, Germany

MICHAEL MUSSINGER
Abteilung für Quantenphysik, Universität Ulm, 89069 Ulm, Germany

Communicated by: A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, J. A. Thas

Abstract. We present the theory and construction of a new class of designs, which we call SEEDs (spontaneous emission error designs), arising in the study of decay processes of certain quantum systems used in the newly emerging field of quantum computing. We show that there is a simple and surprising connection between subspaces of the system Hilbert space, stable against these quantum jumps and the incidence matrices of SEEDs.

Keywords: quantum error correction, resolvable designs, partial designs, large sets

1. Introduction

The phenomenon of "Quantum Jumps" is an aspect of nature which made Max Planck coin the term Quantum Mechanics about a century ago. It has since exercised a rather undesirable effect; limiting the controllable use of Quantum Systems in many areas of science, engineering, communications, and computing. In a recent paper [1] a surprising connection between the physical jump operator of certain quantum systems and the derivation operator of incidence structures was discovered. Quantum systems to which these results can be applied encompass the new and promising field of quantum computation. In this paper the universal concept of a quantum computer will be used as a mathematical model for describing the relations between physical processes and certain methods of combinatorial mathematics.

These close connections have only been discovered during the last few years, although the foundations for the field of quantum computation were laid by Richard Feynman, Paul Benioff, and Yuri Manin already in the early 80s by studying the relationship between the physical and computational processes. Starting from the observation that quantum mechanical processes are hard to simulate on classical computers, they concluded that quantum mechanics might help to speed-up some computations. After preliminary results which were mainly of a theoretical nature, Peter Shor presented an algorithm of practical interest for a computer based on the principles of quantum mechanics [30]. His quantum algorithm for factoring integers is exponentially faster than any classical algorithm known so far.

However quantum computation would still remain in the theoretical domain if there had not been proposals for the physical realisation of quantum computers, see e.g., [12,13,18, 28]. Nevertheless, another obstacle appeared along the way to the realization of quantum computers.

The quantum computer is modeled as a closed system that is isolated from its environment. But in contrast to classical systems, quantum mechanical systems are much more sensitive to disturbances from the environment, e.g., by electro-magnetic fields and radiation. Initially it was believed that there was no way to circumvent this problem by using error correction since arbitrary quantum states cannot be replicated [35]. Again it was Shor who showed that even in the quantum setting error correction is possible [31].

His work initiated a lot of research establishing a theory of quantum error correction. Independently, Steane [33,34] and Calderbank and Shor [10] came up with methods to construct quantum error-correcting codes from classical linear binary codes. Then, Gottesman [19] and Calderbank [9] presented different approaches to generalise the construction of quantum error-correcting codes, but yielding the very same codes. The general conditions for quantum error-correcting codes have been studied by Ekert and Macchiavello [16], and later were extended by Knill and Laflamme [25].

This paper is organised as follows. The ideas of quantum information processing including quantum error correction are summarised in Section 2. In Section 3 we introduce the notion of jump codes, followed by a discussion of the bounds on these codes. In Section 5 we explore the connection between t-SEEDs and jump codes. We then look at the constructions of t-SEEDs which arise from finite geometries in Section 6 and from isodual codes in Section 7. Finally, we give some further constructions of jump codes in Section 8, closing with some open questions in the conclusion.

2. Basics of Quantum Information Processing

2.1. Quantum Information & Quantum Computation

From an abstract point of view, quantum information processing is based on the mathematical framework of quantum mechanics. Ideally, the state of a quantum mechanical system is represented by a unit length vector in a complex Hilbert space $\mathcal{H}$. In the context of quantum information processing, the Hilbert space $\mathcal{H}$ usually has finite dimension. Following [15], the elements of $\mathcal{H}$ are denoted by the so-called ket vectors $|\psi\rangle$, while the elements of the dual space are denoted by bra vectors $\langle\psi|$. The smallest non-trivial example occurs when $\mathcal{H}$ is a two-dimensional space, i.e., $\mathcal{H} \cong \mathbb{C}^2$. Similar to *classical* bits, the states of an orthonormal basis of $\mathbb{C}^2$ are denoted by $|0\rangle$ and $|1\rangle$. An arbitrary state of $\mathcal{H} \cong \mathbb{C}^2$, known as *quantum bit* or *qubit* is given by

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } |\alpha|^2 + |\beta|^2 = 1, \alpha, \beta \in \mathbb{C}. \tag{1}$$

The joint state of a quantum system composed of n physically distinguishable subsystems is modeled by the tensor product of the Hilbert spaces of the subsystems, i.e., $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$. For an n qubit quantum system, the elements of the canonical basis are of the form

$$|b_1 \cdots b_n\rangle := |b_1\rangle\,|b_2\rangle \cdots |b_n\rangle := |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle$$

where $b_i \in \{0, 1\}$. Hence, an arbitrary state of an n qubit quantum system is given by

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x\,|x\rangle\,, \quad \text{where} \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1, \alpha_x \in \mathbb{C}. \tag{2}$$

If more than one coefficient α_x is non-zero, such a state is called a *superposition* of the states with non-zero coefficients. Two quantum states that differ only by a factor of modulus 1 cannot be distinguished. Hence, the state of a quantum mechanical system can be identified with the (complex) ray $c\,|\psi\rangle$ where $c \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ or any representative of that ray.

Quantum information is processed by means of unitary transformations, while the final read-out corresponds to a measurement. It has been shown that in order to implement an arbitrary unitary transformation it is sufficient to operate on a fixed number of subsystems in each step of the computation [2]. Similarly, it is sufficient to measure each of the subsystems individually with respect to fixed bases. Mathematically, that measurement corresponds to a probabilistic projection onto either the space spanned by $|0\rangle$ or by $|1\rangle$. If the state before the measurement is given by (1), then the state after the measurement is

$$|0\rangle \text{ with probability } |\alpha|^2 \quad \text{or} \quad |1\rangle \text{ with probability } |\beta|^2 \tag{3}$$

2.2. Quantum Error Correction

2.2.1. Error-Correcting Codes

A basic principle of quantum information processing is the possibility to perform computations *in superposition* and to use constructive or destructive interference to amplify or to suppress different computational paths. In *real* quantum mechanical systems, however, superpositions and coherence—which is necessary for interference—may be disturbed due to interaction with the environment. Therefore, some means of error-correction are required. As unknown quantum information cannot be copied [35], the *classical* approach using redundancy by replicating the quantum information does not apply. Instead, quantum information has to be encoded in a suitable chosen subspace $\mathcal{C}$ of a larger Hilbert space $\mathcal{H}$. Of course, the way the subspace $\mathcal{C}$ is chosen strongly depends on the error model. An example is the so-called *depolarising* channel which transmits a quantum state undisturbed with probability $1-p$ and outputs a random quantum state (uniformly distributed) with probability p, reflecting a uniform symmetric channel. Although quantum information is continuous, it is sufficient to be able to correct a discrete set of errors, e.g., the *error basis* [24]. The complete characterization of quantum error-correcting codes in terms of error operators is given by the following theorem of Knill and Laflamme [25]:

THEOREM 1. *A subspace $\mathcal{C} \leq \mathcal{H}$ with orthonormal basis $\{|c_i\rangle : i = 1, \dots, K\}$ is a quantum error-correcting code for the set of error operators $\mathcal{E} = \{A_i : i = 1, \dots, L\}$ if and only if the following holds:*

$$\begin{aligned} &(i)\ \ \forall i \neq j \forall k, \ell\colon \langle c_i | A_k^\dagger A_\ell | c_j\rangle = 0 \\ &(ii)\ \ \forall i, j \forall k, \ell\colon \langle c_i |\, A_k^\dagger A_\ell \,| c_i\rangle = \langle c_j | A_k^\dagger A_\ell | c_j\rangle. \end{aligned} \tag{4}$$

In the case of qubits, an error basis is given by the identity and the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The algebraic structure of the Pauli matrices directly links quantum error-correcting codes and self-orthogonal codes over $\mathbb{F}_4$ [4,8]. There are also relations to orthogonal geometry [7].

2.2.2. *Quantum Jumps*

As for classical codes, further side-information, e.g., about the position of an error, might aid in the process of error-correction [21]. In this paper we consider the error model where errors are due to quantum jumps, i.e., the (excited) state $|1\rangle$ may spontaneously decay into the (ground) state $|0\rangle$ [27]. Furthermore, we assume that the decay rate is equal for all subsystems, i.e., independent of the position. Then the corresponding error operator is given by

$$a := |0\rangle\,\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

If the operator acts only on the ith subsystem, the following notation will be used:

$$J_i := a_i := \mathrm{id} \otimes \cdots \otimes \mathrm{id} \otimes |0\rangle\,\langle 1| \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id}. \tag{5}$$

Hence, with some probability a quantum state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is changed into the state $|0\rangle$, erasing all quantum information. Of course, if the initial state is $|\psi\rangle = |0\rangle$, i.e.,

$\beta = 0$, then a jump cannot occur. But note that, in contrast to the measurement process (3), the probability of a jump does not depend on α and β in general.

Physically, the decay process is accompanied by the emission of some quanta, e.g., photons. By continuously monitoring the system one can obtain information about which qubit encountered a quantum jump [1]. Not surprisingly in the context of quantum mechanics, continuously monitoring the quantum system has a side effect on the quantum system itself. Even when no quantum jump occurs, the state of the system is changed due to monitoring. Ignoring normalisation, the dynamics of the system starting in the state $|\psi(t_0)\rangle$ is given by [1]

$$|\psi(t)\rangle = \exp\left(-\kappa/2 \cdot (t-t_0) \sum_{i=1}^{n} a_i^\dagger a_i\right) |\psi(t_0)\rangle \tag{6}$$

$$= \exp\left(-\kappa/2 \cdot (t-t_0) \sum_{i=1}^{n} |1\rangle_i \langle 1|_i\right) |\psi(t_0)\rangle . \tag{7}$$

3. Jump Codes

After these preliminaries are ready to introduce the notion of a t-error protecting jump code. We stress again that in the above model we assume the existence of an observer monitoring the decay channel with a 100% effective measurement. Therefore the set of locations $E = \{x_1, \ldots, x_e\}$ of the qubits, at which the jump error occurred is known due to the observation of spontaneous emissions; see [1].

From equation (7) it follows that between quantum jumps, the state is modified by the time dependent operator (setting $t_0 = 0$)

$$A_0(t) := \exp\left(-\kappa/2 \cdot t \sum_{i=1}^{n} |1\rangle_i \langle 1|_i\right) .$$

The error operator $A_0(t)$ acts on a state $|c_i\rangle$ of an n qubit system of the form (2) as

$$A_0(t)\,|c_i\rangle = \sum_{x\in\{0,1\}^n} e^{-\kappa/2 \cdot t \operatorname{wgt} x} \alpha_x\,|x\rangle$$

where $\operatorname{wgt} x$ denotes the Hamming weight of the binary word x. From condition (4) we obtain

$$\langle c_i|\,A_0(t)^\dagger A_0(t)\,|c_i\rangle = \sum_{x\in\{0,1\}^n} |\alpha_x|^2 e^{-\kappa \cdot t \operatorname{wgt} x} \tag{8}$$

$$= \sum_{w=0}^{n} e^{-\kappa \cdot t w} \sum_{\operatorname{wgt} x = w} |\alpha_x|^2.$$

As (8) must be independent of the state $|c_i\rangle$, the length $\sum_{\operatorname{wgt} x=w} |\alpha_x|^2$ of the projection of $|c_i\rangle$ onto the space spanned by the states $|x\rangle$ with constant Hamming weight w must be constant. Furthermore, if the code $\mathcal{C}$ is at least two-dimensional, this is possible if and only if all the states $|c_i\rangle$ are superpositions of basis states with constant Hamming weight.

Introducing the notation

$$\left|\binom{V}{w}\right\rangle\left\langle\binom{V}{w}\right| := \sum_{\substack{x \in \{0,1\}^n \\ \operatorname{wgt} x = w}} |x\rangle\langle x| \tag{9}$$

for $V = \{1, \dots, n\}$, we obtain the condition

$$\forall i \colon \left\langle c_i \middle| \binom{V}{w} \right\rangle \left\langle \binom{V}{w} \middle| c_i \right\rangle = \langle c_i | c_i \rangle = 1.$$

Note that the diagonal of the operator (9) can be interpreted as the length 2^n incidence vector of all $\binom{n}{w}$ w-subsets of V when each basis state $|x\rangle$ is interpreted as the incidence vector of a particular subset $X \subset V$. Similarly, we use the notation

$$|2^V/2^E\rangle\langle 2^V/2^E| := \sum_{E \subseteq X \subseteq V} |x\rangle\langle x| \tag{10}$$

for the length 2^n incidence vector of the sublattice $2^V/2^E$ of all subsets containing E.

In order to correct $0 \le s \le t$ errors caused by jumps at known positions $E = \{x_1, \dots, x_s\}$, the basis of the code $\mathcal{C}$ must fulfill conditions (4) for the error operators A_k of the form

$$A_0(t_s) \cdot a_{x_s} \cdot A_0(t_{s-1}) \cdot \ldots \cdot a_{x_2} \cdot A_0(t_1) \cdot a_{x_1} \cdot A_0(t_0).$$

Recall that equation (8) implies that all states of the code are superpositions of basis states with constant Hamming weight. Furthermore, a single quantum jump decrements the Hamming weight of all basis states by one. Hence it is sufficient to consider only the error operator $A_0(t)$ and multiple-jump operators of the form

$$J_E := a_{x_s} \cdot \ldots \cdot a_{x_2} \cdot a_{x_1}.$$

As the positions of the errors are assumed to be known, it is not necessary to consider combinations of error operators J_E and $J_{E'}$ with $E \neq E'$. Hence, condition (4) simplifies to

$$\begin{aligned} &\text{(i)} \quad \forall i \neq j \colon \langle c_i | J_E^\dagger J_E | c_j \rangle = 0 \\ &\text{(ii)} \quad \forall i, j \colon \langle c_i | J_E^\dagger J_E | c_i \rangle = \langle c_j | J_E^\dagger J_E | c_j \rangle \end{aligned} \tag{11}$$

for all $E \subset V$, $|E| \le t$. Using the notation introduced in (10), we finally obtain

$$\begin{aligned} &\text{(i)} \quad \forall i \neq j \colon \langle c_i | 2^V/2^E \rangle \langle 2^V/2^E | c_j \rangle = 0, \\ &\text{(ii)} \quad \forall i, j \colon \langle c_i | 2^V/2^E \rangle \langle 2^V/2^E | c_i \rangle = \langle c_j | 2^V/2^E \rangle \langle 2^V/2^E | c_j \rangle. \end{aligned} \tag{12}$$

Note that it is not sufficient that orthogonal states remain orthogonal after quantum jumps (condition (i) in (12)). Additionally, upon projection by a jump operator the states have to be renormalised with the very same scalar (condition (ii) in (12)). This surprising observation provides an example where the linearity of quantum mechanics requires the consideration of a projective argument. Namely that the conditional reconstruction operator must be a *central linear transformation* of the code space.

To prove this assertion let $|c_i\rangle$, for $i = 1, \dots, K$, be an ONB of an K-dimensional subspace $\mathcal{C}$ to be protected against jumps errors J_E of weight at most t. Then for any ONB $|\phi_j\rangle$ of states

$$|\phi_j\rangle = \sum_{i=1}^{K} \alpha_{ij} \, |c_i\rangle$$

to be protected, we must have that $|\phi'_j\rangle = J_E|\phi_j\rangle$ form an orthogonal basis of $J_E\mathcal{C}$. Thus for the matrix $C = \sum_{k=1}^{K} |c_k\rangle \, \langle k|$ (corresponding to the encoding (13)) and any unitary matrix $A = \sum \alpha_{ij} \, |i\rangle \, \langle j|$ we must have that

$$A^\dagger C^\dagger I_E C A$$

is diagonal, where I_E is the matrix $I_E := |2^V/2^E\rangle\langle 2^V/2^E|$ (cf. (10)). By Schur's lemma, this is only possible iff

$$C^\dagger I_E C = \lambda(E) I_{K\times K}$$

for some non-negative real $\lambda(E)$.

We can now define a quantum error-correcting code which protects against at least t detected quantum jumps:

Definition 2. A t-detected-jump-error correcting quantum code (short: jump code) $\mathcal{C} = (n, K, t)_w$ encoding K orthogonal basis states $|i\rangle$ ($i = 0, \dots, K-1$) using n qubits corresponds to a mapping

$$|i\rangle \longmapsto |c_i\rangle \in (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n} \tag{13}$$

where the $|c_i\rangle$ fulfill the properties

(i) $\langle c_i| \binom{V}{w}\rangle\langle\binom{V}{w}|c_i\rangle = \langle c_i|c_i\rangle = 1$

(ii) For all $s = 0, \dots, t$ and for all $T \in \binom{V}{s}$ there exists a constant $\lambda(T)$ such that

$$\langle c_i|\, 2^V/2^T\rangle\langle 2^V/2^T|c_j\rangle = \lambda(T)\delta_{ij}.$$

The first condition assures that all states are superpositions of basis states $|x\rangle$ with Hamming weight $\operatorname{wgt} x = w$. The second condition combines the requirements of (12).

The above conditions are summarised as

THEOREM 3. *Given a jump code $\mathcal{C} = (n, K, t)_w$, then any s-jump error for $0 \le s \le t$ in the n-qubit monitored decay channel can be corrected.*

4. Bounds

4.1. General Bounds

Before we discuss bounds on the parameters of jump codes, we state some useful properties. First, we consider the *binary complement* of a jump code.

LEMMA 4. *If $\mathcal{C}$ is a jump code on n qubits correcting t jump errors, then $\sigma_x^{\otimes n}\mathcal{C}$ can also correct at least t jump errors. In particular, if a jump code $\mathcal{C} = (n, K, t)_w$ exists, then there is also a jump code $\overline{\mathcal{C}} = (n, K, t)_{n-w}$.*

Proof. For a fixed code, the set of correctable erasures (resp. detectable errors) is a linear vector space of operators [20]. A jump code can detect both the local qubit error operators identity I_2 and $a^\dagger a = |1\rangle\langle 1|$. The linear vector space generated by these two operators is invariant under conjugation by σ_x. Furthermore, $\sigma_x^{\otimes n}$ maps the symmetric space of Hamming weight w onto the symmetric space of Hamming weight $n - w$. ■

Next we consider shortening and lengthening operations.

LEMMA 5. *If a jump code $\mathcal{C} = (n, K, t)_w$ exists for $w > t > 1$, then exists also a jump code $\mathcal{C}' = (n-1, K, t-1)_{w-1}$.*

Proof. The code $\mathcal{C}'$ is obtained by applying a jump operator at a position of $\mathcal{C}$ which is not constantly zero and then deleting that position. ■

LEMMA 6. *If a jump code $\mathcal{C} = (n, K, t)_w$ exists, then exist also jump codes $\mathcal{C}0 = (n+1, K, t)_w$ and $\mathcal{C}1 = (n+1, K, t)_{w+1}$.*

Proof. The codes $\mathcal{C}0$ and $\mathcal{C}1$ are obtained by tensoring a qubit $|0\rangle$ resp. $|1\rangle$ to $\mathcal{C}$. ■

Next, we derive a straightforward upper bound on the dimension of a jump code.

LEMMA 7. *The dimension K of a jump code $\mathcal{C} = (n, K, t)_w$ is bounded from above by*

$$K \le \min\left\{\binom{n-t}{w-t}, \binom{n-t}{w}\right\}. \tag{14}$$

Proof. The dimension of the space of all words of length n and Hamming weight w is $\binom{n}{w}$. This implies the bound $K \le \binom{n}{w}$. A jump on j positions reduces the Hamming weight to $w - j$. After the jump, the j positions of the jump are zero. There are $\binom{n-j}{w-j}$ such words. A jump may not reduce the dimension of the code, hence $K \le \binom{n-j}{w-j}$. The minimal value is achieved for $j = t$, as

$$\binom{n}{w} = \frac{n}{w}\binom{n-1}{w-1} = \frac{n(n-1)\cdots(n-t+1)}{w(w-1)\cdots(w-t+1)}\binom{n-t}{w-t}.$$

Using the same argument for the complemented code $\overline{\mathcal{C}} = (n, K, t)_{n-w}$ (cf. Lemma 4) yields the upper bound

$$K \le \binom{n-t}{(n-w)-t} = \binom{n-t}{w}.$$

■

If we are free to choose the Hamming weight w of the states of a jump code, we get the following bound.

LEMMA 8. *The upper bound of Lemma 7 is maximal for $w = \lfloor n/2 \rfloor$, i. e.,*

$$K \leq \binom{n-t}{\lfloor n/2 \rfloor - t}. \tag{15}$$

Proof. Consider the function $f(x) := \binom{n-t}{x}$. In the interval $0 \leq x \leq (n-t)/2$, $f(x)$ is increasing, and decreasing in the interval $(n-t)/2 \leq x \leq n-t$. Furthermore, $f(x)$ has the symmetry $f(n-t-x) = f(x)$.

For $n = 2\nu$ even, $f(\nu) = f(\nu - t)$ and the bound (14) is maximal for $w = \nu$. For $n = 2\nu + 1$ odd, using $\nu \geq (n-t)/2$ and $\nu - t \leq (n-t)/2$ we get $f(\nu) \geq f(\nu+1) = f(\nu - t) \leq f(\nu + 1 - t)$. Again, the bound (14) is maximal for $w = \nu$. ■

An optimal code, i.e., a code achieving this upper bounds, exists for $t = 1$ and even length [1]:

COROLLARY 9. *For even length n, the $(n, \frac{1}{2}\binom{n}{n/2}, 1)_{n/2}$ jump code with basis states $1/\sqrt{2}(|x\rangle + |\overline{x}\rangle)$ (where $\overline{x}$ denotes the binary complement of the bitstring x) is optimal.*

4.2. *Specific Bounds*

LEMMA 10. *There is no jump code $\mathcal{C} = (5, 4, 1)_w$.*

Proof. For $n = 5$ and $t = 1$, lemma 7 yields a maximal upper bound $K \leq 4$ for $w = 2$ or $w = 3$. Using Lemma 4, it is sufficient to consider only the case $w = 2$.

Let $\{|c_1\rangle, |c_2\rangle, |c_3\rangle, |c_4\rangle\}$ be an ONB of $\mathcal{C} = (5, 4, 1)_2$. If all $|c_i\rangle$ were of the form $|c_i\rangle = |0\rangle|c_i'\rangle$, then $\{|c_i'\rangle\}$ would be an ONB of a jump code $\mathcal{C}' = (4, 4, 1)_2$. But for $n = 4$ and $t = 1$, the upper bound (15) is 3. So the first qubit is not constantly zero. Hence we can apply a jump to the first qubit. Then $J_1\mathcal{C}$ is a 4-dimensional subspace of the space with basis $\{|01000\rangle, |00100\rangle, |00010\rangle, |00001\rangle\}$. From (12) it follows that the states $J_1\,|c_i\rangle$ are proportional to an ONB. Hence we can assume

$$J_1\,|c_1\rangle = \alpha\,|01000\rangle \qquad J_1\,|c_3\rangle = \alpha\,|00010\rangle$$
$$J_1\,|c_2\rangle = \alpha\,|00100\rangle \qquad J_1\,|c_4\rangle = \alpha\,|00001\rangle$$

with $\alpha \in \mathbb{R}$ and $\alpha > 0$. Then, the ONB of the code can be written as

$$\begin{aligned}
|c_1\rangle = \alpha\,|11000\rangle &+ \beta_{11}\,|01100\rangle + \beta_{12}\,|01010\rangle + \beta_{13}\,|01001\rangle \\
&+ \beta_{14}\,|00110\rangle + \beta_{15}\,|00101\rangle + \beta_{16}\,|00011\rangle, \\
|c_2\rangle = \alpha\,|10100\rangle &+ \beta_{21}\,|01100\rangle + \beta_{22}\,|01010\rangle + \beta_{23}\,|01001\rangle \\
&+ \beta_{24}\,|00110\rangle + \beta_{25}\,|00101\rangle + \beta_{26}\,|00011\rangle,
\end{aligned}$$

$$\begin{aligned}|c_3\rangle = \alpha\,|10010\rangle \;&+\; \beta_{31}\,|01100\rangle + \beta_{32}\,|01010\rangle + \beta_{33}\,|01001\rangle\\ &+\; \beta_{34}\,|00110\rangle + \beta_{35}\,|00101\rangle + \beta_{36}\,|00011\rangle,\\ |c_4\rangle = \alpha\,|10001\rangle \;&+\; \beta_{41}\,|01100\rangle + \beta_{42}\,|01010\rangle + \beta_{43}\,|01001\rangle\\ &+\; \beta_{44}\,|00110\rangle + \beta_{45}\,|00101\rangle + \beta_{46}\,|00011\rangle.\end{aligned}$$

A jump on the second qubit results in

$$\begin{aligned}J_2\,|c_1\rangle &= \alpha\,|10000\rangle + \beta_{11}\,|00100\rangle + \beta_{12}\,|00010\rangle + \beta_{13}\,|00001\rangle,\\ J_2\,|c_2\rangle &= \beta_{21}\,|00100\rangle + \beta_{22}\,|00010\rangle + \beta_{23}\,|00001\rangle,\\ J_2\,|c_3\rangle &= \beta_{31}\,|00100\rangle + \beta_{32}\,|00010\rangle + \beta_{33}\,|00001\rangle,\\ J_2\,|c_4\rangle &= \beta_{41}\,|00100\rangle + \beta_{42}\,|00010\rangle + \beta_{43}\,|00001\rangle.\end{aligned}$$

The vector $\beta_{11}\,|00100\rangle + \beta_{12}\,|00010\rangle + \beta_{13}\,|00001\rangle$ must be orthogonal to the three linear independent vectors $J_2\,|c_i\rangle$ for $i = 2, 3, 4$. Hence $\beta_{11} = \beta_{12} = \beta_{13} = 0$. Considering jumps at positions 3–5, by symmetry we get

$$\begin{aligned}\beta_{21} &= \beta_{24} = \beta_{25} = 0,\\ \beta_{32} &= \beta_{34} = \beta_{36} = 0,\\ \beta_{43} &= \beta_{45} = \beta_{46} = 0.\end{aligned}$$

The ONB of the code has now the form

$$\begin{aligned}|c_1\rangle &= \alpha\,|11000\rangle + \beta_{14}\,|00110\rangle + \beta_{15}\,|00101\rangle + \beta_{16}\,|00011\rangle\\ |c_2\rangle &= \alpha\,|10100\rangle + \beta_{22}\,|01010\rangle + \beta_{23}\,|01001\rangle + \beta_{26}\,|00011\rangle\\ |c_3\rangle &= \alpha\,|10010\rangle + \beta_{31}\,|01100\rangle + \beta_{33}\,|01001\rangle + \beta_{35}\,|00101\rangle\\ |c_4\rangle &= \alpha\,|10001\rangle + \beta_{41}\,|01100\rangle + \beta_{42}\,|01010\rangle + \beta_{44}\,|00110\rangle.\end{aligned}\tag{16}$$

For jumps at positions 3–5 we get:

$$\begin{aligned}J_3\,|c_1\rangle &= \beta_{14}\,|00010\rangle + \beta_{15}\,|00001\rangle & J_3\,|c_2\rangle &= \alpha\,|10000\rangle\\ J_4\,|c_1\rangle &= \beta_{14}\,|00100\rangle + \beta_{16}\,|00001\rangle & J_4\,|c_3\rangle &= \alpha\,|10000\rangle\\ J_5\,|c_1\rangle &= \beta_{15}\,|00100\rangle + \beta_{16}\,|00010\rangle & J_5\,|c_4\rangle &= \alpha\,|10000\rangle.\end{aligned}$$

From (11) (ii) it follows that $|\beta_{14}| = |\beta_{15}| = |\beta_{16}| = |\alpha|/\sqrt{2}$. Again by symmetry, we get $|\beta_{k\ell}| = |\alpha|/\sqrt{2}$ for all k, ℓ in (16).

On the other hand, orthogonality of $|c_1\rangle$ and $|c_2\rangle$ implies

$$0 = \langle c_1|c_2\rangle = \overline{\beta_{16}}\beta_{26},$$

a contradiction to $\alpha \neq 0$. Therefore, a jump code $\mathcal{C} = (5, 4, 1)_w$ cannot exist. ■

Using Lemma 5, we get

COROLLARY 11. *There is no jump code* $\mathcal{C} = (6, 4, 2)_w$.

In Table 1 we provide upper and lower bounds on the number of basis states K_w of a jump code $\mathcal{C} = (n, K_w, t)_w$ for $n \leq 14$. The lower bounds are mainly based on SEEDs (see Section 5) found by computer search, see Section 8.1.

Table 1. Bounds $K_w(n,t)$ on the dimension of a jump code $\mathcal{C}=(n,K_w,t)_w$. With the exception of the marked entries, the upper bounds are given by (15). The lower bounds follow from various constructions, including computer search. The subscript indicates the Hamming weight w. Entries with $K<2$ are left blank.

$n\backslash t$	1	2	3	4	5	6
4	3_2					
5	3_3^a					
6	10_3	2_3-3^b				
7	10_3-15	3_3-5				
8	35_4	4_5-15	3_4-5			
9	35_4-56	4_5-21	3_4-6			
10	126_5	6_5-56	3_4-21	2_5-6		
11	126_5-210	10_5-84	4_5-28	3_5-7		
12	462_6	10_5-210	6_6-84	3_5-28	3_6-7	
13	462_6-792	55_4^c-330	6_6-120	3_5-36	3_6-8	
14	1716_7	55_6-792	6_6-330	5_5-120	3_6-36	2_7-8

[a] by Lemma 10
[b] by Corollary 11
[c] from an LS(2, 4, 13), see Lemma 23

5. Block Designs and Jump Codes

In this section we will show that t-error protecting jump codes are naturally connected with t-designs and their variants such as partially balanced designs. To denote the class of designs required in this case we give

Definition 12. Let $v>k>t$ and l be integers. A t-spontaneous emission error design, denoted by t-SEED$(v,k;l)$, is a system $\mathcal{B}\subset\binom{V}{k}$ of k-subsets of a set V of v elements with a partition $\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(l)}$ of $\mathcal{B}$, i.e.,

$$\mathcal{B}=\mathcal{B}^{(1)}\dot{\cup}\cdots\dot{\cup}\mathcal{B}^{(l)}, \tag{17}$$

satisfying the generalised t-design property:

For all integers $s\in[1\cdots t]$ there is associated to each s-subset T of V a multiplicity $\lambda(T)$ such that for all indices $i\in[1\cdots l]$ there exits $\lambda_i(T)$ blocks $B_1^{(i)},\ldots,B_{\lambda_i(T)}^{(i)}$ in $\mathcal{B}^{(i)}$ satisfying the normalised multiplicity condition

$$\frac{\lambda_i(T)}{|\mathcal{B}^{(i)}|}:=\frac{\left|\left\{B\in\mathcal{B}^{(i)}:T\subset B\right\}\right|}{\left|\mathcal{B}^{(i)}\right|}=\lambda(T). \tag{18}$$

Remark 13. This definition encompasses the resolvability of a t-design giving more freedom by allowing a *local* parameter $\lambda(T)$ rather than the usual λ_t.

Remark 14. If $l=1$ and $\lambda(T)=\lambda$ for all $T\in\binom{V}{t}$ then a trivial t-SEED$(v,k;1)$ is given by any t-design $S_\lambda(t,k;v)$ [5] thus justifying our terminology.

The close relation between t-SEEDs and t-error correcting jump codes is described by

THEOREM 15. *If a t-SEED$(v, k; l)$ exists, then there is a jump code $\mathcal{C} = (v, l, t)_k$ with l states on v qubits.*

Proof. For $i \in [0 \cdots l-1]$ we take the encoding

$$\left|\mathcal{B}^{(i)}\right\rangle \longrightarrow \frac{1}{\sqrt{\left|\mathcal{B}^{(i)}\right|}} \sum_{B \in \mathcal{B}^{(i)}} |B\rangle \tag{19}$$

with $|B\rangle := |\chi_B(i), \ldots, \chi_B(v)\rangle$ and χ_B is the characteristic function of B, i.e., $\chi_B(i) = 1$ if $i \in B$, else $\chi_B(i) = 0$. Equivalently, $|B\rangle = |I_B\rangle$ where $I_B \in \{0, 1\}^v$ is the incidence vector of the block B.

A t-jump error in positions $x_1, \ldots, x_t$ corresponds to a t-fold derivation at the points $x_1, \ldots, x_t$. For the block classes $\mathcal{B}^{(i)}$, this is denoted by $\mathcal{B}^{(i)}_{x_1,\ldots,x_t} := \{B \setminus \{x_1, \ldots, x_t\} | \{x_1, \ldots, x_t\} \subset B \in \mathcal{B}^{(i)}\}$. As $k > t$ and $\mathcal{B}^{(i)} \bigcap \mathcal{B}^{(j)} = \emptyset$ for $i \neq j$, it follows that $\mathcal{B}^{(i)}_{x_1,\ldots,x_t} \bigcap \mathcal{B}^{(j)}_{x_1,\ldots,x_t} = \emptyset$. This proves condition (i) in (12), as for a the t-jump operator $J_{x_1,\ldots,x_t}$

$$J_{x_1,\ldots,x_t} \left|\mathcal{B}^{(i)}\right\rangle = \frac{1}{\sqrt{\left|\mathcal{B}^{(i)}\right|}} \sum_{B \in \mathcal{B}^{(i)}_{x_1,\ldots,x_t}} |B\rangle\,. \tag{20}$$

The squared norm of the state (20) is

$$\frac{\left|\mathcal{B}^{(i)}_{x_1,\ldots,x_t}\right|}{\left|\mathcal{B}^{(i)}\right|} = \frac{\left|\left\{B \in \mathcal{B}^{(i)} : \{x_1, \ldots, x_t\} \subset B\right\}\right|}{\left|\mathcal{B}^{(i)}\right|} = \lambda(\{x_1, \ldots, x_t\}),$$

so condition (18) implies condition (ii) in (12). ■

Remark 16. For all prime powers q there exists a 1-SEED$(q^2, q; q+1)$.

Proof. As block classes $\mathcal{B}^{(i)}$ take the $q+1$ parallel classes of lines in the affine geometry $AG(2, q)$ over the field $GF(q)$ of q elements. ■

In the special case of $q = 2$ this resembles the example shown in Figure 1 ([1], Fig. 1).

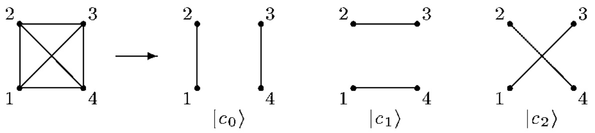

Figure 1. Graphical representation of the affine plane of 4 points and 6 lines. The partition into 3 disjoint parallel classes of lines forming a 1-SEED(4, 2; 3) defines the states of the jump code $\mathcal{C} = (4, 3, 1)_2$.

THEOREM 17. *Any system $\mathcal{B} \subset \binom{V}{k}$ of k-subsets of a set V of v elements with a partition $\mathcal{B} = \mathcal{B}^{(1)} \dot{\cup} \cdots \dot{\cup} \mathcal{B}^{(l)}$ into disjoint block classes $\mathcal{B}^{(i)}$, fulfilling the regular t-design property:*

for all $T \in \binom{V}{k}$ there exists λ blocks $B_j^{(i)} \in \mathcal{B}^{(i)}$ $(j = 1, \ldots, \lambda)$
so that $T \subset B_j^{(i)}$

holds for all $\mathcal{B}^{(i)}$ is a t-SEED$(v, k; l)$.

Proof. In this case each $(V, \mathcal{B}^{(i)})$ is an $S_\lambda(t, k; v)$ so that for all $T \in \binom{V}{s}$ $\lambda(T) = \lambda_s$ with $\lambda_s = \lambda_t\binom{v-s}{t-s}/\binom{k-s}{t-s}$ so that with the disjointness condition requirements (17) and (18) are fulfilled. ■

We now give a suite of examples of t-SEEDs. In what follows we refer to the book [5].

COROLLARY 18. *Any t-resolvable s-design $S(s, k; v)$ forms a t-SEED$(v, k; \binom{v-t}{s-t}/\binom{k-t}{s-t})$.*

Proof. Note that the condition of Theorem 17 just describes t-resolvability. ■

EXAMPLE 19. *For $m \geq 2$ there exists a 2-resolvable $S(3, 4; 4^m)$ and thus a jump code $\mathcal{C} = (2^{2m}, 2^{2m-1} - 1, 2)_4$.*

LEMMA 20. *If $v \equiv 3 \bmod 6$ there exists a jump code $\mathcal{C} = (v, \frac{v-1}{2}, 1)_3$.*

Proof. If $v \equiv 3 \bmod 6$ there exists a resolvable Steiner triple system on v points. The blockset of $\frac{v(v-1)}{6}$ triples is resolved into $\frac{v-1}{2}$ parallel classes. Any solution to Kirkman's problem provides the corresponding 1-SEED. ■

Remark 21. As a special combinatorial construction we mention the case of *doubly-resolvable* designs, which use 2-resolvable 3-designs $S(3, k; v)$ each of whose factors $S(2, k; v)$ is itself 1-resolvable. The associated jump codes $\mathcal{C} = (v, \frac{v-2}{k-2}, 2)_k$ and $\mathcal{C}' = (v, \frac{(v-1)(v-2)}{(k-1)(k-2)}, 1)_k$ are nested in the sense that the basis vectors of $\mathcal{C}$ are the "diagonal sums" of the $\frac{(v-1)}{(k-1)}$ basis vectors of the 1-jump code generated by each parallel class.

Highly regular SEED*s* are given by large sets of t-designs; see the survey in ([13], Section 3.4):

Definition 22. A *large set* of t-designs $S_\lambda(t, k; v)$ designs, denoted LS$[N](t, k, v)$, is a partition $[(X, \mathcal{B}^{(i)})]_{i=1}^{N}$ of the complete design into N disjoint t-designs $S_\lambda(t, k; v)$ where $\lambda = \binom{v-t}{k-t}/N$. Large sets are also denoted by LS$_\lambda(t, k, v)$ to emphasise the value of λ. The λ can be omitted if it is one.

LEMMA 23. *Any large set* LS$[N](t, k, v)$ *yields a t-SEED$(v, k; N)$. Any large set* LS$_\lambda$ *(t, k, v) yields a t-SEED$(v, k; \binom{v-t}{k-t}/\lambda)$.*

From [14, Table 3.44] we quote some results on the existence of largs sets of t-designs with $\lambda = 1$ and derive parameters of t-SEEDs.

- An LS$(1, k, v)$ exists if and only if k divides v. For $v \equiv 0 \bmod k$, a 1-SEED$(v, k; \binom{v-1}{k-1})$ exists.
- An LS$(2, 3, v)$ exists if and only if $v \equiv 1$ or 3 (mod 6) and $v \neq 7$. For $v \equiv 1$ or 3 (mod 6) and $v \neq 7$, a 2-SEED$(v, 3; v-2)$ exists.
- An LS$(2, 4, 13)$ exists [11]. The corresponding 2-SEED$(13, 4; 55)$ meets the upper bound of Lemma 7.

6. Finite Geometries and Jump Codes

We now describe a construction of a family of t-SEEDs for arbitrary t which almost meet the upper bound asymptotically. Our construction uses methods from classical geometry.

Definition 24. Let p be a prime and let $V = GF(p)^2$ be the points of an affine plane. Choose $\mathcal{B} = \mathcal{K}_p$, where for $t \in [1 \cdots p]$

$$\mathcal{K}_t = \{K | K = \{(x, y) \in V, y = f(x)\}\},$$

and $f(x)$ is a polynomial of degree less than t, i.e., the set of all curves defined by polynomials of degree less than t.

Such a curve $K \in \mathcal{B}$ defined by a polynomial $f(x)$ can be described by the vector of values $(f(i))$. Obviously we have the following

LEMMA 25. *For all pairwise distinct elements $x_1, \ldots, x_t$ and each tuple of values $(y_1, \ldots, y_t)$ there exists a unique curve $K \in \mathcal{K}_t$ which interpolates these points, i.e., the polynomial f defining the curve K is uniquely determined by the conditions $y_i = f(x_i)$.*

We obtain disjoint classes $\mathcal{B}^{(i)}$ (cf. Definition 12) by an action of a group as follows:

LEMMA 26. *Let $G_t \cong \mathbb{Z}_p^{p-t}$ be the group in its representation $G \cong \mathbb{Z}_p^{p-t} \times \{0\}$ on $\mathcal{K} := \mathcal{K}_t$ through the action*

$$y \rightarrow y + g \quad \textit{for } g = (g_1, \ldots, g_{p-t}, 0, \ldots, 0),$$

i.e., on the first $p-t$ vertical lines of $GF(p)^2$. Then $\mathcal{K}^h \bigcap \mathcal{K}^g = \emptyset$ if $h \neq g$, $h, g \in G$.

Proof. Without loss of generality let $h = 0$, $g \neq 0$. Suppose $z = \{(i, z_i)\} \in \mathcal{K}^h \bigcap \mathcal{K}^g$. Then there must exist polynomials $u, v \in GF(p)[x]$ of degree less than t such that $u(i) = z_i$ and $v(i) = z_i - g_i$ for $i = 1, \ldots, p$. As $g_i = 0$ for $i = p-t+1, \ldots, p$, $u(i) = v(i)$ on t places. Therefore $u = v$ thus $g = 0$, a contradiction. ■

THEOREM 27. *Let $t \in [1 \cdots (p-1)]$, p be a prime power. Let G_t and $\mathcal{K}_t^g$ for $g \in G_t$ be defined as above. Then $(GF(p)^2, \mathcal{K}_t^g)$ forms a partial t-design (a divisible t-design) with the property that each t-subset T of $GF(p)^2$ is contained in $\lambda(T)$ blocks where $\lambda(T) \in \{0, 1\}$.*

Proof. Let $t \in [1 \cdots (p-1)]$ and set $\mathcal{B}^g := \mathcal{K}_t^g$. The partition of $\mathcal{B}^g$ of $\mathcal{K}$ induced by the $g \in G_t$ forms a t-SEED$(v, k; l)$ with $v = p^2,\ k = p$ and $l = p^{p-t}$. ■

From Lemma 7, the upper bound on the dimension $l = p^{p-t}$ of the codes of Theorem 27 is given by

$$l \leq \binom{p^2 - t}{p - t}.$$

For $p \to \infty$ we obtain

$$\lim_{p\to\infty} \frac{\log \binom{p^2-t}{p-t}}{\log l} = \lim_{p\to\infty} \frac{\log \binom{p^2-t}{p-t}}{(p-t)\log p} = 1.$$

Hence, $\log_2 l$, the number of logical qubits that can be encoded using the above construction, asymptotically approaches the upper bound.

The authors would like to thank D. Glynn and D. Jungnickel who after the talk at Oberwolfach [3] pointed out connections to Laguerre planes which lead to the above construction.

7. Isodual Codes and Jump Codes

7.1. *The Construction*

In this section we show how to construct jump codes $\mathcal{C} = (v, 2, t)_k$ from t-SEEDs using isodual binary codes. By an *isodual* code C we mean a binary linear code which is *equivalent* to its *dual* code $C^\perp$; see [29]. Equivalence means that $C^\perp$ is obtained from C by a permutation σ of coordinates of all the codewords.

Let $G = \mathrm{Aut}(C)$ be the automorphism group of C, i.e., the group of permutations of coordinates of the codewords which preserve the code. Then for linear codes $G = \mathrm{Aut}(C^\perp)$, see [26]. Hence G acts on $C^\perp$ and σ normalises G, i.e., $\sigma G = G\sigma$.

By isoduality C and $C^\perp$ have identical *weight distributions*. Let W_i be the set of codewords of weight i in C and $W_i^\perp$ the corresponding set of codewords in $C^\perp$.

LEMMA 28. *If C and $C^\perp$ are isodual codes, then the orbits of G on $W_i^\perp$ are the images under σ of the orbits of G on W_i.*

Proof. Let $\mathcal{O} = \{c_{i_1}^\sigma, \ldots, c_{i_n}^\sigma\}$ be an image under σ of an orbit of G on W_i. For any $g \in G$, $\mathcal{O}^g = \{c_{i_1}^{\sigma g}, \ldots, c_{i_n}^{\sigma g}\}$. As σ normalises G, $\mathcal{O}^g = \{c_{i_1}^{h\sigma}, \ldots, c_{i_n}^{h\sigma}\}$ for some $h \in G$. Since $\{c_{i_1}, \ldots, c_{i_n}\}$ is a G orbit, it follows that $\mathcal{O}^g = \mathcal{O}$ and that $\mathcal{O}$ is a G orbit. ■

In what follows we shall assume that $C \neq C^\perp$, i.e., C is not self-dual.

For isodual codes we obtain by Lemma 28 the following decomposition of the codewords of weight i into orbits:

$$W_i = \mathcal{O}_{i_1} \dot\cup \cdots \dot\cup \mathcal{O}_{i_k} \tag{21}$$

$$W_i^\perp = \mathcal{O}_{i_1}^\sigma \dot\cup \cdots \dot\cup \mathcal{O}_{i_k}^\sigma. \tag{22}$$

We can always assume that for some weight i there is a pair $\mathcal{O}_{i_j}$ and $\mathcal{O}^{\sigma}_{i_j}$ of disjoint orbits in the decomposition (21) and (22). Otherwise $W_i = W_i^{\perp}$ for all Hamming weights, since $\mathcal{O}_{i_j}$ and $\mathcal{O}^{\sigma}_{i_j}$ are either disjoint or equal because they are both G orbits. But if $W_i = W_i^{\perp}$ for all Hamming weights then $C = C^{\perp}$, contrary to our assumption.

THEOREM 29. *Suppose C and $C^{\perp}$ are isodual codes of length n with non trivial automorphism group $G = \mathrm{Aut}(C)$. Let G act on C and $\mathcal{O}_{i_j}$ and $\mathcal{O}^{\sigma}_{i_j}$ be disjoint orbits of vectors in C and $C^{\perp}$ with weight i. Suppose that $t < i$. For each integer s with $1 \leq s \leq t$ decompose the s-subsets of $\{1, \ldots, n\}$ into orbits $\Theta_s = \{\Theta_{s_1}, \ldots, \Theta_{s_m}\}$ with respect to the induced action of G on the s-subsets. Suppose that for each s the orbits in Θ_s are preserved by σ, i.e., $\Theta^{\sigma}_{s_i} = \Theta_{s_i}$ for all i. Then the vectors in $\mathcal{O}_{i_j}$ and $\mathcal{O}^{\sigma}_{i_j}$ give a t-SEED$(n, i; 2)$.*

Proof. The orbits $\mathcal{O}_{i_j}$ and $\mathcal{O}^{\sigma}_{i_k}$ are disjoint, so we have only to establish the generalised t-design property.

Let $\{p_1, \ldots, p_s\}$ be a s-subset of each of the blocks $B_1, \ldots, B_m$ of $\mathcal{O}_{i_j}$, where $m \geq 1$ is maximal. Then $\{p^{\sigma}_1, \ldots, p^{\sigma}_s\}$ is a subset of each of the blocks $B^{\sigma}_1, \ldots, B^{\sigma}_m$ of $\mathcal{O}^{\sigma}_{i_j}$. Now $\{p_1, \ldots, p_s\} \in \Theta_{s_j}$ for some index s_j and by σ-invariance $\{p^{\sigma}_1, \ldots, p^{\sigma}_s\} \in \Theta_{s_j}$. Since Θ_{s_j} is a G orbit there is an element $h \in G$ such that $\{p_1, \ldots, p_s\} = \{p^{\sigma h}_1, \ldots, p^{\sigma h}_s\}$. This implies that $\{p_1, \ldots, p_s\}$ is a subset of each of the blocks $B^{\sigma h}_1, \ldots, B^{\sigma h}_m$ of $\mathcal{O}^{\sigma}_{i_j}$. Now using $\sigma G = G\sigma$, we have $\{B^{\sigma h}_1, \ldots, B^{\sigma h}_m\} = \{B^{g\sigma}_1, \ldots, B^{g\sigma}_m\}$ for some $g \in G$. And since the blocks $B_1, \ldots, B_m$ belong to a G orbit, so do the m blocks $B^g_1, \ldots, B^g_m$. Hence $\{p_1, \ldots, p_s\}$ is a subset of m blocks of the orbit $\mathcal{O}^{\sigma}_{i_j}$.

The case where $\{p_1, \ldots, p_s\}$ is not covered by any blocks is handled by a similar argument by noting that if $\{p_1, \ldots, p_s\} \not\subset B_i$, then $\{p^{\sigma}_1, \ldots, p^{\sigma}_s\} \not\subset B^{\sigma}_i$. In this way we have shown that local frequencies are preserved. By Theorem 17, $\mathcal{O}_{i_j}$ and $\mathcal{O}^{\sigma}_{i_j}$ give a t-SEED$(n, i; 2)$. ■

We note the following bound on the t-SEED$(n, i; 2)$ obtained from even isodual codes $C = [2n, n, d]$; where the notation $[2n, n, d]$ denotes a code of length $2n$, dimension n, and minimum distance d.

LEMMA 30. *The t parameter of a t-SEED$(n, i; 2)$ constructed using the* wgt = i *codewords of an isodual code $C = [2n, n, d]$ (cf. Theorem 29), satisfies $t \leq i - \lfloor d/2 \rfloor$, provided that a t-subset is covered by at least two blocks of* wgt = i *codewords of C.*

Proof. An orbit $\mathcal{O}_{i_j}$ of wgt = i codewords of C is a nonlinear subcode of C with the property that the Hamming distance between any two codewords is $\geq d$; see [26]. By the hypothesis a t-subset of coordinates is covered by at least two blocks of $\mathcal{O}_{i_j}$. Comparing the Hamming distance of these two blocks, we get $2(i - t) \geq d$, or $t \leq i - \lfloor d/2 \rfloor$. ■

7.2. Application of Isoduality

We now give some examples of Theorem 29.

Consider the code $C = [18, 9; 6]$ which is unique [32]. A 2-SEED(18, 6, 2) is defined by the supports of the codewords of weight six in the isodual [18, 9, 6] codes C and $C^{\perp}$. The two block classes are given by

$$\mathcal{B}^{(0)} = \{8, 11, 12, 13, 14, 17\}^G,$$
$$\mathcal{B}^{(1)} = \{9, 12, 13, 14, 17, 18\}^G.$$

The automorphism group G of C has order 2448 and has generators

$$(1, 10, 6)(2, 3, 9)(4, 13, 8)(5, 11, 12)(7, 14, 17)(15, 18, 16),$$
$$(1, 10, 4, 11, 15, 13, 17, 7)(2, 14, 9, 5, 8, 18, 3, 6).$$

The block classes $\mathcal{B}^{(0)}$ and $\mathcal{B}^{(1)}$ are given by the supports of 102 codewords of weight six which form a 2-(18, 6; 10) design. In this case G is the 2-transitive group PSL(2, 17).

Another example arises from a [22, 11, 6] code C of [22], with generator matrix A_5. The automorphism group G has order 768 which has two distinct orbits of length 48 on the weight six code words of C. The generators of G the group of order 768 are

$$(1, 2)(3, 20)(5, 16)(6, 15)(7, 18)(8, 17)(9, 14)(11, 12)(21, 22),$$
$$(1, 5, 2, 11, 4, 20, 22, 18, 21, 12, 19, 3)(6, 9, 15, 17, 14, 8)(7, 13, 16, 10),$$
$$(2, 13, 4)(3, 20)(5, 7, 11, 18, 16, 12)(6, 8, 9, 17, 15, 14)(10, 19, 21).$$

A 2-SEED(22, 6; 2) is defined by the supports of the codewords of weight six in the isodual [22, 11, 6] codes C and $C^{\perp}$. The two block classes are given by

$$\mathcal{B}^{(0)} = \{1, 2, 5, 6, 7, 8\}^G,$$
$$\mathcal{B}^{(1)} = \{1, 2, 5, 7, 15, 17\}^G.$$

We mention two more examples: a 2-SEED(6, 3; 2) from the [6, 3, 3] isodual code C. In this code there are 4 codewords of weight 3, whose supports form a 1-(6, 3; 2) design and a partially balanced $t = 2$ design with two frequencies $\lambda(T) = 0, 1$. Similarly, the unique [10, 5, 4] isodual code [23] gives a 2-SEED(10, 4; 2).

Quite a bit is known about the *extremal* isodual codes of lengths up to 48 see [17,23]. By Lemma 30, we expect that the extremal codes should give SEEDs with the highest value of t.

8. Further Constructions of Jump Codes

8.1. SEEDs with Prescribed Symmetry Group

Most of the lower bounds in Table 1 have been obtained by computer search on SEEDs implemented in MAGMA [6]. In order to reduce the search space, one can considers SEEDs with a given symmetry group. Let $G \leq S_n$ be a permutation group acting on n letters. Then the induced action of G on the set of w-subsets of $V = \{1, \ldots, n\}$ partitions $\binom{V}{w}$ into orbits. Similar to the construction in Theorem 29, one can use some of the orbits as block classes $\mathcal{B}^{(i)}$, and has then to check whether condition (18) hold.

Condition (18) is particularly easy to check when G is t-transitive.

LEMMA 31. *Let $G \leq S_n$ be a t-transitive permutation group. For $w > t$, G partitions the set of w-subsets of $\{1, \ldots, n\}$ into orbits $\mathcal{O}^{(i)}$. A collection $\mathcal{O}^{(1)}, \ldots, \mathcal{O}^{(l)}$ of orbits is a t-*SEED$(n, w; l)$ *if for all i, j*

$$\frac{\left|\left\{B \in \mathcal{O}^{(i)} : \{1, \ldots, t\} \subset B\right\}\right|}{\left|\mathcal{O}^{(i)}\right|} = \frac{\left|\left\{B \in \mathcal{O}^{(j)} : \{1, \ldots, t\} \subset B\right\}\right|}{\left|\mathcal{O}^{(j)}\right|}.$$

Proof. As G is t-transitive, it is sufficient to check condition (18) only for one representative of the t-subsets. ■

8.2. Concatenated Jump Codes

Next we discuss the construction of jump codes by concatenation.

THEOREM 32. *Let $\mathcal{C} = (n, p, t)_w$ be jump code of prime dimension with basis states $|\phi_0\rangle, \ldots, |\phi_{p-1}\rangle$. Furthermore, let $\mathcal{C}_p = [\![N, K, D]\!]_p$ be a quantum error-correcting code in the space $(\mathbb{C}^p)^{\otimes N}$. Then the concatenation of $\mathcal{C}$ as inner and $\mathcal{C}_p$ as outer code yields a jump code $\tilde{\mathcal{C}} = (Nn, p^K, T)_{Nw}$ on Nn qubits with $T \geq D(t+1) - 1$.*

Proof. The states $|\psi\rangle$ of the concatenated code $\tilde{\mathcal{C}}$ can be written as

$$|\psi\rangle = \sum_{x \in \mathbb{F}_p^N} \alpha_x |\phi_{x_1}\rangle |\phi_{x_2}\rangle \cdots |\phi_{x_N}\rangle,$$

i.e., they are superpositions of product states where each of the N factors $|\phi\rangle$ is a superposition of basis states with constant Hamming weight w. For each of the N factors of length n, we distinguish two cases: if there are no more than t jumps in a single factor then they can be corrected by the jump code $\mathcal{C} = (n, p, t)_w$.

Now assume that there are more than t jumps in a single factor. This type of error corresponds to an erasure error [21] for the outer code $\mathcal{C}_p$. When there are less than $D(t+1)$ jump errors, then there are at most $D-1$ factors with more than t jump errors, i.e., at most $D-1$ erasures. Those erasures can be corrected by the outer code $\mathcal{C}_p$. So all errors can be corrected. ■

Consider the code of Figure 1 with basis $|\phi_0\rangle = |1100\rangle + |0011\rangle$, $|\phi_1\rangle = |1010\rangle + |0101\rangle$, and $|\phi_2\rangle = |1001\rangle + |1001\rangle$. Here any 2-jump error corresponds to a projection onto one of the basis states. (More than two jumps do not occur, as there are only two excited states.) If we use this code as inner code, the outer code has only to be able to correct errors caused by measurements in a fixed basis. This is equivalent to being able to correct phase errors. In general, we obtain

COROLLARY 33. *Let $\mathcal{C} = (n, p, t)_w$ be jump code of prime dimension with basis states $|\phi_0\rangle, \ldots, |\phi_{p-1}\rangle$. Additionally, we require the following stronger version of condition (i) in (12):*

$$\forall E \subset V \forall i \neq j \colon \langle\phi_i|\, J_E^\dagger J_E |\phi_j\rangle = 0. \tag{23}$$

Then the concatenation with a quantum code $\mathcal{C}_p = [\![N, K]\!]_p$ that can correct up to $D - 1$ phase errors at known positions yields a jump code $\tilde{\mathcal{C}} = (Nn, p^K, T)_{Nw}$ on Nn qubits with $T \geq D(t+1) - 1$.

Proof. Condition (23) asserts that after a quantum jump the images of the basis states $|\phi_i\rangle$ remain orthogonal. Hence any jump error J_E that cannot be corrected by $\mathcal{C}$ corresponds to a projection onto the space $J_E\mathcal{C}$. That projection can be refined to orthogonal projections onto some of the states $J_E\,|\phi_i\rangle$. So the error corresponds to a measurement, or equivalently, a phase error for the outer code $\mathcal{C}_p$. ■

9. Conclusion

We have investigated a new and surprising connection between combinatorial designs, codes, and a recently proposed model of error control in quantum systems. We have tried to include the known combinatorial constructions which lead to t-SEEDs. Realising that our list is necessarily incomplete we apologise to the authors whose results we may have omitted. It is an open question what other constructions of t-SEEDs are possible. We have yet to completely understand the question whether jump codes derived from t-SEEDs are as powerful as general jump codes.

Acknowledgments

This work is supported by the DFG (SPP 1078) and by the EC (IST-1999-10596).

References

1. G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes, *Physical Review Letters,* Vol. 86, No. 19 (2001) pp. 4402–4405.
2. A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin and H. Weinfurter, Elementary gates for quantum computation, *Physical Review A,* Vol. 52, No. 5 (1995) pp. 3457–3467.
3. T. Beth, A class of designs protecting against quantum jumps. In (A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel and J. A. Tha, eds.), *Finite Geometries,* Oberwolfach: Mathematisches Forschungsinstitut, Report No. 52/2001, p. 4
4. T. Beth and M. Grassl, The quantum Hamming and hexacodes, *Fortschritte der Physik,* Vol. 46, No. 4–5 (1998) pp. 459–491.
5. T. Beth, D. Jungnickel and H. Lenz, *Design Theory,* Encyclopaedia of Mathematics, 2nd ed., Cambridge University Press, Cambridge (1999).
6. W. Bosma, J. J. Cannon and C. Playoust, The Magma algebra system I: the user language, *Journal of Symbolic Computation,* Vol. 24, No. 3–4 (1997) pp. 235–266.
7. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Physical Review Letters,* Vol. 78, No. 3 (1997a) pp. 405–408.
8. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, In *Proceedings ISIT 97* (1997b) p. 292.

9. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$. *IEEE Transactions on Information Theory,* Vol. 44, No. 4 (1998) pp. 1369–1387.
10. A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Physical Review A,* Vol. 54, No. 2 (1996) pp. 1098–1105.
11. L. G. Chouinard II, Partitions of the 4-subset of a 13-set into disjoint projective planes, *Discrete Mathematics,* Vol. 45 (1983) pp. 297–300.
12. J. I. Cirac and P. Zoller, Quantum computation with cold trapped ions, *Physical Review Letters,* Vol. 74, No. 20 (1995) pp. 4091–4094.
13. C. J. Colbourn and J. H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs,* CRC Press (1996).
14. D. G. Cory, A. F. Fahmy and T. F. Havel, Ensemble quantum computing by nuclear resonance spectroscopy, Technical Report TR-10-96, B. C. M. P., Harvard Medical Medical School, Boston (1996).
15. P. M. A. Dirac, *The Principles of Quantum Mechanics,* 4th ed., Clarendon Press, Oxford (1958).
16. A. Ekert and C. Macchiavello, Quantum error correction for communication, *Physical Review Letters,* Vol. 77, No. 12 (1996) pp. 2585–2588.
17. J. Fields, P. Gaborit, W. C. Huffman and V. Pless, On the classification of formally self-dual codes, In: *Proceedings of the 36th Allerton Conference on Communication, Control and Computing* (1998) pp. 566–575.
18. N. A. Gershenfeld and I. L. Chuang, Bulk spin-resonance quantum computation, *Science,* Vol. 275, No. 5298 (1997) pp. 350–356.
19. D. Gottesman, A class of quantum error-correcting codes saturating the quantum hamming bound, *Physical Review A,* Vol. 54, No. 3 (1996) pp. 1862–1868.
20. M. Grassl and T. Beth, A note on non-additive quantum codes, Technical Report quant-ph/9703016, Los Alamos National Laboratory (1997).
21. M. Grassl, T. Beth and T. Pellizzari, Codes for the quantum erasure channel, *Physical Review A,* Vol. 56, No. 1 (1997) pp. 33–38.
22. M. Harada and P. R. J. Östergård, Classification of extremal formally self-dual even codes of length 22, to appear in *Graphs and Combinatorics* (2002).
23. G. T. Kennedy and V. Pless, On designs and formally self-dual codes, *Designs, Codes and Cryptography,* (1994) pp. 43–55.
24. A. Klappenecker and M. Rötteler, Beyond stabilizer codes I: nice error bases, *IEEE Transactions on Information Theory,* LANL preprint quant-ph/0010082, Vol. 48, No. 8 (2002) pp. 2392–2395.
25. E. Knill and R. Laflamme, Theory of quantum error-correcting codes, *Physical Review A,* Vol. 55, No. 2 (1997) pp. 900–911.
26. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes,* North–Holland, Amsterdam (1977).
27. T. Pellizzari, T. Beth, M. Grassl and J. Müller-Quade, Stabilization of quantum states in quantum optical systems, *Physical Review A,* Vol. 54, No. 4 (1996) pp. 2698–2702.
28. T. Pellizzari, S. A. Gardiner, J. I. Cirac and P. Zoller, Decoherence, continuous observation, and quantum computing: a cavity QED model, *Physical Review Letters,* Vol. 75, No. 21 (1995) pp. 3788–3791.
29. E. M. Rains and N. J. A. Sloane, Self-dual codes. In (V. P. Pless and W. C. Huffman eds.), *Handbook of Coding Theory,* North-Holland (1998).
30. P. W. Shor, Algorithms for quantum computation: discrete logarithm and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* IEEE Computer Society Press (1994) pp. 124–134.
31. P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Physical Review A,* Vol. 52, No. 4 (1995) pp. R2493–R2496.
32. J. Simonis, The [18, 9, 6] code is unique, *Discrete Mathematics,* Vol. 106/107 (1992) pp. 439–448.
33. A. Steane, Multiple particle interference and quantum error correction, *Proceedings of the Royal Society London Series A,* Vol. 452 (1996a) pp. 2551–2577.
34. A. M. Steane, Error correcting codes in quantum theory, *Physical Review Letters,* Vol. 77, No. 5 (1996b) pp. 793–797.
35. W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature,* Vol. 299, No. 5886 (1982) pp. 802–803.