Eutactic quantum codes

Karl Svozil*

Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

(Received 10 April 2003; revised manuscript received 3 November 2003; published 8 March 2004)

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.

DOI: 10.1103/PhysRevA.69.034303 PACS number(s): 03.67.Hk, 03.65.Ta

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 are 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: in the secret-sharing scheme proposed here, one party receives part of a quantum state and the other party receives the other part. The parts are components of a vector lying in subspaces of a higher-dimensional Hilbert space. While the possible quantum states to be sent are orthogonal, the parts are not, so that the parties must put their parts together to decipher the message.

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 $x_i=\langle\mathbf{x}|\mathbf{e}_i\rangle$, $i=1,\ldots,n$ with respect to the basis $\mathcal{E}$. Hence, any vector from the origin $\mathbf{v}=\mathbf{x}$ has a representation in terms of the basis vectors given by $\mathbf{v}=\Sigma_{i=1}^{n}\langle\mathbf{v}|\mathbf{e_i}\rangle\mathbf{e_i}=\mathbf{v}\Sigma_{i=1}^{n}[\mathbf{e_i}^T\mathbf{e_i}]$, where the matrix notation has been used, in which $\mathbf{e_i}$ and $\mathbf{v}$ are row vectors and "T" indicates transposition. ($\langle\cdot|\cdot\rangle$ and the matrix $[\mathbf{e_i}^T\mathbf{e_i}]$ stand for the scalar product and the dyadic product of the vector $\mathbf{e_i}$ with itself, respectively). Hence, $\Sigma_{i=1}^{n}[\mathbf{e_i}^T\mathbf{e_i}]=\mathbb{I}_n$, where $\mathbb{I}_n$ is 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. Such systems are often referred to as *eutactic stars* [10–14]. When properly normed, the sum of the dyadic products of their vectors yields unity, i.e., $\Sigma_{i=1}^{m}[\mathbf{f_i}^T\mathbf{f_i}]=\mathbb{I}_n$, giving raise to redundant eutactic coordinates $x_i'=\langle\mathbf{x}|\mathbf{f}_i\rangle$, $i=1,\ldots,m>n$. Indeed, many properties of operators and tensors defined with respect to standard orthonormal bases directly translate into eutactic coordinates [14].

In terms of m-ary (radix m) measures of quantum information based on state partitions [15], k elementary m-state systems can carry k *nits* [16–18]. A nit can be encoded by the 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., Refs. [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

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

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

$$\mathcal{F}^{\perp}=\{P^{\perp}\mathbf{e}_1,\ \ldots,P^{\perp}\mathbf{e}_m\}$$

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.

Let us consider an example for a two-component two-share configuration, in which each party obtains one substate from two possible ones. In particular, consider the two shares $\{\mathbf{w},\mathbf{x}\}$ and $\{\mathbf{y},\mathbf{z}\}$ defined in four-dimensional complex Hilbert space by

$$\mathbf{w}=\left(0,0,-\frac{1}{2\sqrt{2}},\frac{1}{\sqrt{2}}\right),\quad \mathbf{x}=\frac{1}{2}\left(0,0,-\frac{3}{2},-1\right),$$

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

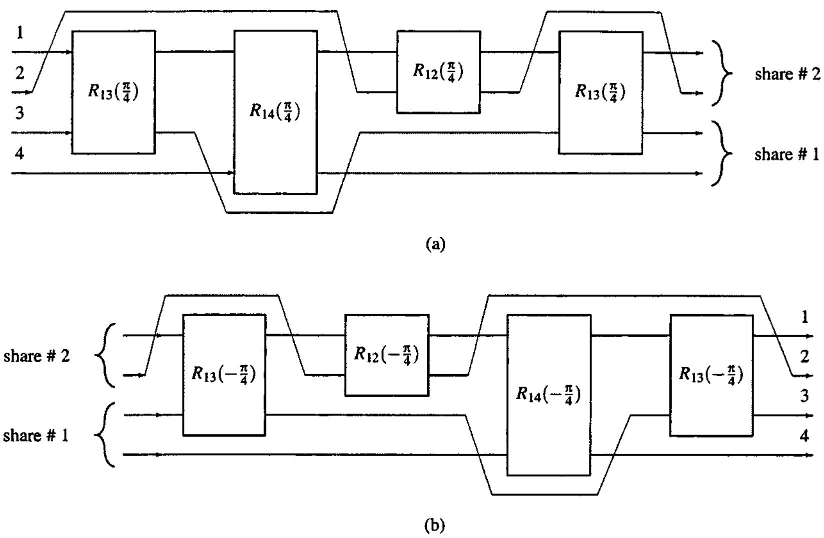

FIG. 1. Experimental realization of (a) the encoding stage of a two-component two-share configuration by an array of effectively two-dimensional beam splitters depicted as boxes. The decoding stage (b) is just the encoding stage (a) in reverse order, with inverse beam splitters.

$$\mathbf{y} = \frac{1}{2}\left(\frac{1}{\sqrt{2}}, -1, 0, 0\right), \quad \mathbf{z} = \frac{1}{2\sqrt{2}}\left(-\frac{1}{\sqrt{2}}, -1, 0, 0\right).$$

While $\{\mathbf{w},\mathbf{x}\}$ and $\{\mathbf{y},\mathbf{z}\}$ constitute eutactic stars in $\mathbb{R}^2$, the coherent superposition of $\mathbf{w}$ with $\mathbf{y}$, and $\mathbf{x}$ with $\mathbf{z}$ yield two orthogonal vectors in $\mathbb{R}^4$:

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

which could be used as a bit representation. As can be readily verified, the shares in Eq. (1) are obtained by applying the projections $P = \mathrm{diag}(1,1,0,0)$ and $P^{\perp} = \mathrm{diag}(0,0,1,1)$ to the vectors in Eq. (2) ["$\mathrm{diag}(a,b,\ldots)$" stands for the diagonal matrix with $a,b,\ldots$ at the diagonal entries]. The comeasurable projection operators corresponding to the vectors in Eq. (2) are given by

$$[(\mathbf{w}+\mathbf{y})^T(\mathbf{w}+\mathbf{y})] = \frac{1}{4}\begin{pmatrix} \frac{1}{2} & -\frac{1}{\sqrt{2}} & -\frac{1}{2} & 1 \\ -\frac{1}{\sqrt{2}} & 1 & \frac{1}{\sqrt{2}} & -\sqrt{2} \\ -\frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} & -1 \\ 1 & -\sqrt{2} & -1 & 2 \end{pmatrix} \tag{3}$$

and

$$[(\mathbf{x}+\mathbf{z})^T(\mathbf{x}+\mathbf{z})] = \frac{1}{4}\begin{pmatrix} \frac{1}{4} & \frac{1}{2\sqrt{2}} & \frac{3}{4} & \frac{1}{2} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2} & \frac{3}{2\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{3}{4} & \frac{3}{2\sqrt{2}} & \frac{9}{4} & \frac{3}{2} \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{3}{2} & 1 \end{pmatrix}, \tag{4}$$

whereas the shares given to the parties are not comeasurate, i.e., $[\mathbf{w}^T\mathbf{w}][\mathbf{x}^T\mathbf{x}] - [\mathbf{x}^T\mathbf{x}][\mathbf{w}^T\mathbf{w}] \neq 0$ and $[\mathbf{y}^T\mathbf{y}][\mathbf{z}^T\mathbf{z}] - [\mathbf{z}^T\mathbf{z}][\mathbf{y}^T\mathbf{y}] \neq 0$. Only after recombining the shares it is possible to reconstruct the information, i.e., to decide whether $(\mathbf{w}+\mathbf{y})$ or $(\mathbf{x}+\mathbf{z})$ has been communicated. This configuration demonstrates the protocol, but it is not optimal, as four dimensions have been used to represent a single bit. A more effective coding in base four could utilize the additional two "quadrit" states $(1/2)(1,\sqrt{2},-1,0)$ and $(1/2)(3/2,-1/\sqrt{2},1/2,-1)$.

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 in such a way that the single input/output terminals each correspond to one dimension. Consider, for example, the two-component two-share configuration discussed above. The two bit states (2) can be constructed from the orthogonal pair of vectors $\mathbf{e}_1 = (0,0,0,1)$ and $\mathbf{e}_2 = (1,0,0,0)$ by subjecting them to four successive rotations in two-dimensional subspaces of $\mathbb{R}^4$, i.e., $\mathbf{w}+\mathbf{y} = R_{13}(\pi/4)R_{12}(\pi/4)R_{14}(\pi/4)R_{13}(\pi/4)\mathbf{e}_1$ and $\mathbf{x}+\mathbf{z} = R_{13}(\pi/4)R_{12}(\pi/4)R_{14}(\pi/4)R_{13}(\pi/4)\mathbf{e}_2$, where R_{12}, R_{14}, and R_{13} represent the usual clockwise rotations in the 1-2, 1-4, and 1-3 planes. The corresponding (lossless) interferometric configuration is depicted in Fig. 1; the boxes standing for a 50:50 mixing.

The encoding phase depicted in Fig. 1(a) consist of either inserting a particle into the first or the fourth terminal. Formally, its state undergoes the particular types of mixing transformations outlined above. Finally, the two upper and two lower exit terminals are subdivided into the two shares. The decoding phase depicted in Fig. 1(b) requires both shares, which are recombined in a reverse interferometric setup, in which the original states are reconstructed by performing the reverse mixings in reverse order.

Some configurations are not usable for secret sharing. The "worst case" scenario might 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 simple setup would correspond to a two-dimensional case, in which a particle would enter one of two input ports. A successive beam splitter would then scramble the original signal. In this setup, the two shares would just correspond to the two output ports of the beam splitter. Even though both parties would know that the other party would possess a one-dimensional share, due to phase coherence it would not be possible in a straightforward manner to reconstruct the secret message by manufacturing the missing one-component share.

As has already been pointed out, the proposed scheme does not necessarily involve entangled multipartite states; 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, in the encrypted stage, that is, before the decoding, no particle detection is allowed, since this would destroy coherence. The decoding transformation is the coherent combination of the two shares whose channels each correspond, respectively, to one and only one secret message.

Here we have proposed to look into possibilities to utilize the higher-dimensional components of the quantum state by combining two or more states defined in effectively lower-dimensional subspaces. Only after all parties have put their parts of the states together are they able to decypher the message. The "extra dimensions" not used by the "flattened out" subspaces might be very useful for other purposes as well. For instance, one might speculate that they could be exploited for computational purposes such as speedups, analogously to the introduction of the complex plane for the solution of certain problems, such as integrals, in the analysis. There, the challenge might be to extend the existing quantum algorithms to higher dimensions, thereby exploiting multidimensional connectedness in search spaces and the like, and at the same time being able to reconstruct the results in lower dimensions.

[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, Phys. Rev. A **59**, 1829 (1999).

[4] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[5] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[6] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).

[7] D. P. DiVincenzo, P. Hayden, and B. M. Terhal, e-print quant-ph/0207147; URL http://arxiv.org/abs/quant-ph/0207147

[8] G. Krenn and A. Zeilinger, Phys. Rev. A **54**, 1793 (1996).

[9] J. L. Cereceda, Phys. Rev. A **56**, 1733 (1997).

[10] L. Schläfli, in *Theorie der vielfachen Kontinuität* (Zürcher & Furrer, Zürich, 1901), Vol. 38, pp. 1–237.

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

[12] H. S. M. Coxeter, *Regular Polytopes*, 3rd ed. (Dover, New York, 1973).

[13] J. J. Seidel, Colloq. Math. Soc. Janos Bolyai **18**, 983 (1976).

[14] D. Hasse and H. Stachel, Beitr. Algebra Geom. **37**, 367 (1996).

[15] K. Svozil, Phys. Rev. A **66**, 044306 (2002).

[16] A. Zeilinger, Found. Phys. **29**, 631 (1999).

[17] Č. Brukner and A. Zeilinger, Acta Phys. Slov. **49**, 647 (1999).

[18] N. Donath and K. Svozil, Phys. Rev. A **65**, 044302 (2002).

[19] G. Birkhoff and J. von Neumann, Ann. Math. **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, NJ, 1955).

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

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

[23] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994); also see *The Unitary and Rotation Groups* (Ref. [24]).

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