CDMTCS

Research

Report

Series

Eutactic quantum codes

Karl Svozil

University of Technology, Vienna

CDMTCS-214

April 2003

Centre for Discrete Mathematics and

Theoretical Computer Science

Eutactic quantum codes

Karl Svozil*

Institut für Theoretische Physik, University of Technology Vienna,

Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

Abstract

We consider sets of quantum observables corresponding to *eutactic stars*. Eutactic stars are systems of vectors which are the lower dimensional "shadow" image, the orthogonal view, of higher dimensional orthonormal bases. Although these vector systems are not comeasurable, they represent redundant coordinate bases with remarkable properties. One application is quantum secret sharing.

PACS numbers: 03.67.-a,03.67.Hk,03.65.Ta

Keywords: quantum information theory,quantum measurement theory

The increased experimental feasibility to manipulate single or few particle quantum states, and the theoretical concentration on the algebraic properties of the mathematical models underlying quantum mechanics have stimulated a wealth of applications in information and computation theory [1, 2]. In this line of reasoning, we shall consider quantized systems which can be considered to be in a coherent superposition of constituent states in such a way that only the coherent superposition of these pure states is in a predefined state; whereas one or all of the constituent states are not. Heuristically speaking, only the coherently combined states yield the "encoded message," the constituents or "shares" do not.

This feature could be compared to "quantum secret sharing" schemes [3–7], as well as to "entangled entanglement scenarios [8, 9]. There, mostly entangled multipartite system are investigated. Thus, while the above cases concentrate mainly on quantum entanglement, in what follows quantum coherence will be utilized.

We shall deal with the general case first and consider examples later. Consider an orthonormal basis $\mathcal{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of the n-dimensional real Hilbert space $\mathbb{R}^n$ [whose origin is at $(0, \ldots, 0)$]. Every point $\mathbf{x}$ in $\mathbb{R}^n$ has a coordinate representation $x_i = (\mathbf{x}, \mathbf{e}_i)$, $i = 1, \ldots, n$ with respect to the basis $\mathcal{E}$ [$(\cdot, \cdot)$ stands for the scalar product]. Hence, any vector from the origin $\mathbf{v} = \mathbf{x}$ has a representation in terms of the basis vectors given by $\mathbf{v} = \sum_{i=1}^{n} (\mathbf{v}, \mathbf{e_i})\mathbf{e_i} = \mathbf{v}\sum_{i=1}^{n} [\mathbf{e_i}^T \mathbf{e_i}]$, where the matrix notation has been used, in which $\mathbf{e_i}$ and $\mathbf{v}$ are row vectors and "^{T}" indicates transposition. (The matrix $[\mathbf{e_i}^T \mathbf{e_i}]$ is the dyadic product of the vector $\mathbf{e_i}$ with itself). Hence, $\sum_{i=1}^{n} [\mathbf{e_i}^T \mathbf{e_i}] = \mathbb{I}_n$, where $\mathbb{I}_n$ in the n-dimensional identity matrix.

Next, consider more general redundant bases consisting of systems of "well-arranged" linear dependent vectors $\mathcal{F} = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ with $m > n$, which are the orthogonal projections of orthonormal bases of m- (i.e., higher-than-n-) dimensional Hilbert spaces [10–14]. Such systems are are often referred to as *eutactic stars*. When properly normed, the sum of the their dyadic product to sum up to unity; i.e., $\sum_{i=1}^{m} [\mathbf{f_i}^T \mathbf{f_i}] = \mathbb{I}_n$, giving raise to redundant eutactic coordinates $x_i' = (\mathbf{x}, \mathbf{f}_i)$, $i = 1, \ldots, m > n$. Indeed, many properties of operators and tensors defined with respect to standard orthonormal bases directly translate into eutactic coordinates [14].

According to Zeilinger's [15–17] generalized [18] foundational principle, k elementary m-state systems can carry k *nits* (the term nit stands for a radix m measure of quantum information). It is possible to encode a radix m nit by the pure one dimensional subspaces of $\mathbb{R}^m$ spanned by some orthonormal basis vectors $\mathcal{E}' = \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$. In the quantum logic approach pioneered by Birkhoff and von Neumann (e.g., [19–22]), every such basis vector corresponds to the physical proposition that “the system is in a particular one of m different states.” All the propositions corresponding to orthogonal base vectors are comeasurable.

On the contrary, the propositions corresponding to the eutactic star

$$\mathcal{F} = \{P\mathbf{e}_1, \dots, P\mathbf{e}_m\}$$

formed by some orthogonal projection P of $\mathcal{E}'$ is no longer comeasurable (or it just spans a one dimensional subspace). Neither is the eutactic star

$$\mathcal{F}^\perp = \left\{P^\perp\mathbf{e}_1, \dots, P^\perp\mathbf{e}_m\right\}$$

formed by the orthogonal projection $P^\perp$ of $\mathcal{E}'$. Indeed, the elements of $\mathcal{F}$ and $\mathcal{F}^\perp$ may be considered as “shares” in the context of quantum secret sharing. Thereby, not all shares may be equally suitable for cryptographic purposes. This scenario can be generalized to multiple shares in a straightforward way.

For a configuration of just two shares, the optimal configuration is one in which all orthonormal vector spanning $\mathbb{R}^m$ have the same component in the direction of one share; and the other shares consists of the normal projection along this direction. As an example, consider the two shares $\{\mathbf{w}\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ defined by

$$\begin{gathered} \mathbf{w} = \left(0, 0, \tfrac{1}{\sqrt{3}}\right), \\ \mathbf{x} = \left(\sqrt{\tfrac{2}{3}}, 0, 0\right), \quad \mathbf{y} = \left(-\tfrac{1}{\sqrt{6}}, \tfrac{1}{\sqrt{2}}, 0\right), \quad \mathbf{z} = \left(-\tfrac{1}{\sqrt{6}}, -\tfrac{1}{\sqrt{2}}, 0\right). \end{gathered} \tag{1}$$

While $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ and $\{\mathbf{w}\}$ constitute eutactic stars in $\mathbb{R}^2$ and $\mathbb{R}$, respectively, the coherent superposition of $\mathbf{w}$ with all the other states forms an orthogonal basis of $\mathbb{R}^3$.

$$\{\mathbf{w}+\mathbf{x}, \mathbf{w}+\mathbf{y}, \mathbf{w}+\mathbf{z}\} = \left\{\left(\sqrt{\frac{2}{3}}, 0, \frac{1}{\sqrt{3}}\right), \left(-\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{3}}\right), \left(-\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{3}}\right)\right\} \tag{2}$$

The corresponding comeasurable projection operators are given by

$$E_1 = \begin{pmatrix} \frac{2}{3} & 0 & \frac{\sqrt{2}}{3} \\ 0 & 0 & 0 \\ \frac{\sqrt{2}}{3} & 0 & \frac{1}{3} \end{pmatrix}, \qquad E_2 = \begin{pmatrix} \frac{1}{6} & \frac{-1}{2\sqrt{3}} & \frac{-1}{3\sqrt{2}} \\ \frac{-1}{2\sqrt{3}} & \frac{1}{2} & \frac{1}{\sqrt{6}} \\ \frac{-1}{3\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{3} \end{pmatrix}, \qquad E_3 = \begin{pmatrix} \frac{1}{6} & \frac{1}{2\sqrt{3}} & \frac{-1}{3\sqrt{2}} \\ \frac{1}{2\sqrt{3}} & \frac{1}{2} & -\frac{1}{\sqrt{6}} \\ \frac{-1}{3\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{3} \end{pmatrix}, \tag{3}$$

whereas the “shares” either contain no information at all, such as $[\mathbf{w}^T\mathbf{w}]$; or are not comeasurable, such as $[\mathbf{x}^T\mathbf{x}]$, $[\mathbf{y}^T\mathbf{y}]$ and $[\mathbf{z}^T\mathbf{z}]$.

Note, however, that some configurations are not usable for secret sharing. The "worst case" scenario might just be one in which the first share coincides with a basis vector of the orthonormal basis spanning $\mathbb{R}^m$. In this case, the second share just consists of the remaining base states, making possible the detection of the original message. Take, for instance, the basis $\{(0,0,1),(0,1,0),(1,0,0)\}$ which, when projected along the z-axis, results in the shares $\{(0,0,1)\}$ and $\{(0,1,0),(1,0,0)\}$. These shares enable the parties to deterministically discriminate between the first state and the rest (first share), and between all states (second share).

A possible experimental realization of an arbitrary m-dimensional configuration could be a general interferometer with m inputs and m output terminals [23], which are partitioned according to the orthogonal projections involved. They should be arranged such that the single input/output ports corresponds to one dimension.

As has already been pointed out, the proposed scheme does not necessarily involve entangled multipartite schemes; thus the parties are not given particles as shares. Rather, in the interferometric realization they are given interferometric channels; and in order to reconstruct the original message it is important to keep quantum coherence among all the parties. Thus, no particle detection is allowed. Yet, even in the quantum secret sharing schemes discussed so far, particles have to be handled very carefully in order to maintain entanglement among the shares.

* Electronic address: svozil@tuwien.ac.at; URL: http://tph.tuwien.ac.at/~svozil

[1] J. Gruska, *Quantum Computing* (McGraw-Hill, London, 1999).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[3] M. Hillery, V. Buzek, , and A. Berthiaume, Physical Review A **59**, 1829 (1999), quant-ph/9806063, URL http://link.aps.org/abstract/PRA/v59/p1829.

[4] R. Cleve, D. Gottesman, and H.-K. Lo, Physical Review Letters **83**, 648 (1999), quant-ph/9901025, URL http://link.aps.org/abstract/PRL/v83/p648.

[5] T. of quantum secret sharing, Physical Review A **61**, 042311 (2000), quant-ph/9910067, URL http://link.aps.org/abstract/PRA/v61/e042311.

[6] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Physical Review A **86**, 5807 (2001), quant-

ph/0011042, URL `http://link.aps.org/abstract/PRL/v86/p5807`.

[7] D. P. DiVincenzo, P. Hayden, and B. M. Terhal (2002), quant-ph/0207147, URL `http://arxiv.org/abs/quant-ph/0207147`.

[8] G. Krenn and A.Zeilinger, Physical Review A **54**, 1793 (1996), URL `http://link.aps.org/abstract/PRA/v54/p1793`.

[9] J. L. Cereceda, Physical Review A **56**, 1733 (1997), URL `http://link.aps.org/abstract/PRA/v56/p1733`.

[10] L. Schäfli, in *Denkschrift der Schweizerischen Naturforschenden Gesellschaft*, edited by J. H. Graf (1901), vol. 38, pp. 1–237.

[11] H. Hadwiger, Comm. Math. Helv. **13**, 90 (1940).

[12] H. S. M. Coxeter, *Regular Polytopes, Third edition* (Dover Publications, New York, 1973).

[13] J. J. Seidel, Colloquia Mathematica Societatis Janos Bolyai **18**, 983 (1976).

[14] D. Hasse and H. Stachel, Beitr. Algebra Geom. **37**, 367 (1996), URL `http://www.emis.de/journals/BAG/vol.37/no.2/`.

[15] A. Zeilinger, Foundations of Physics **29**, 631 (1999).

[16] Č. Brukner and A. Zeilinger, Acta Physica Slovaca **49**, 647 (1999).

[17] N. Donath and K. Svozil, Physical Review A **65**, 044302 (2002), quant-ph/0105046, URL `http://link.aps.org/abstract/PRD/v65/p044302`.

[18] K. Svozil, Physical Review A **66**, 044306 (2002), quant-ph/0205031, URL `http://link.aps.org/abstract/PRD/v66/p044306`.

[19] G. Birkhoff and J. von Neumann, Annals of Mathematics **37**, 823 (1936).

[20] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932), english translation: *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1955.

[21] G. W. Mackey, *The Mathematical Foundations of Quantum Mechanics* (W. A. Benjamin, Reading, MA, 1963).

[22] K. Svozil, *Quantum Logic* (Springer, Singapore, 1998).

[23] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Physical Review Letters **73**, 58 (1994), see also [24].

[24] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, 1962).