Cryptography & Graphs

Research Group at the University of Lleida

Quantum models and applications

SXD

IMTech & BSC

19/4/2023

Index

- Hermitian vector spaces
- Quantum systems
- The q-bit heuristic model
- A quaternion portrait of a q-bit
- Registers of q-bits
- q-gates and q-computations
- A. Spinor spherical coordinates
- B: The algebra $\mathcal{G}_n$

Hermitian vector spaces

The ground of the familiar modeling of n-dimensional euclidean geometry is *a real vector space E endowed with a positive-definite quadratic form* or, equivalently, with a symmetric scalar product $x \cdot x'$ such that $x \cdot x > 0$ for $x \neq 0$. Then

- Vectors have *length*, $|x| = +\sqrt{x \cdot x}$; this length is a *norm* for E, which is often denoted $\|x\|$.
- Non-zero vectors $x, x' \in E$ define the *angle* $\alpha = \alpha(x, x') \in [0, \pi]$ by the formula $\cos(\alpha) = (x \cdot x')/|x||x'|$ (based on the Cauchy-Schwarz inequality).
- $\alpha = 0$ if and only if $x' = tx$ with $t > 0$ and $\alpha = \pi$ if and only if $x' = tx$ with $t < 0$; in any case, the angle does not vary if we rescale the vectors: if t, t' are positive real numbers, then $\alpha(tx, t'x') = \alpha(x, x')$.
- But note that $\alpha(-x, x') = \alpha(x, -x') = \pi - \alpha(x, x')$.

A *hermitian* vector space is a *complex* vector space H endowed with a scalar product $\langle x|x'\rangle \in \mathbb{C}$ $(x, x' \in H)$ satisfying the following properties:

(1) It is $\mathbb{C}$-*linear in* x';

(2) *Conjugate-symmetric*: $\langle x'|x\rangle = \overline{\langle x|x'\rangle}$ (the overline means complex conjugation). In particular, it is *conjugate-linear* (same as *anti-linear*) in x. Since $\langle x|x\rangle$ is self-conjugate for any x, it is a real number.

(3) *Positive-definite*: $\langle x|x\rangle > 0$ if $x \neq 0$.

For any $x \in H$, we set $|x| = \sqrt{\langle x|x\rangle}$ (*norm* or *length* of x; it is also customary to denote it by $\|x\|$). If $|x| = 1$, we say that x is *unitary*, or a *unit vector*.

For example, $\mathrm{u}(x) = x/|x|$ (*normalization* of x) is unitary for any $x \neq 0$.

We say that $x, x' \in H$ are *orthogonal* if $\langle x|x'\rangle = 0$, and we will write $x \perp x'$ to denote this relation.

A basis $e_1, \ldots, e_n$ of H is said to be *orthonormal* if $\langle e_j|e_k\rangle = \delta_{jk}$ for any j, k. This means that the e_j are unit vectors such that $e_j \perp e_k$ for $j \neq k$.

The components $\lambda_j \in \mathbb{C}$ of a vector $x \in H$ with respect to an orthonormal basis $e_1, \ldots, e_n$ are given by $\lambda_j = \langle e_j|x\rangle$, so that $x = \langle e_1|x\rangle e_1 + \cdots + \langle e_n|x\rangle e_n$.

We will often use the relations $x \sim x'$ and $x \equiv x'$ $(x, x' \in H)$. The first is a shorthand for stating that $x' = \lambda x$, for some non-zero $\lambda \in \mathbb{C}$. For example, we have $x \sim \mathrm{u}(x)$ for any non-zero $x \in H$ (in this case $\lambda = 1/|x|$ is real). The second relation is a shorthand for stating that $x' = \lambda x$ for some $\lambda \in \mathbb{C}$ such that $|\lambda| = 1$. In other words, $x' = e^{i\varphi}x$ for some $\varphi \in \mathbb{R}$.

$\mathbb{C}^n$ with the scalar product

$$\langle \xi | \xi' \rangle = \bar{\xi}_1 \xi'_1 + \cdots + \bar{\xi}_n \xi'_n,$$

is a Hermitian space.

For the treatment of *q*-bits, the basic space we initially need is $\mathbb{C}^2$.

For historical reasons, the elements of this space are called (Pauli) *spinors* and we will re-index them as $\xi = (\xi_0, \xi_1)$.

Thus, in this case the Hermitian scalar product reads

$$\langle \xi | \xi' \rangle = \bar{\xi}_0 \xi'_0 + \bar{\xi}_1 \xi'_1.$$

Moreover, we will use the notation $e_0 = (1, 0)$ and $e_1 = (0, 1)$.

Theorem

(1) Let H be a Hermitian vector space. Then, for all $x, x' \in H$,
$|\langle x|x'\rangle| \leqslant |x||x'|$.

(2) Equlity holds if and only if $x' \sim x$.

Proof. (1) Let $\alpha = \arg\langle x|x'\rangle$, so that $e^{-i\alpha}\langle x|x'\rangle = |\langle x|x'\rangle|$.

We have $\langle tx + e^{-\alpha i}x'|tx + e^{-\alpha i}x'\rangle \geqslant 0$ for any $t \in \mathbb{R}$. On expanding, we get $|x|^2t^2 + e^{-\alpha i}\langle x|x'\rangle t + e^{\alpha i}\langle x'|x\rangle t + |x'|^2 \geqslant 0$. In this expression, $e^{-\alpha i}\langle x|x'\rangle + e^{\alpha i}\langle x'|x\rangle = 2\mathrm{re}(e^{-\alpha i}\langle x|x'\rangle) = 2|\langle x|x'\rangle|$, by the definition of α. Therefore the inequality is equivalent to $|x|^2t^2 + 2|\langle x|x'\rangle|t + |x'|^2 \geqslant 0$. Since this holds for any t, $|\langle x|x'\rangle|^2 - |x|^2|x'|^2 \leqslant 0$, and this proves (1).

(2) If the equality $|\langle x|x'\rangle| = |x||x'|$ holds, then $tx + e^{-\alpha i}x' = 0$ for some t and hence $x' \sim x$. And it is immediate to check that $x' \sim x$ implies $|\langle x|x'\rangle| = |x||x'|$. □

If $x, x' \in H$ are non-zero vectors, the Theorem (p. 8) tells us that

$$0 \leqslant |\langle x|x'\rangle|/|x||x'| \leqslant 1$$

and hence there is a unique real number $\beta = \beta(x, x') \in [0, \pi/2]$ such that

$$\cos(\beta) = |\langle x|x'\rangle|/|x||x'|.$$

- $\beta = \pi/2$ precisely when $\langle x|x'\rangle = 0$ (that is, precisely when $x \perp x'$)
- $\beta = 0$ if and only if $x' \sim x$.
- $\beta(x, x') = \beta(y, y')$ when $y \sim x$ and $y' \sim x'$.

Let $H_{\mathbb{R}}$ be H regarded as a real vector space. In this space we may consider the bilinear form $(x,x') = \mathrm{re}\langle x|x'\rangle$ (note that $\langle x|x'\rangle$ *is* $\mathbb{R}$*-bilinear*). It is symmetric, because

$$(x',x) = \mathrm{re}\langle x'|x\rangle = \mathrm{re}\overline{\langle x|x'\rangle} = \mathrm{re}\langle x|x'\rangle = (x,x').$$

And it is positive definite, for $(x,x) = \mathrm{re}\langle x|x\rangle = \langle x|x\rangle > 0$ if $x \neq 0$.

The euclidean angle between $x, x' \in H_{\mathbb{R}}$ will be denoted by $\alpha(x,x')$.

Orthogonal vectors in H are also orthogonal in $H_{\mathbb{R}}$.

The converse is not true: if $u \in H$ is a unit vector, then $\langle u|iu\rangle = i \neq 0$, but $(u,iu) = \mathrm{re}(i) = 0$.

- $\beta(u,iu) = 0$, as $|i| = 1$, and $\alpha(u,iu) = \pi/2$.
- $\alpha(u,-u) = \pi$, but $\beta(u,-u) = 0$.

The $\mathbb{C}$-endomorphisms of H are usually called *operators*.

If L is an operator, its *adjoint*, denoted $L^\dagger$, is defined as the unique endomorphism of H such that

$$\langle L^\dagger y|x\rangle = \langle y|Lx\rangle.$$

The map $L \mapsto L^\dagger$ is conjugate-linear. If $L^\dagger = L$, we say that L is *selfadjoint* or *hermitian*.

Example. Let $F \subseteq H$ be a vector subspace. The *orthogonal projection*

$$P_F : H \to H,\ x \mapsto x',\ \text{where } x = x' + x'',\ x' \in F,\ x'' \in F^\perp$$

is selfadjoint, as the expressions $\langle P_F y|x\rangle$ and $\langle y|P_F x\rangle$ are both equal to $\langle y'|x'\rangle$. For instance, $\langle y|P_F x\rangle = \langle y' + y''|x'\rangle = \langle y'|x'\rangle$, as $\langle y''|x'\rangle = 0$.

If $v \in H$ is a non-zero vector, instead of $P_{\langle v\rangle}$ we will simply write P_v.

If we know an orthonormal basis $e_1, \dots, e_r$ of F, then

$$P_F(x) = \langle e_1|x\rangle e_1 + \cdots + \langle e_r|x\rangle e_r.$$

In particular we have, for any non-zero vector $v \in H$,

$P_v(x) = \langle v|x\rangle v$ if v is unitary, or
$P_v(x) = \frac{1}{|v|^2}\langle v|x\rangle v$ otherwise.

Let A be the matrix of an operator L of the hermitian space H with respect to an orthonormal basis $e_1, \dots, e_n$, that is, $A = (a_{ij})$, where

$L(e_j) = a_{1j}e_1 + \cdots + a_{nj}e_n$.

Then the matrix of $L^\dagger$, with respect to the same basis, is $A^\dagger$:

$L^\dagger(e_i) = \bar{a}_{i1}e_1 + \cdots + \bar{a}_{in}e_n$.

This implies that L is self-adjoint if and only if the matrix A is self-adjoint (that is, $A^\dagger = A$).

An operator U is said to be *unitary* if $U^\dagger U = I$.

It is clear that U is unitary if and only if its matrix A is a unitary matrix ($A^\dagger A = I_n$). Equivalently, U is unitary if and only if $\langle Ux|Ux'\rangle = \langle x|x'\rangle$ for all $x, x' \in H$. This condition implies that $|Ux| = |x|$ for all $x \in H$. The converse is also true because of the identity

$$4\langle x|x'\rangle = |x+x'|^2 - |x-x'|^2 + i|ix+x'|^2 - i|-ix+x'|^2,$$

which can be expressed as $\sum_{\nu=0}^{\nu=3} i^\nu |i^\nu x + x'|$.

The unitary operators of H form a group with the composition operation (the *unitary group* of H). It is denoted by $\mathrm{U}(H)$. If H has dimension n, $\mathrm{U}(H) \simeq \mathrm{U}_n$ (the group of unitary matrices of order n).

The *special unitary group* of H is

$$\mathrm{SU}(H) = \{U \in \mathrm{U}(H) : \det(U) = 1\}.$$

Clearly, $\mathrm{SU}(H) \simeq \mathrm{SU}_n$, the group of unitary matrices whose determinant is 1.

Example. The matrices of SU$_2$ have the form

$$\begin{bmatrix} \xi_0 & -\bar{\xi}_1 \\ \xi_1 & \bar{\xi}_0 \end{bmatrix},$$

where $\xi_0, \xi_1 \in \mathbb{C}$ with $\xi_0\bar{\xi}_0 + \xi_1\bar{\xi}_1 = 1$.

Quantum systems

State vectors
Pure states
The ket map

The modeling of quantum systems is analogous to the modeling of euclidean geometry by finite dimensional positive-definite real quadratic spaces, but using complex Hilbert spaces instead of real spaces. Moreover, for quantum computing only hermitian spaces (Hilbert spaces of finite dimension) are required.

- Each *quantum system* is modeled on a complex Hilbert space H.
- The non-zero elements of H are called *state vectors*, or simply *vectors*.
- For quantum computing we may restrict H to have finite dimension, i.e. to be a *hermitian vector space*.

The (pure) *states* are the elements of $\Sigma = \mathbb{P}H$ (*projective space of* H).

This means that each non-zero $x \in H$ determines a state, which here we will denote by $|x\rangle$ (Dirac *ket* notation), and that two non-zero $x, x' \in H$ determine the same state ($|x\rangle = |x'\rangle$) if and only if $x' \sim x$.[1]

Remark. Each state can be represented by a unit vector, as $x \sim \mathrm{u}(x)$. But unit vectors representing the same state differ by a *phase* factor (a unit complex number), and hence *sates and unit vectors are quite different concepts*.

[1] In mathematics, the projective point represented by x is denoted by $[x]$. N

Example

$\mathbb{PC}^2 \simeq \mathbb{C} \sqcup \{\infty\} = \widehat{\mathbb{C}}$:

For $\xi = (\xi_0, \xi_1) \in \mathbb{C}^2 - \{(0,0)\}$,

$$|\xi\rangle = \begin{cases} |(1, \xi_1/\xi_0)\rangle & \text{if} \quad \xi_0 \neq 0 \\ |(0,1)\rangle & \text{otherwise} \end{cases}$$

In the other direction, $\widehat{\mathbb{C}} \to \mathbb{PC}^2$: $z \mapsto |(1, z)\rangle$ for $z \in \mathbb{C}$, and $\infty \mapsto |(0,1)\rangle$.

Given two different states, $X = |x\rangle$ and $X' = |x'\rangle$, each state of the projective line XX' is said to be a (quantum) *superposition* of X and X'. By definition, such states have the form $|\xi x + \xi' x'\rangle$, with $\xi, \xi' \in \mathbb{C}$ and $\xi x + \xi' x' \neq 0$.

In the special case of the complex projective line, $\mathbb{P}^1_{\mathbb{C}} = \mathbb{P}\mathbb{C}^2$, any state is the superposition of any two different states, for example of $|e_0\rangle$ and $|e_1\rangle$, as any (ξ_0, ξ_1) is obviously equal to $\xi_0 e_0 + \xi_1 e_1$.

Usually the abridgements $|0\rangle$ and $|1\rangle$ are used instead of $|e_0\rangle$ and $|e_1\rangle$.

Warning

Dirac's ket notation is usually abused by writing $\xi|x\rangle + \xi'|x'\rangle$ instead of $|\xi x + \xi' x'\rangle$.

For example, in the case of $\mathbb{P}^1_{\mathbb{C}}$, the expression $\xi_0|0\rangle + \xi_1|1\rangle = \xi_0|e_0\rangle + \xi_1|e_1\rangle$ means $|\xi_0 e_0 + \xi_1 e_1\rangle = |\xi_0, \xi_1\rangle$.

But $\xi|x\rangle + \xi'|x'\rangle$ does not make sense mathematically, as Σ is not a vector space (and even less a complex vector space), in practice it is understood that the state expressed by $|x\rangle$ "remembers" the vector x that has been used to represent it and thus calculations can usually be interpreted unambiguously.

For example, if $e_1, \ldots, e_n$ is a basis of H and $x = \Sigma\lambda_j e_j$, then custom favors to write the expression $\Sigma\lambda_j|e_j\rangle$, which in this case is unambiguously decoded as $|\Sigma\lambda_j e_j\rangle = |x\rangle$.

We define a *quantoscope* (to “observe” or “measure” the system) as a set of pairs $A = \{(a_1, V_1), \ldots, (a_r, V_r)\}$ such that:

1. The a_j are distinct *real* numbers. The set $\{a_1, \ldots, a_r\}$ is the *dial* of the quantoscope, and we assume it is ordered; and
2. The V_j are non-zero vector subspaces of H such that $V_j \perp V_k$ for $j \neq k$ (orthogonality condition), and $H = \oplus_j V_j$. The latter means that any $x \in H$ can be written in a unique way as $x = x_1 + \cdots + x_r$ with $x_j \in V_j$, and the orthogonality condition implies the *Pythagoras theorem*:

   $$|x|^2 = |x_1|^2 + \cdots + |x_r|^2.$$

   Note also that $x_j = P_{V_j}(x)$ (the orthogonal projection of x on V_j). For a unit vector $u \in H$, we have

   $$1 = |u_1|^2 + \cdots + |u_r|^2,$$

   which means that the quantities $p_j = |u_j|^2$ form a *probability distribution* on the set $\{1, \ldots, r\}$.

An *observation* or *measurement* with the quantoscope A, assuming that the system is in the state $|u\rangle$ (u unitary), consists in carrying out the following two operations:

(i) to select at random a value a_j with probability $p_j = |u_j|^2$, where $u_j = P_{V_j}(u)$ (we say that a_j is the *result* or *outcome* of the observation), and

(ii) to update the state of the system to $|u_j\rangle$.
Note that $p_j \neq 0$ if a_j is selected and hence $u_j \neq 0$.

If $u \in V_j$, then $u_j = u$ and $p_j = 1$, which means that the outcome a_j of the measurement is certain and that the system's state does not change.

Let us associate to each quantoscope A the operator $\widehat{A} = \Sigma_j a_j P_{V_j}$. This operator is selfadjoint and $A \mapsto \widehat{A}$ is a one-to-one map of the set of quantoscopes to the space of selfadjoint operators of H.

Conversely, given a selfadjoint operator A', its distinct eigenvalues $a_1, \ldots, a_r$ are real, and the corresponding eigenspaces $V_1, \ldots, V_r$ are an orthogonal decomposition of H. Thus we see that $A = \{(a_1, V_1), \ldots, (a_r, V_r)\}$ is a quantoscope, and we will say that it is the quantoscope *associated to* (or *defined by*) A'.

Example

The quantoscope associated to the orthogonal projection P_V of H onto the subspace V is $\{(1, V), (0, V^{\perp})\}$. Assuming that the system is in the state $|u\rangle$, u unitary, a measurement with this quantoscope selects 1 or 0 at random with probabilities $|P_V(u)|^2$ and $|P_{V^\perp}(u)|^2$, while resetting the state to $|P_V(u)\rangle$ or $|P_{V^\perp}(u)\rangle$, respectively.

To concur with the conventional terminology, henceforth we will refer to self-adjoint operators of H as *observables* of the system.

By a *measurement* of an observable we understand a measurement with the associated quantoscope. As specified before, such a measurement supplies, if the state of the system is $|u\rangle$ (u unitary), a random eigenvalue a_j of the observable with probability $p_j = |u_j|^2$, $u_j = P_{V_j}(u)$, and resets the state of the system to $|u_j\rangle$. Note that in general the vector u_j is not unitary.

The (matrices of the) observables of $\mathbb{C}^2$ have the form

$$\begin{bmatrix} s+t & a+bi \\ a-bi & s-t \end{bmatrix}, \quad s,t,a,b \in \mathbb{R}.$$

They form a 4-dimensional real vector space with basis

$$\sigma_0 = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} & i \\ -i & \end{bmatrix}.$$

The eigenvalues of $\sigma_1, \sigma_2, \sigma_3$ are ±1 and the eigenvectors are

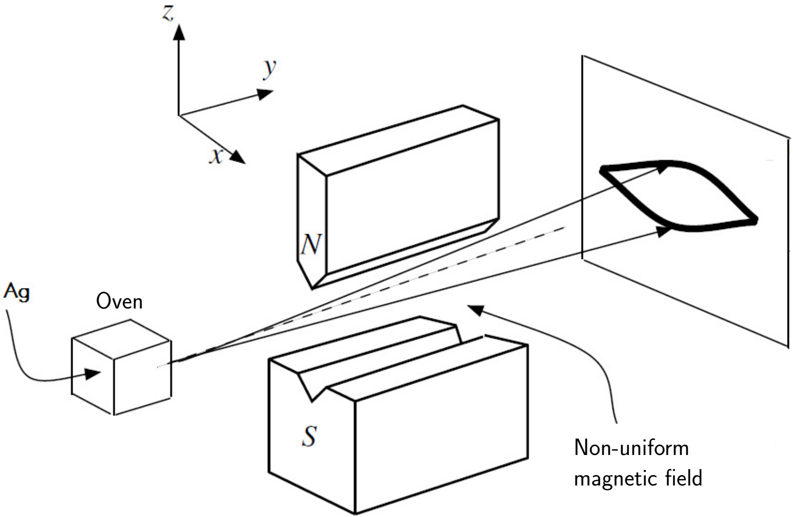
	$+1$	-1
σ_1	e_0	e_1
σ_2	$e_0 + e_1$	$e_0 - e_1$
σ_3	$ie_0 + e_1$	$ie_0 - e_1$

The q-bit heuristic model

Stern-Gerlach experiments

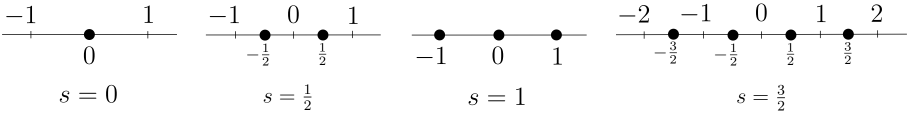
Composition of S-G experiments

Pure states of a q-bit and its state vectors



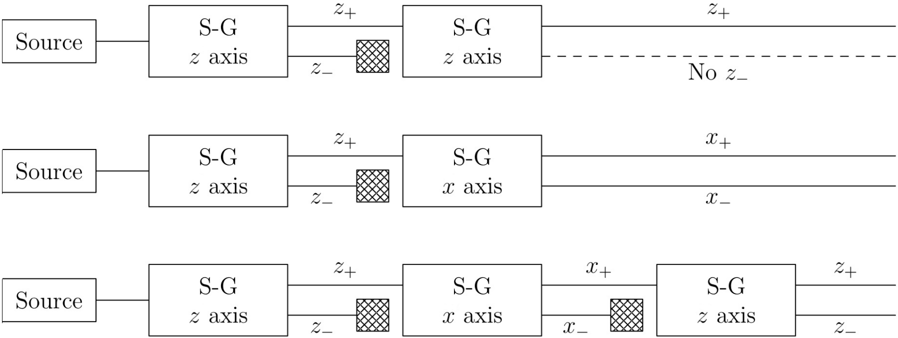
Scheme of the Stern-Gerlach experiment. N

In general, the values j observed in an SG experiment have (in appropriate units) the form $j = -s, -s+1, \ldots, s-1, s$, with s a non-negative integer or half-integer characteristic of the system. In all cases, the number of values j is $s-(-s)+1 = 2s+1$.



Possible values of spin for $s = 0, \frac{1}{2}, 1, \frac{3}{2}$.

Excluding $s=0$, corresponding to a spinless system, the simplest case (as in the original SG experiments) is $s = 1/2$, with two possible values: $j = \pm\frac{1}{2}$. It is such systems, called *quantum bits*, or simply *q-bits*, that we will consider in this section (the reasons for this naming will become clear below).

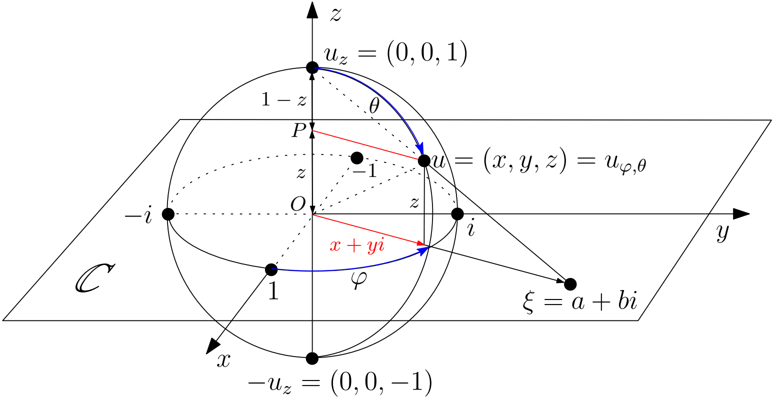


Composition of S-G experiments
(from WP, Stern–Gerlach_experiment)

- The SG experiments suggest to model the states of q-bit by the points of $\Sigma = S^2$

Henceforth we will use an orthonormal basis u_x, u_y, u_z of E_3, with u_z aligned with the SG magnetic field. As usual, a point $xu_x + yu_y + zu_z$ will also be denoted by (x, y, z).

Now on one hand $S^2 \simeq \widehat{\mathbb{C}} = \mathbb{C} \sqcup \{\infty\}$, via the stereographic projection of S^2 from the north pole $u_z = (0,0,1)$ onto the equatorial plane $z = 0$ (that we identify with $\mathbb{C}$) and with $u_z \mapsto \infty$.



Stereographic projection $u = u_{\varphi,\theta} \mapsto \xi = a + bi$ of S^2 to $\widehat{\mathbb{C}} \sqcup \{\infty\}$. The angles φ and θ (*longitude* and *colatitude* of u with respect to the orthonormal basis u_x, u_y, y_z) are the *spherical coordinates* of u.

On the other hand, $\widehat{\mathbb{C}} \simeq [\mathbb{C}^2]$, via the map $\xi \mapsto [1, \xi]$ ($\xi \in \mathbb{C}$) and $\infty \mapsto [0,1] = [e_1]$. By composing both bijections, we have a bijection $S^2 \simeq [\mathbb{C}^2]$, and so we can take the (Pauli) spinor space $\mathbb{C}^2$ as the space of state vectors of the q-bit, and identify its state space $[\mathbb{C}^2]$ with the sphere S^2.

Theorem (Stereographic projection in spherical coordinates)

Let $u = (x, y, z) \in S^2 - \{u_z\}$ and $\xi = a + bi \in \mathbb{C}$ its stereographic projection. Then

(1) $a = x/(1-z), \quad b = y/(1-z)$.

(2) $\xi = e^{i\varphi} \cot \frac{\theta}{2}$

(3) $(1, \xi) \sim (\sin \frac{\theta}{2}, e^{i\varphi} \cos \frac{\theta}{2}) \sim (e^{-i\varphi/2} \sin \frac{\theta}{2}, e^{i\varphi/2} \cos \frac{\theta}{2})$.

Proof. (1) In terms of Fig/p. 33, the right triangles $u_z O \xi$ and $u_z P u$ are similar, so $\xi/1 = (x + yi)/(1 - z)$.

(2) From (1) and $(x, y, z) = (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$, we get $\xi = (\cos\varphi\sin\theta + i\sin\varphi\sin\theta)/(1-\cos\theta) = e^{i\varphi}\frac{2\sin\theta}{\sin^2(\theta/2)} = e^{i\varphi}\cot\frac{\theta}{2}$.

(3) Immediate consequence of (2) and the definitions. □

Theorem (Inverse stereographic projection)

The expressions of (x, y, z) in terms of (a, b), or of ξ, are as follows:
(1) $x = 2a/(1 + a^2 + b^2)$, $y = 2b/(1 + a^2 + b^2)$,
$z = (a^2 + b^2 - 1)/(a^2 + b^2 + 1)$.
(2) $x = (\xi + \bar{\xi})/(\xi\bar{\xi} + 1)$, $y = i(\bar{\xi} - \xi)/(\xi\bar{\xi} + 1)$,
$z = (\xi\bar{\xi} - 1)/(\xi\bar{\xi} + 1)$.

Proof

(1) From the relations $1 - z^2 = x^2 + y^2 = (1 - z)^2(a^2 + b^2)$, we get $(1 + z)/(1 - z) = a^2 + b^2$ and from this relation we find the expression for z. Then the expressions for $x = a(1 - z)$ and $y = b(1 - z)$ follow readily.

(2) An immediate consequence of the relations
$a^2 + b^2 = \xi\bar{\xi}$, $2a = \xi + \bar{\xi}$ and $2bi = \xi - \bar{\xi}$. □

Let us use Dirac's notation $|\xi_0, \xi_1\rangle \in S^2$ to denote the state corresponding to $(\xi_0, \xi_1) \in \mathbb{C}^2$. If $\xi_0 \neq 0$, $|\xi_0, \xi_1\rangle = |1, \xi\rangle$ ($\xi = \xi_1/\xi_0$). In particular, $|1, 0\rangle = |e_0\rangle$ is the point $-u_z = (0, 0, -1)$ (the south pole of S^2). The state $|0, 1\rangle = |e_1\rangle$ is $(0, 0, 1) = u_z$, the north pole of S^2. In next statement we derive formulas for the coordinates x, y, z of $|\xi_0, \xi_1\rangle$.

Theorem (Representation of S^2 by spinors)

If $(x, y, z) = |\xi_0, \xi_1\rangle$, then

$$\begin{aligned} x &= (\xi_0\bar{\xi}_1 + \xi_1\bar{\xi}_0)/(\xi_0\bar{\xi}_0 + \xi_1\bar{\xi}_1), \\ y &= i(\xi_0\bar{\xi}_1 - \xi_1\bar{\xi}_0)/(\xi_0\bar{\xi}_0 + \xi_1\bar{\xi}_1), \\ z &= (\xi_1\bar{\xi}_1 - \xi_0\bar{\xi}_0)/(\xi_0\bar{\xi}_0 + \xi_1\bar{\xi}_1). \end{aligned} \tag{1}$$

Proof. Replace ξ in the expressions of x, y, z in Theorem/(2)/p. 36, and multiply numerators and denominators by $\xi_0\bar{\xi}_0$. □

A quaternion model of a q-bit

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$$

To replace $\mathbb{C}^2$ by the quaternion algebra $\mathbb{H}$.
This requires *choosing a complex structure* for $\mathbb{H}$, *defining a Hermitian structure* relative to that structure, and *reproducing the measurement statistics*.

Complex structure. Let $\mathbb{C} = \langle 1, \mathrm{i} \rangle \subset \mathbb{H}$. Then $\mathbb{H}$ is a $\mathbb{C}$-vector space and $\{1, \mathrm{j}\}$ is a $\mathbb{C}$-basis:

$$\mathfrak{q} = a1 + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} = (a + b\mathrm{i})1 + (c + d\mathrm{i})\mathrm{j} = \xi_0 + \xi_1\mathrm{j}.$$

Henceforth we will write $\xi_0 = \mathrm{cx}(\mathfrak{q})$.

Theorem (Complex components of $\mathfrak{q}$)

If $\mathfrak{q} = \xi_0 + \xi_1 \mathrm{j}$, $\xi_0, \xi_1 \in \mathbb{C}$, then

$$\mathrm{cx}(\mathfrak{q}) = \xi_0 = \frac{1}{2}(\mathfrak{q} - \mathrm{i}\mathfrak{q}\mathrm{i}), \quad \xi_1 = -\frac{1}{2}(\mathfrak{q}\mathrm{j} + \mathrm{i}\mathfrak{q}\mathrm{k}). \tag{2}$$

Proof. Since the expression $\frac{1}{2}(\mathfrak{q} - \mathrm{i}\mathfrak{q}\mathrm{i})$ is $\mathbb{R}$-linear in $\mathfrak{q}$, it is enough to check that it supplies $\mathfrak{q}$ for $\mathfrak{q} = 1, \mathrm{i}$ and 0 if $\mathfrak{q} = \mathrm{j}, \mathrm{k}$. In fact, if $\mathfrak{q}$ commutes with i, as is the case for the elements of $\mathbb{C}$, the formula supplies $\mathfrak{q}$, and if $\mathfrak{q}$ anti-commutes with i, as is the case for all elements of $\langle \mathrm{j}, \mathrm{k} \rangle$, it supplies 0. The second part follows similarly: $-\frac{1}{2}(\mathfrak{q}\mathrm{j} + \mathrm{i}\mathfrak{q}\mathrm{k})$ yields 0 for $\mathfrak{q} = 1, \mathrm{i}$ and $\mathfrak{q}$ for $\mathfrak{q} = \mathrm{j}, \mathrm{k}$. □

Proposition

(1) We have $\xi \mathrm{j} = \mathrm{j}\bar{\xi}$ and $\mathrm{j}\xi = \bar{\xi}\mathrm{j}$ for any $\xi \in \mathbb{C}$. Indeed, for the first relation, use that i and j anticommute. For the second, replace ξ by $\bar{\xi}$ in the first.
(2) If $\xi \in \mathbb{C}$ and $\mathfrak{q} \in \mathbb{H}$, then $\mathrm{cx}(\xi\mathfrak{q}) = \mathrm{cx}(\mathfrak{q}\xi) = \xi \mathrm{cx}(\mathfrak{q})$. This follows from the first relation in Eq. (2).
(3) For $\mathfrak{q} = \xi_0 + \xi_1 \mathrm{j}$, $\xi_0, \xi_1 \in \mathbf{C}$, $\bar{\mathfrak{q}} = \bar{\xi}_0 - \mathrm{j}\bar{\xi}_1 = \bar{\xi}_0 - \xi_1 \mathrm{j}$.

Theorem

Let $\langle\cdot|\cdot\rangle : \mathbb{H}\times\mathbb{H}\to\mathbb{C}$ be defined by $\langle\mathfrak{q}|\mathfrak{q}'\rangle = \mathrm{cx}(\mathfrak{q}'\bar{\mathfrak{q}})$. Then:
(1) $\langle\mathfrak{q}|\mathfrak{q}\rangle = \mathrm{cx}(\mathfrak{q}\bar{\mathfrak{q}}) = \mathfrak{q}\bar{\mathfrak{q}} = |\mathfrak{q}|^2$.
(2) The scalar product $\langle\mathfrak{q}|\mathfrak{q}'\rangle$ is hermitian.
(3) For $\xi_0,\xi_1,\xi_0',\xi_1'\in\mathbb{C}$ we have $\langle\xi_0+\xi_1\mathrm{j}|\xi_0'+\xi_1'\mathrm{j}\rangle = \bar{\xi}_0\xi_0'+\bar{\xi}_1\xi_1'$.
(4) For the euclidean scalar product of $\mathbb{H}$, we have
$(a+b\,\mathrm{i}+c\,\mathrm{j}+d\,\mathrm{k}, a'+b'\mathrm{i}+c'\mathrm{j}+d'\mathrm{k}) = aa'+bb'+cc'+dd'$
This is equivalent to say that the basis 1, i, j, k is orthonormal.
(5) If $v=(x,y,z)\in E_3$, let $v^*=x\,\mathrm{i}+y\,\mathrm{j}+z\,\mathrm{k}$. Then $(v^*)^2=-|v|^2$ and $|v^*|^2=|v|^2$. In particular $(v^*)^2=-1$ for any unit vector $v\in E_3$.
(6) Given $\mathfrak{q}=\xi_0+\xi_1\mathrm{j}$, let $\mathfrak{q}^\perp=-\bar{\xi}_1+\bar{\xi}_0\mathrm{j}$. Then $\mathfrak{q}^\perp$ is orthogonal to $\mathfrak{q}$ and $|\mathfrak{q}^\perp|=|\mathfrak{q}|$.

Next question is how to realize the state space of $\mathbb{H}$, which is the (abstract) sphere $[\mathbb{H}]$, as the sphere $S^2 \subset E_3$. In other words, if

$$S^3 = S^3(\mathbb{H}) = \{\mathfrak{q} \in \mathbb{H} : |\mathfrak{q}|^2 = 1\},$$

we are seeking a map $S^3 \to S^2$, $\mathfrak{q} \mapsto |\mathfrak{q}\rangle$, that is onto and such that $|\mathfrak{q}\rangle = |\mathfrak{q}'\rangle$ *if and only if* $\mathfrak{q}' \equiv \mathfrak{q}$ (this map is usually called the *Hopf fibration*).

For that, a more convenient generalized *ket map* $\kappa : \mathbb{H} \to E_3$ is defined as follows. If $\mathfrak{q} = \xi_0 + \xi_1 \mathbf{j}$ $(\xi_0, \xi_1 \in \mathbb{C})$, let $\kappa(\mathfrak{q}) = 0$ if $\mathfrak{q} = 0$, and otherwise set, with $r = |\mathfrak{q}|$, $\kappa(\mathfrak{q}) = \alpha \boldsymbol{u}_x + \beta \boldsymbol{u}_y + \gamma \boldsymbol{u}_z$, where

$$\alpha = \frac{\xi_1\bar{\xi}_0 + \xi_0\bar{\xi}_1}{r},\ \beta = \mathbf{i}\frac{\xi_0\bar{\xi}_1 - \xi_1\bar{\xi}_0}{r},\ \gamma = \frac{\xi_1\bar{\xi}_1 - \xi_0\bar{\xi}_0}{r}. \tag{3}$$

Note that these are the equations (1), p. 37, multiplied by r (in those formulas the denominator is r^2 and here it is r). It follows that $\alpha^2 + \beta^2 + \gamma^2 = r^2$, so indeed $\kappa : S^3_r \to S^2_r$. For $r = 1$, we clearly have $\kappa(\mathfrak{q}) = |\mathfrak{q}\rangle$ for any $\mathfrak{q} \in S^3$.

If $\xi_0 = a + b\mathrm{i}$, $\xi_1 = c + d\,\mathrm{i}$, $\mathfrak{q} = \xi_0 + \xi_1\mathrm{j} = a + b\mathrm{i} + c\mathrm{j} + d\,\mathrm{k}$, from Eq. (3) we get:

$$\kappa(\mathfrak{q}) = \big(2(ac+bd), 2(ad-bc), c^2+d^2-(a^2+b^2)\big)/r. \tag{4}$$

Examples

(1) $\kappa(e^{i\varphi}\mathfrak{q}) = \kappa(\mathfrak{q})$, for any $\varphi \in \mathbb{R}$. Thus $\kappa(\mathfrak{q}') = \kappa(\mathfrak{q})$ if $\mathfrak{q}' \equiv \mathfrak{q}$.

(2) $\kappa(1) = \kappa(\mathrm{i}) = -u_z$ (the south pole of S^2) and $\kappa(\mathrm{j}) = \kappa(\mathrm{k}) = u_z$ (the north pole of S^2). Note that $\mathrm{i} \equiv 1$ and $\mathrm{k} = \mathrm{ij} \equiv \mathrm{j}$, so it is enough to check that $\kappa(1) = -u_z$ and $\kappa(\mathrm{j}) = u_z$.

(3) If $\kappa(\mathfrak{q}) = u_z$ then $\mathfrak{q} \sim \mathrm{j}$.

Notation. The vectors $\mathrm{j} = \mathrm{j}^1$ and $1 = \mathrm{j}^0$ represent the parallel anti-parallel states of the q-bit. As we will see, this notations are handy to represent the state vectors of q-bit registers. For the q-bit, the equation $\mathfrak{q} = \xi_0\mathrm{j}^0 + \xi_1\mathrm{j}^1$ expresses the fact that any state is a *superposition* of the states $u_z = \kappa(\mathrm{j}^1)$ and $-u_z = \kappa(\mathrm{j}^0)$.

Theorem

The map $\kappa : S_r^3 \to S_r^2$ is surjective and for $\mathfrak{q}, \mathfrak{q}' \in S_r^3$ we have $\kappa(\mathfrak{q}') = \kappa(\mathfrak{q})$ *if and only if* $\mathfrak{q}' \equiv \mathfrak{q}$.

Proof. For $u = u_{\varphi,\theta} \in S^2$, let

$$\check{u} = \sin\tfrac{\theta}{2} + e^{\mathrm{i}\varphi}\cos\tfrac{\theta}{2}\mathrm{j} \in S^3. \tag{5}$$

Then $r\check{u} \in S_r^3$ and $\kappa(r\check{u}) = ru$. This proves surjectivity. For the second claim, see the first proof of Theorem 3 in [1]. □

Theorem

If $u = \alpha u_x + \beta u_y + \gamma u_z \in S^2 - \{u_z\}$. Then

$$\check{u} = \frac{1}{\sqrt{2(1-\gamma)}}(1 - \gamma + \alpha \mathrm{j} + \beta \mathrm{k}).$$

Proof. See Theorem 4 in [1]. □

Now let us answer the question about probabilities. Let $u \in S^2$ be a state. This defines the quantoscope $A_u = \{(-1, (-u)\check{}), (1, \check{u})\}$. What is the probability of obtaining 1 if before measurement with A_u the state is $v \in S^2$? The answer is given by the following result, which is in agreement with the experimental statistics.

Theorem

The probability of observing 1 with A_u, if the state before measurement is $v \in S^2$, is $p_u(v) = \cos^2(\alpha/2)$, where α is the euclidean angle between u and v (that is, $\cos(\alpha) = u \cdot v$).

Proof. According to the way measurement with A_u works, $p_u(v) = |\langle\check{u}|\check{v}\rangle|^2$, with $\langle\check{u}|\check{v}\rangle = \mathrm{cx}(\check{v}\bar{\check{u}})$. The result is obtained on inserting the expressions for $\check{u}$ and $\check{v}$ in spherical coordinates and then going through a little trigonometric joggling. See Theorem 5 in [1] for details. □

The proof of the preceding theorem shows that $|\langle \check{u}|\check{v}\rangle|^2 = \cos^2(\alpha/2)$. Therefore $\cos(\alpha/2) = |\langle \check{u}|\check{v}\rangle| = \cos(\beta)$, where $\beta = \beta(\check{u}, \check{v})$, and hence $\beta = \alpha/2$.

Example. If $u = u_{\varphi,\theta} \in S^2$, then $\alpha(u, -u) = \pi$. It follows that $\beta(\check{u}, (-u)\check{}) = \pi/2$, which means that $\check{u}$ and $(-u)\check{}$ must be orthogonal.

This can be checked directly by using the trigonometric expressions $\check{u} = s + ce^{\mathrm{i}\varphi}\mathrm{j}$ and $(-u)\check{} = \check{u}_{\varphi+\pi,\pi-\theta} = c - se^{\mathrm{i}\varphi}$, where $s = \sin\frac{\theta}{2}$ and $c = \cos\frac{\theta}{2}$.

Let $\mathfrak{u} \in S^3(\mathbb{H})$ and define $D_{\mathfrak{u}}$ as the observable associated to the quantoscope $\{(1, \mathfrak{u}), (-1, \mathfrak{u}^{\perp})\}$: $D_{\mathfrak{u}} = P_{\mathfrak{u}} - P_{\mathfrak{u}^{\perp}}$. It is self-adjoint and unitary, and it does not change if $\mathfrak{u}$ or $\mathfrak{u}^{\perp}$ is multiplied by a phase factor (as $P_{\mathfrak{u}} = P_{\langle \mathfrak{u} \rangle}$, by definition). Since $D_{\mathfrak{u}}^2 = I$, and hence $(\mathrm{i}D_{\mathfrak{u}})^2 = -I$, we have

$$e^{\mathrm{i}\alpha D_{\mathfrak{u}}} = \cos(\alpha) I + \sin(\alpha)\, \mathrm{i} D_{\mathfrak{u}}. \tag{6}$$

Theorem

The vectors $\mathfrak{u}$ and $\mathfrak{u}^{\perp}$ are eigenvectors of the operator $U_{\underline{,}\alpha} = e^{\mathrm{i}\alpha D_{\mathfrak{u}}}$ and the corresponding eigenvalues are $e^{\mathrm{i}\alpha}$ and $e^{-\mathrm{i}\alpha}$.

Proof. We have

$$U_{\mathfrak{u},\alpha}(\mathfrak{u}) = \cos(\alpha)(\mathfrak{u}) + \sin(\alpha)\, \mathrm{i} D_{\mathfrak{u}}(\mathfrak{u}) = \cos\alpha\, \mathfrak{u} + \sin\alpha\, \mathrm{i}\mathfrak{u} = e^{\mathrm{i}\alpha}\mathfrak{u},$$

as $D_{\mathfrak{u}}(\mathfrak{u}) = \mathfrak{u}$. The reasoning for $\mathfrak{u}^{\perp}$ is similar. □

Theorem

The rotation of E_3 about $u \in S^2$ of amplitude 2α is given by $R_{u,2\alpha}(v) = \kappa(U_{\check{u},\alpha}\check{v})$.

Proof. See Theorem 9 in [1]. □

Given $U \in \mathrm{SU}(\mathbb{H})$, define the rotation $R_U : E_3 \to E_3$ by the relation $R_U(v) = \kappa(U\check{v})$.

Theorem

The axis of R_U is $\langle\kappa(\mathfrak{u})\rangle$, where $\mathfrak{u}$ is **any** unit eigenvector of U, and its amplitude 2α is determined by the relation $2\cos\alpha = \mathrm{tr}(U)$.

Proof. See Theorem 10 in [1]. □

(1) If $u = u_{\varphi,\theta} = (x, y, z)$, the matrix of the operator $D_{\check{u}}$ with respect to the basis $\{1, \mathrm{j}\}$ is

$$\begin{bmatrix} -\cos\theta & e^{-\mathrm{i}\varphi}\sin\theta \\ e^{\mathrm{i}\varphi}\sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} -z & x - \mathrm{i}y \\ x + \mathrm{i}y & z \end{bmatrix}. \tag{7}$$

In particular, abridging $D_{\check{u}_x}, D_{\check{u}_y}, D_{\check{u}_z}$ to X, Y, Z, we have:

$$X \simeq \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \; Y \simeq \begin{bmatrix} & -\mathrm{i} \\ \mathrm{i} & \end{bmatrix}, \; Z \simeq \begin{bmatrix} -1 & \\ & 1 \end{bmatrix}.$$

(2) The matrix of $U_{\check{u},\alpha} = e^{\mathrm{i}D_{\check{u}}\alpha}$ with respect to the same basis is

$$\begin{bmatrix} \cos\alpha - \mathrm{i}\cos\theta\sin\alpha & \mathrm{i}e^{-\mathrm{i}\varphi}\sin\theta\sin\alpha \\ \mathrm{i}e^{\mathrm{i}\varphi}\sin\theta\sin\alpha & \cos\alpha + \mathrm{i}\cos\theta\sin\alpha \end{bmatrix}$$

$$= \begin{bmatrix} \cos\alpha - \mathrm{i}z\sin\alpha & y + \mathrm{i}x \\ -y + \mathrm{i}x & \cos\alpha + \mathrm{i}z\sin\alpha \end{bmatrix} \tag{8}$$

(3) In particular we have

$$U_{\check{u}_x,\alpha} = e^{\mathrm{i}\alpha X} \simeq \begin{bmatrix} \cos\alpha & \mathrm{i}\sin\alpha \\ \mathrm{i}\sin\alpha & \cos\alpha \end{bmatrix}$$

$$U_{\check{u}_y,\alpha} = e^{\mathrm{i}\alpha Y} \simeq \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

$$U_{\check{u}_z,\alpha} = e^{\mathrm{i}\alpha Z} \simeq \begin{bmatrix} e^{-\mathrm{i}\alpha} & \\ & e^{\mathrm{i}\alpha} \end{bmatrix}.$$

Proof. See §**20** in [1]. □

Registers of q-bits

The algebra $\mathbb{H}^{(n)}$ of a q-register

Basis of $\mathbb{H}^{(n)}$ derived from $\{1, \mathbf{j}\}$

Split elements and the Segre conditions

The state space $\Sigma_n = \mathbb{P}\mathbb{H}^{(n)}$

Split and entangled states

If $H_1, \dots, H_n$ are the hermitian spaces of n quantum systems, the hermitian space $H_1 \otimes \cdots \otimes H_n$ defines the composition of those systems.[2]

The hermitian scalar product of the composite system is determined by the following rule:

$$\langle x_1 \otimes \cdots \otimes x_n | x_1' \otimes \cdots \otimes x_n' \rangle = \langle x_1 | x_1' \rangle \cdots \langle x_n | x_n' \rangle.$$

[2] We refer to [2] for a justification of this postulate.

The hermitian space of n qbits, considered as a single quantum system, is $\mathbb{H}^{(n)} = \mathbb{H}^{\otimes n}$, where the n factors $\mathbb{H}$ refer to the ordered array formed by the q-bits.

This description has an *important feature that is not present in the conventional treatment* of q-registers: $\mathbb{H}^{(n)}$ is a *unital associative* $\mathbb{C}$*-algebra*. Its structure is determined by $\mathbb{C}$-multilinearity and the rule

$$(\mathfrak{q}_1 \otimes \cdots \otimes \mathfrak{q}_n)(\mathfrak{q}_1' \otimes \cdots \otimes \mathfrak{q}_n') = (\mathfrak{q}_1\mathfrak{q}_1') \otimes \cdots \otimes (\mathfrak{q}_n\mathfrak{q}_n'). \tag{9}$$

The Hermitian scalar product of $\mathbb{H}^{(n)}$ is determined by the rule

$$\langle \mathfrak{q}_1 \otimes \cdots \otimes \mathfrak{q}_n | \mathfrak{q}_1' \otimes \cdots \otimes \mathfrak{q}_n' \rangle = \langle \mathfrak{q}_1 | \mathfrak{q}_1' \rangle \cdots \langle \mathfrak{q}_n | \mathfrak{q}_n' \rangle \tag{10}$$

and $\bar{\mathbb{C}}/\mathbb{C}$-multilinearity. We note that $\mathfrak{q}_1 \otimes \cdots \otimes \mathfrak{q}_n$ *and* $\mathfrak{q}_1' \otimes \cdots \otimes \mathfrak{q}_n'$ *are orthogonal if and only if* $\mathfrak{q}_k$ *and* $\mathfrak{q}_k'$, for some $k \in 1..n$, are orthogonal. Note also that

$$|\mathfrak{q}_1 \otimes \cdots \otimes \mathfrak{q}_n|^2 = |\mathfrak{q}_1|^2 \cdots |\mathfrak{q}_n|^2. \tag{11}$$

Let $B = \{0, 1\}$. For each $\nu = (\nu_1, \ldots, \nu_n) \in B^n$, set

$$\mathsf{j}^{\nu} = \mathsf{j}^{\nu_1} \otimes \cdots \otimes \mathsf{j}^{\nu_n} \in \mathbb{H}^{(n)}.$$

Then $\{\mathsf{j}^{\nu} \mid \nu \in B^n\}$ *is an orthonormal basis* of $\mathbb{H}^{(n)}$ and hence a general element of $\mathbb{H}^{(n)}$ has the form

$$\xi = \sum_{\nu \in B^n} \xi_{\nu} \mathsf{j}^{\nu},\ \xi_{\nu} \in \mathbb{C}.$$

We have $\mathsf{j}^{\nu}\mathsf{j}^{\nu'} = \epsilon(\nu, \nu')\mathsf{j}^{\nu+\nu'}$, where $\epsilon(\nu, \nu')$ is the parity of the number of $k \in 1..n$ such that $\nu_k = \nu'_k = 1$, that is, the parity of the number of 1's in $\nu\nu'$ (component-wise binary product).

Remark. Classical computations happen in B^n. Quantum computations happen in $\mathbb{H}^{(n)}$, where the binary space B^n appears just as indices for the basis $\{\mathsf{j}^{\nu}\}$ of $\mathbb{H}^{(n)}$.

Remark. j^{ν} *corresponds to the popular notation* $|\nu\rangle$.

The *Hadamard q-vector of order n* is defined as

$$\boldsymbol{h}^{(n)} = \rho^n \sum_{\nu \in B^n} j^{\nu},$$

where $\rho = 1/\sqrt{2}$. Since the norm squared of $\sum_{\nu \in B^n} j^{\nu}$ is $|B^n| = 2^n$, the factor ρ^n insures that $\boldsymbol{h}^{(n)}$ is a unit vector.

We also have the expression

$$\boldsymbol{h}^{(n)} = \rho^n (j^0 + j^1) \otimes \overset{n)}{\cdots} \otimes (j^0 + j^1).$$

Indeed, to expand this product we have to choose 0 or 1 in each factor, which makes for 2^n choices, and for the choice $\nu = \nu_0, \ldots, \nu_n$ we get j^{ν}.

An element $\xi \in \mathbf{H}^{(n)}$ is said to be *composite* (or *split*) if it is of the form $\xi = \mathfrak{q}_1 \otimes \cdots \otimes \mathfrak{q}_n$, with $\mathfrak{q}_1, \ldots, \mathfrak{q}_n \in \mathbb{H}$.

The ν component of this element is $\xi_\nu = \xi_{\nu_1}(\mathfrak{q}_1) \cdots \xi_{\nu_n}(\mathfrak{q}_n)$, where we set, for $\mathfrak{q} \in \mathbb{H}$, $\mathfrak{q} = \xi_0(\mathfrak{q}) + \xi_1(\mathfrak{q})\mathrm{j}$. Now *these ξ_ν are not independent*. Indeed, we can write relations among them as follows.

Partition the ν's into those that begin with 0 and those that begin with 1. Then form the $2 \times 2^{n-1}$ matrix whose rows correspong to the ξ_ν's of these two groups. Since the two rows are proportional, all the 2×2 minors of the matrix vanish. These are the *Segre relations* and it happens that they are also sufficient (and in general redundant) to insure that a vector $\xi \in \mathbb{H}^{(n)}$ is split. N

For $n = 2$, we get a single relation: $\det \begin{bmatrix} \xi_{00} & \xi_{01} \\ \xi_{10} & \xi_{11} \end{bmatrix} = 0$. For $n = 3$ we have the matrix $\begin{pmatrix} \xi_{000} & \xi_{001} & \xi_{010} & \xi_{011} \\ \xi_{100} & \xi_{101} & \xi_{110} & \xi_{111} \end{pmatrix}$ and 6 relations.

The vectors that are not split are said to be *entangled*. For $n = 2$, the vector $\xi^{\mathrm{EPR}} = \mathsf{j}^{00} + \mathsf{j}^{11}$ is entangled. A random element of $\mathbb{H}^{(n)}$, $n \geqslant 2$, is entangled, in the (technical) sense that the composite vectors form a set of measure zero.

By definition, $\Sigma_n = \mathbf{H}^{(n)} - \{0\}/\sim$, a space of complex dimension $2^n - 1$. Let

$$\kappa : \mathbf{H}^{(n)} - \{0\} \to \Sigma_n$$

be the ket map, which by definition is onto and satisfies $\kappa(\xi) = \kappa(\xi')$ if and only if $\xi \sim \xi'$.

The condition for $\xi \in \mathbf{H}^{(n)}$ to be a unit vector is that

$$\sum_{\nu\in B^n} |\xi_\nu|^2 = 1.$$

This equation represents the *unit sphere* of the Euclidean space $\mathbb{H}_{\mathbb{R}}^{(n)}$. Since this Euclidean space has of dimension $2 \times 2^n = 2^{n+1}$, that sphere is denoted by $S^{2^{n+1}-1}$, and thus

$$\Sigma_n = S^{2^{n+1}-1}/\equiv.$$

The map $\kappa : S^{2^{n+1}-1} \to \Sigma_n$ is onto and with the property that $\kappa(\xi) = \kappa(\xi')$ if and only if $\xi \equiv \xi'$.

For $n = 1, 2, 3$ the (real) dimension of these spheres is $3, 7, 15$ and hence the real dimension of Σ_n is $2, 6, 14$.

A state $\kappa(\xi)$ is said to be *composite* if ξ is a composite vector. This is well defined, because if ξ is composite and $\xi \sim \xi'$, then ξ' is composite.

Let $\Sigma'_n \subset \Sigma_n$ be the set of composite states. We have an onto map $(S^2)^n \to \Sigma'_n$ defined by

$$(v_1, \ldots, v_n) \mapsto \kappa(\check{v}_1 \otimes \cdots \otimes \check{v}_n).$$

This shows that entangled states are specified by $2n$ real parameters, or n complex parameters, whereas general states are specified by $2^n - 1$ complex parameters. This again confirms the assertion that *a random state is entangled*.

q-gates and q-computations

The evolution of the system H in a time interval $[0, t]$ is governed by a unitary operator U_t, in the sense that if $\xi_0 \in H$ represents the state of the system at time $t = 0$, then $U_t\xi_0$ represents the state of the system at time t.

If $U_t = e^{\mathrm{i}\mathfrak{h}t}$, where $\mathfrak{h}$ is an observable, we say that the evolution is *hamiltonian*, and that $\mathfrak{h}$ is the *hamiltonian* of the system. Notice that it is indeed a unitary operator: $e^{\mathrm{i}\mathfrak{h}t}(e^{\mathrm{i}\mathfrak{h}t})^\dagger = e^{\mathrm{i}\mathfrak{h}t}e^{-\mathrm{i}\mathfrak{h}^\dagger t} = I$.

If the evolution of the system is hamiltonian and the hamiltonian $\mathfrak{h}$ does not depend on t, then the state vector $x = U_t x_0$ satisfies the *Schrödinger equation*: $\dot{x} = \mathrm{i}\mathfrak{h}x$.

Example. The operator $U_{u,2\alpha} = e^{\mathrm{i}\alpha D_{\breve{u}}}$ introduced in the first Theorem on p. 50 provides, as a function of α, a hamiltonian evolution in $\mathbb{H}$ with $\mathfrak{h} = D_{\breve{u}}$. In this case Scrödinger's equation says that $\dot{\mathfrak{q}} = \mathrm{i}D_{\breve{u}}\mathfrak{q}$. This fact is important in relation to the engineering of q-computers, as it is the basis for implementing rotating operations of q-bit.

A q-*computation of order* n is a unitary operator $U : \mathbb{H}^{(n)} \to \mathbb{H}^{(n)}$. With the composition, these operators form the unitary group of $\mathbb{H}^{(n)}$ that here will be denoted by $\mathcal{U}^{(n)}$. Since $UU^\dagger = I$, $U^{-1} = U^\dagger$. We express this by saying that q-computations are *reversible* and that the reverse of a q-computation U is $U^\dagger$.

The matrix of a q-computation U with respect to the orthonormal basis $\{j^\nu\}$ is the unitary matrix $\boldsymbol{U} = (u^\nu_{\nu'})_{\nu,\nu' \in B^n}$ defined by

$$U(j^\nu) = \sum_{\nu' \in B^n} u^\nu_{\nu'} \mathrm{j}^{\nu'}.$$

These unitary matrices form a group, $\boldsymbol{\mathcal{U}}^{(n)}$, with the multiplication operation, and the map $\mathcal{U}^{(n)} \to \boldsymbol{\mathcal{U}}^{(n)}$, $U \mapsto \boldsymbol{U}$, is an isomorphism.

If $\boldsymbol{\xi}$ is the row of components of $\xi \in \mathbf{H}^{(n)}$, and $\mathbf{j}$ the column formed with the j^ν, then we have (using Einstein's summation criterion) that

$$U(\xi) = \xi_\nu U(\mathrm{j}^\nu) = \xi_\nu u^\nu_{\nu'} \mathrm{j}^{\nu'} = \boldsymbol{\xi}\boldsymbol{U}\mathbf{j}.$$

This means that the row of components of $U(\xi)$ is $\boldsymbol{\xi}\boldsymbol{U}$.

A reversible classical computation on n bits is a bijective map $f : B^n \to B^n$. To this map we may associate the linear map $U_f = \mathbb{H}^{(n)} \to \mathbb{H}^{(n)}$ that is uniquely defined by imposing that $U_f(\mathrm{j}^{\nu}) = \mathrm{j}^{f(\nu)}$. Since $\nu \mapsto f(\nu)$ is a permutation of the ν's, U_f permutes the j^{ν}, so it is unitary, and hence a q-computation of order n. We say that U_f is the *q-computation defined by* f. As we will se below, some of the fundamental q-computations are defined by classical reversible computations.

The only classical computations on one bit ν are the identity and the negation. If we denote the negation by $\textsc{not}$, we can write $\textsc{not}(\nu) = 1 + \nu$. Thus $\textsc{not}(0) = 1$ and $\textsc{not}(1) = 0$. The *q*-computation defined by $\textsc{not}$ is the operator X defined in Theorem/(1), p. 51, as $X(\mathrm{j}^{\nu}) = \mathrm{j}^{1+\nu}$.

In contrast to the classical computations, the *q*-computations of order 1 are given by unitary operators of $\mathbb{H}$. Two additional simple cases are the operators Y and Z defined in Theorem/(1), p. 51: $Y(\mathrm{j}^{\nu}) = (-1)^{\nu}\mathrm{i}\mathrm{j}^{1+\nu}$ and $Z(\mathrm{j}^{\nu}) = (-1)^{1+\nu}\mathrm{j}^{1+\nu}$. The significance of X, Y, Z in relation to rotations of E_3 has been established in Theorem/(3), p. 51.

Two other important examples of *q*-computations of order 1 are the *Hadamard gate*, H, and the *phase gate*, U_α ($\alpha \in [0, 2\pi)$).

They are defined as follows: $\mathrm{H}(\mathsf{j}^\nu) = \frac{1}{\sqrt{2}}(\mathsf{j}^0 + (-1)^\nu \mathsf{j}^1)$ and $\mathrm{U}_\alpha(\mathsf{j}^0) = \mathsf{j}^0$ and $\mathrm{U}_\alpha(\mathsf{j}^1) = e^{i\alpha}\mathsf{j}^1$.

Their matrices are $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $\operatorname{diag}(1, e^{i\alpha})$, respectively. The latter is hamiltonian, with $\mathfrak{h} = P_\mathsf{j}$, for $P_\mathsf{j} \simeq \operatorname{diag}(0, 1)$ and hence $e^{\mathrm{i}P_\mathsf{j}\alpha} \simeq \operatorname{diag}(1, e^{i\alpha})$.

The *controlled*-NOT *gate* is the *q*-computation of order 2 defined as follows: $\textsc{cnot}(\mathsf{j}^{\nu_1}\mathsf{j}^{\nu_2}) = \mathsf{j}^{\nu_1}\mathsf{j}^{\nu_1+\nu_2}$. If $\nu_1 = 0$, it does nothing, and when $\nu_1 = 1$ it negates the second *q*-bit. It corresponds to the classical computation $B^2 \to B^2$, $(\nu_1, \nu_2) \mapsto (\nu_1, \nu_1 + \nu_2)$.

If U is a q-computation of order 1, it can be applied to any one of the q-bits of a q-register. If we let U_s denote the operator U when applied to the s-th q-bit, its action is determined by the following rule: $U_s(\mathrm{j}^{\nu}) = \mathrm{j}^{\nu_1} \otimes \cdots \otimes \mathrm{j}^{\nu_{s-1}} \otimes U(\mathrm{j}^{\nu_s}) \otimes \mathrm{j}^{\nu_{s+1}} \otimes \cdots \otimes \mathrm{j}^{\nu_n}$. More generally, it can be applied to the q-bits whose indices are $s_1 < \cdots < s_p$, in which case it will be denoted $U_{s_1,\dots,s_p}$. For example, $\mathrm{H}_{1,2,\dots,n}(j^{00\cdots0}) = \boldsymbol{h}^{(n)}$, the Hadamard q-vector of order n (see the Example on p. 57). Similarly, CNOT can be applied to any two q-bits in a q-register. If we let r, s be the indices of the two q-bits, $\mathrm{CNOT}_{r,s}$ maps $\cdots \otimes \mathrm{j}^{\nu_r} \otimes \cdots \otimes \mathrm{j}^{\nu_s} \otimes \cdots \mapsto \cdots \otimes \mathrm{j}^{\nu_r} \otimes \cdots \otimes \mathrm{j}^{\nu_r+\nu_s} \otimes \cdots$.

In general, a *q-program* is a finite sequence of gates that can be of the form U_s, where U is a phase gate or a Hadamard gate, or of the form $\mathrm{CNOT}_{r,s}$. The composition of these gates is a q-computation of order n and the main result of the theory of quantum computation is that any q-computation of order n can be obtained by a q-program. For references, see [3].

The result of a q-computation U with input vector ξ is the value $\nu \in B^n$ supplied by a measure of the output state $\xi' = U\xi$ by means of the quantoscope $\{(\nu, \mathrm{j}^\nu)\}_{\nu \in B^n}$. The probability of getting a particular ν is $|\langle \mathrm{j}^\nu | \xi' \rangle|^2 = |\xi'_\nu|^2$, and after measurement the system state is set to $\kappa(\mathrm{j}^\nu)$.

For many applications it is also important to measure any given subset of q-bits. This can be explained as follows. Let

$$J = \{j_1, \ldots, j_m\} \; (1 \leqslant j_1 < \cdots < j_m \leqslant n)$$

be the positions of the q-bits to be measured. For any $\lambda \in B^m$, let $F_\lambda \subset \mathbb{H}^{(n)}$ be the space generated by the j^ν such that $\nu_{j_s} = \lambda_s$ for $s = 1, \ldots, m$. Then $\{(\lambda, F_\lambda)\}_{\lambda \in B^m}$ is a quantoscope that measures the bits at the positions J. Assuming that the state vector before measuring is ξ, it supplies a value $\lambda \in B^m$ with probability $p_\lambda = |P_{F_\lambda}(\xi)|^2$ and resets the state to $\kappa(P_{F_\lambda}(\xi))$. It is clear that $P_{F_\lambda}(\xi) = \sum_{\nu_{j_s} = \lambda_s} \xi_\nu \mathrm{j}^\nu$, hence $p_\lambda = \sum_{\nu_{j_s} = \lambda_s} |\xi_\nu|^2$.

Example. If we want to measure the first *q*-bit of a *q*-register or order 3, then $m = 1$, $B^m = B$, $\lambda \in B$, and $F_\lambda = \langle \mathrm{j}^{\lambda 00}, \mathrm{j}^{\lambda 01}, \mathrm{j}^{\lambda 10}, \mathrm{j}^{\lambda 11}\rangle$. In this case $P_{F_\lambda}(\xi) = \sum_{\nu_1=\lambda} \xi_\nu \mathrm{j}^\nu$, its square norm is $p_\lambda = \sum_{\nu_1=\lambda} |\xi_\nu|^2$, and after the measurement the state is set to $\kappa(\sum_{\nu_1=\lambda} \xi_\nu \mathrm{j}^\nu)$.

Conclusions and outlook

- Introduction to Hermitian spaces, with highlightings of some important concepts, like the Hermitian angle.

- Hermitian structure of $\mathbb{H} = \mathcal{G}_3^+$ (the *geometric quaternions*) and its use for a geometric algebra account of a q-bit.

- The *algebras* $\mathbb{H}^{(n)}$, that supply a transparent formalism for modeling q-bit registers of arbitrary length, both conceptually and computationally. Especially apt to encode quantum gates.

- Segre relations and entanglement. One step further would be to tackle in this formalism references such as [4] and some related works of Jordi Tura (`https://jtura.cat/`), particularly his memoir [5].

- The algebras $\mathbb{H}^{(n)}$ may be a suitable resource for research in discreet mathematics, as for example quantum error-correcting codes.

Thank you!

sebastia.xambo@upc.edu

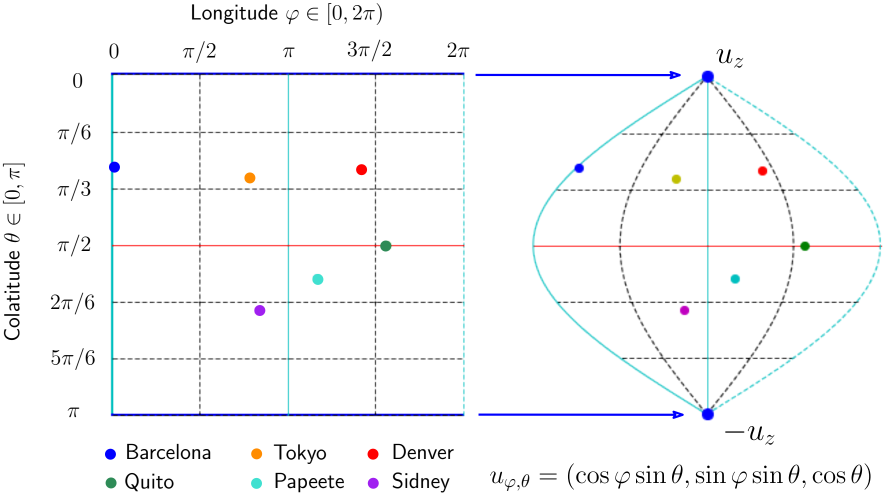
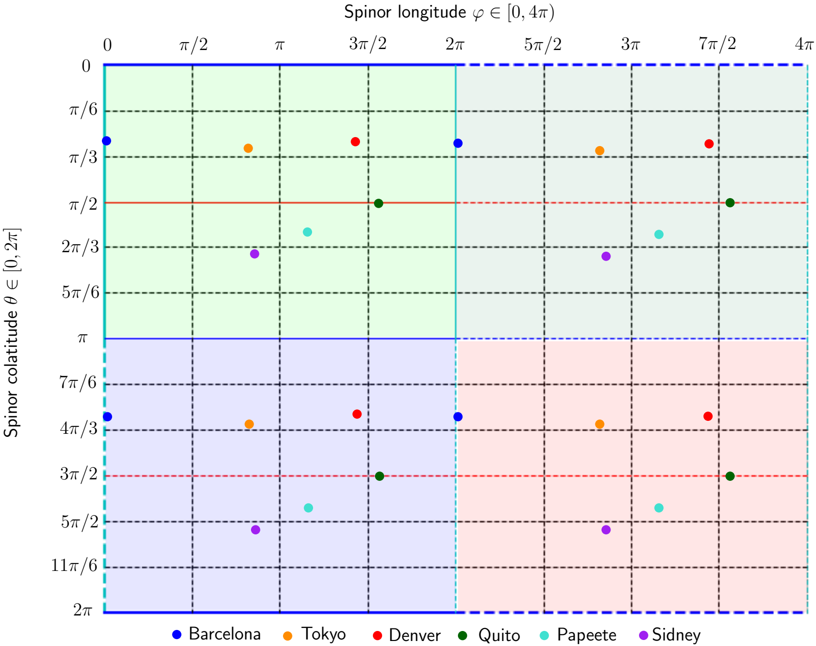

Longitude $\varphi \in [0, 2\pi)$
0
$\pi/2$
π
$3\pi/2$
2π
Colatitude $\theta \in [0, \pi]$
0
$\pi/6$
$\pi/3$
$\pi/2$
$2\pi/6$
$5\pi/6$
π
u_z
$-u_z$
● Barcelona
● Tokyo
● Denver
● Quito
● Papeete
● Sidney
$u_{\varphi,\theta} = (\cos\varphi \sin\theta, \sin\varphi \sin\theta, \cos\theta)$

Figura 16.1: On the left, we have the rectangle of points (φ, θ) with $\varphi \in [0, 2\pi)$ and $\theta \in [0, \pi]$. The parameter φ is the *longitude* measured eastward from a given meridian (vertical segment on the left, in cyan), say the Greenwich one. The parameter θ is the *colatitude* and is measured along a meridian from the north pole u_z to the south pole $-u_z$.

← N



Spinor longitude $\varphi \in [0, 4\pi)$
0
$\pi/2$
π
$3\pi/2$
2π
$5\pi/2$
3π
$7\pi/2$
4π
Spinor colatitude $\theta \in [0, 2\pi]$
0
$\pi/6$
$\pi/3$
$\pi/2$
$2\pi/3$
$5\pi/6$
π
$7\pi/6$
$4\pi/3$
$3\pi/2$
$5\pi/2$
$11\pi/6$
2π
● Barcelona
● Tokyo
● Denver
● Quito
● Papeete
● Sidney

The geometric algebra $\mathcal{G}_n$

We denote the *geometric algebra* of the euclidean space E_n by $\mathcal{G}_n$.

Its elements are called *multivectors*.

The *geometric*, *wedge*, and *inner* products of two multivectors x, x' are denoted by xx', $x \wedge x'$, and $x \cdot x'$, respectively (the wedge product is also called *outer* or *exterior* product). They are bilinear and the first two, xx' and $x \wedge x'$, are *associative*.

We first summarize a few general facts about $\mathcal{G}_n$ and at the end we consider the particularities about $\mathcal{G}_2$ and $\mathcal{G}_3$ needed later.

With the wedge product, $\mathcal{G}_n$ *coincides with the exterior algebra of* E_n, so that $\mathcal{G}_n = \oplus_{k=0}^{n} \mathcal{G}_n^k$, where $\mathcal{G}_n^k$ is spanned, as a real vector space, by the nonzero outer products of the form $v_1 \wedge \cdots \wedge v_k$, $v_1, \ldots, v_k \in E_n$ (such outer products are called k-*blades*, and the elements of $\mathcal{G}_n^k$, k-*vectors*).

Since, $\mathcal{G}_n^0 = \mathbb{R}$ and $\mathcal{G}_n^1 = E_n$, the 0-vectors are *scalars* and the 1-vectors are just *vectors*. *Bivector* is a synonym of 2-vector, and *pseudoscalar* of n-vector.

The k-blades $x = v_1 \wedge \cdots \wedge v_k$ represent oriented k-volumes of E_n (oriented areas when $k = 2$). Note that the condition $v \wedge x = 0$ is equivalent $v \in \langle v_1, \ldots, v_k \rangle$. This shows that the latter space can be denoted L_x. Then it is clear that $L_{\lambda x} = L_x$ for any non-zero scalar λ, and in fact this is the only redundancy, in the sense that *two k-blades represent the same linear space if and only if they are proportional* ($x' \sim x$ is our preferred notation).

It generalizes the euclidean scalar product $v \cdot v' \in \mathbb{R}$ of vectors to a product $x \cdot x' \in \mathcal{G}_n$ for any $x, x' \in \mathcal{G}_n$, and the following rules are sufficient to evaluate all cases:

(1) $\lambda \cdot x = x \cdot \lambda = 0$ for any scalar λ and any multivector x.
By bilinearity we may assume $x \in \mathcal{G}_n^k$, $x' \in \mathcal{G}_n^{k'}$, $k, k' \geqslant 1$.

(2) If $k > k'$, $x \cdot x' = (-1)^{kk'+k'} x' \cdot x$. So we may assume $k \leqslant k'$.

(3) If $k = 1$, so $x = v \in E_n$, and $x' = v'_1 \wedge \cdots \wedge v'_{k'}$, $v'_1, \ldots, v'_{k'} \in E_n$,
$x \cdot x' = \sum_{i=1}^{k'} (-1)^{i-1} (v \cdot v'_i) v'_1 \wedge \cdots \wedge v'_{i-1} \wedge v'_{i+1} \wedge \cdots \wedge v'_{k'}$.

(4) If $x = v_1 \wedge \cdots \wedge v_k$, $2 \leqslant k \leqslant k'$, $x \cdot x' = (v_1 \wedge \cdots \wedge v_{k-1}) \cdot (v_k \cdot x')$.

The geometric product is determined by the following rule:

If $v \in E_n$, then $vx = v \cdot x + v \wedge x$ for any multivector x.

In particular we see, given vectors $v, v' \in E_n$, that

$v^2 = v \cdot v$ (for $v \wedge v = 0$) and that $vv' = -v'v \Leftrightarrow v \cdot v' = 0$.

Notice that $2v \cdot v' = vv' + v'v$ and $2v \wedge v' = vv' - v'v$.

With the geometric product, $\mathcal{G}_n$ is isomorphic to the *Clifford algebra* of E_n.

It is the linear automorphism of $\mathcal{G}_n$, $x \mapsto \hat{x}$, such that $\hat{x} = (-1)^k x$ for all $x \in \mathcal{G}_n^k$. It is an *involution* (that is, $\hat{\hat{x}} = x$ for all x) called the *parity* or *grade involution* of $\mathcal{G}_n$.

It is an automorphism for the geometric, wedge, and inner products:

$\widehat{xx}' = \hat{x}\hat{x}'$, $\widehat{x \wedge x}' = \hat{x} \wedge \hat{x}'$, and $\widehat{x \cdot x}' = \hat{x} \cdot \hat{x}'$.

The set $\mathcal{G}_n^+ = \{x \in \mathcal{G}_n \,|\, \hat{x} = x\}$ is the *even* subalgebra. It elements are the multivectors that have no odd grades.

The set $\mathcal{G}_n^- = \{x \in \mathcal{G}_n \,|\, \hat{x} = -x\}$ is a vector subspace of $\mathcal{G}_n$ and its elements are the multivectors that have no even grades.

Clearly, $\mathcal{G}_n = \mathcal{G}_n\psi \oplus \mathcal{G}_n^-$.

Reverse involution

It is the linear automorphism of $\mathcal{G}_n$, $x \mapsto \tilde{x}$, such that $\tilde{x} = (-1)^{k/\!\!/2}x$ for $x \in \mathcal{G}_n^k$, where $k/\!\!/2 = \lfloor k/2 \rfloor$.

It is an *involution* (that is, $\tilde{\tilde{x}} = x$ for all x). It is called the *reverse involution* because

$$\begin{aligned}(v_1 \wedge \cdots \wedge v_k)^\sim &= (-1)^{k/\!\!/2} v_1 \wedge \cdots \wedge v_k \\ &= (-1)^{\binom{k}{2}} v_1 \wedge \cdots \wedge v_k = v_k \wedge \cdots \wedge v_1\end{aligned}$$

(we have used that $k/\!\!/2$ has the same parity as $\binom{k}{2}$).

It is an *antiisomorphism* of $\mathcal{G}_n$ in the sense that

$\widetilde{xx}' = \tilde{x}'\tilde{x}$, $\widetilde{x \wedge x}' = \tilde{x}' \wedge \tilde{x}$, and $\widetilde{x \cdot x}' = \tilde{x}' \cdot \tilde{x}$.

The composition of the parity and reverse involutions is the *Clifford involution*, $x \mapsto \bar{x}$. It is an anti-automorphism of $\mathcal{G}_n$ (for the three products), and $\bar{x} = (-1)^{(k+1)/\!\!/2}x$ for $x \in \mathcal{G}_n^k$.

If $\boldsymbol{e} = e_1, \ldots, e_n$ is a basis of E_n, then the k-vectors

$$e_J = e_{j_1} \wedge \cdots \wedge e_{j_k}, \quad 1 \leqslant j_1 < \cdots < j_k \leqslant n$$

form a basis of $\mathcal{G}_n^k$. Thus any k-vector is a linear combination of the form $\sum_{|J|=k} \lambda_J e_J$, $\lambda_J \in \mathbb{R}$. It follows that $\dim \mathcal{G}_n^k = \binom{n}{k}$ and $\dim \mathcal{G}_n = 2^n$. If the basis $\boldsymbol{e}$ is orthogonal, then $e_J = e_{j_1} \cdots e_{j_k}$.

In particular we have $\dim \mathcal{G}_n^n = 1$ and $e_{1..n} = e_1 \wedge \cdots \wedge e_n$ is a basis. If $\boldsymbol{e}$ is orthonormal, then $e_{1..n}^2 = (-1)^{k/\!\!/2} e_{1..n} \tilde{e}_{1..n} = (-1)^{k/\!\!/2}$. This implies that if $\boldsymbol{e}'$ is another orthonormal basis, then $e'_{1..n} = \pm e_{1..n}$, where the sign indicates whether the two basis have the same $(+)$ or opposite $(-)$ orientations. If E_n is oriented, then its pseudoscalar is $e_{1..n}$, where $e_1, \ldots, e_n$ is any orthonormal positive basis.

Let E_2 be the oriented euclidean plane, and $\boldsymbol{i}$ its pseudoscalar (a positively oriented unit area). As $\boldsymbol{i}^2 = (-1)^{2/\!/2} = -1$, $\mathcal{G}_2^+ = \mathbb{R} \oplus \mathbb{R}\boldsymbol{i}$ is isomophic to the complex field, and we set $\mathbf{C} = \mathcal{G}_2^+$ (geometric complex numbers). The reverse involution $\tilde{x}$ coincides with the Clifford involution $\bar{x}$, and they define the conjugation automorphism of $\mathbf{C}$: If $x = a + b\boldsymbol{i}$, then $\tilde{x} = \bar{x} = a - b\boldsymbol{i}$. The rotation of E_2 of amplitude α, R_α, is given by $R_\alpha(v) = ve^{\boldsymbol{i}\alpha} = e^{-\boldsymbol{i}\alpha}v$. These relations are a direct consequence of the fact that if e_1, e_2 is a positive orthonormal basis, then $e_1\boldsymbol{i} = e_2$ and $e_2\boldsymbol{i} = -e_1$, while $\boldsymbol{i}e_1 = -e_2$ and $\boldsymbol{i}e_2 = e_1$ ($\boldsymbol{i}$ anticommutes with vectors).

Let E_3 be the oriented euclidean space, and $\mathbf{i}$ its pseudoscalar (a positively oriented unit volume). We have $\mathbf{i}^2 = (-1)^{3/\!/2} = -1$, and in this case $\mathbf{i}$ commutes with vectors. The algebra of *geometric quaternions* is $\mathcal{H} = \mathcal{G}_3^+$. Its elements have form $\mathfrak{q} = a + v\mathbf{i}$ ($a \in \mathbb{R}$ and $v \in E_3$). From $\mathfrak{q}\bar{\mathfrak{q}} = (\alpha + v\mathbf{i})(\alpha - v\mathbf{i}) = \alpha^2 + v^2$ we see that $\mathcal{H}$ is a (skew) field: the inverse of $\mathfrak{q} \neq 0$ is $\bar{\mathfrak{q}}/(\mathfrak{q}\bar{\mathfrak{q}}) = \bar{\mathfrak{q}}/|\mathfrak{q}|^2$.

For a unit quaternion $\mathfrak{q} \neq \pm 1$ there exists $\alpha \in (0, \pi)$ and a unit vector $u \in S^2(E_3)$ such that $\mathfrak{q} = \cos\alpha + \mathbf{i}u\sin\alpha$, and α and u are uniquely deteremined by $\mathfrak{q}$. Indeed, the condition that $\mathfrak{q} = a + \mathbf{i}v$ is a unit quaternion is $a^2 + |v|^2 = 1$. Since $|v| \geqslant 0$, there is a unique $\alpha \in [0, \pi]$ such that $a = \cos\alpha$ and $|v| = \sin\alpha$. Assuming that $\mathfrak{q} \neq \pm 1$, we have $\alpha \in (0, \pi)$ and hence $v = (v/|v|)|v| = u\sin\alpha$, where $u = v/|v| \in S^2(E_3)$. Thus we can write $\mathfrak{q} = \cos\alpha + \mathbf{i}u\sin\alpha$. Since $(\mathbf{i}u)^2 = -1$, we finally have $\mathfrak{q} = e^{\mathbf{i}u\alpha}$, the *polar form* of $\mathfrak{q}$. The polar form of general quaternions $\mathfrak{q}$ that are not real is $\mathfrak{q} = re^{\mathbf{i}u\alpha}$, where $r \in \mathbb{R}^+$, $\alpha \in (0, \pi)$, and $u \in S^3(E_3)$.

The field $\mathcal{H}$ is isomorphic to the field $\mathbb{H}$ of Hamilton's algebraic quaternions in many ways. For instance, if u_x, u_y, u_z is a positive basis of the oriented euclidean space E_3, then $\mathbf{i} = u_x u_y u_z$ is its pseudoscalar and the unit areas $\mathrm{i} = u_z\mathbf{i} = u_x u_y$, $\mathrm{j} = u_y u_z$, $\mathrm{k} = u_x u_z$ satisfy Hamilton's relations: $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1$.

Notes

The fact that $|x\rangle$ and $[x]$ obey the same proportionality rule is not a coincidence, for although Dirac never mentioned projective geometry explicitly in his research papers and books, later in his life he acknowledged having used it in his reasonings all along. This is a fascinating story, a bit mysterious, for which we can only refer to the literature, for instance the biography [6] and the references there, particularly [7].

A general projective geometric approach to quantum systems is possible and provides deep insights for quantum theory and its surprisingly close relation to classical mechanics, [8]. P

“The classical theory predicts that the atomic magnets assume all possible directions with respect to the direction of the magnetic field. On the other hand, the quantum theory predicts that we shall find only two directions parallel and antiparallel to the field (new theory, the old one gave also the direction perpendicular to the field)” (from Stern’s Nobel lecture).

P

The number of Segre 2×2 determinants is $2^{2n-3} - 2^{n-2}$. The minimum number of sufficient conditions turns out to be $2^n - n - 1$ and for $n \geqslant 2$, $2^{2n-3} - 2^{n-2} \geqslant 2^n - n - 1$, with equality ($= 1$) only for $n = 2$. For $n = 3$, the values are 6 and 4 (so 2 redundant equations); for $n = 4$, 28 and 11, so 17 redundant equations; and for large n, the number of redundant equations is asymptotically equal to the number of equations. For $n = 10$, for example, the two numbers are 130816 and 1013, which means 129803 redundancies.

P

References I

[1] S. Xambó-Descamps, "Geometric algebra speaks quantum Esperanto," 2023.

Submitted to AACA (18 Jan 2023). Based on the lecture presented at ICACGA-2022 with the same title.

[2] D. Aerts and I. Daubechies, "Physical justification for using the tensor product to describe two quantum systems as one joint system," *Helvetica Physica Acta*, vol. 51, no. 5-6, 1978.

[3] J. Rué and S. Xambó, "Introducció matemàtica a la computació quàntica," *Butlleí de la SCM*, vol. 28, no. 2, pp. 183–231, 2013.

English version: *Mathematical essentials of quantum computing* `http://www-ma2.upc.edu/sxd/QC/qc.pdf`.

References II

[4] M. Gharahi, S. Mancini, and G. Ottaviani, "Fine-structure classification of multiqubit entanglement by algebraic geometry," *Physical Review Research*, vol. 2, no. 4, p. 043003, 2020.

[5] J. Tura, *Characterizing entanglement and quantum correlations constrained by symmetry*.

Springer, 2017.

[6] G. Farmelo, *The strangest man: the hidden life of Paul Dirac*.

Faber & Faber, 2009.

[7] P. Galison, "The suppressed drawing: Paul Dirac's hidden geometry," *Representations*, vol. 72, pp. 145–166, 2000.

pdf.

References III

[8] A. Ashtekar and T. Schilling, “Geometrical formulation of quantum mechanics,” in *On Einstein’s Path: Essays in Honor of Engelbert Schucking*, pp. 23–65, Springer, 1999.