Red GAS

V Reunión Anual · USAL

En memoria de José María Muñoz Porras

Dos facetas de $\mathbf{P}^1_K$ y sus ramificaciones

S. Xambó

UPC/BSC

22/01/2020

Resumen

En una primera parte se considerará la recta proyectiva compleja y sus conexiones con la topología, el electromagnetismo, la relatividad, y la computación cuántica.

La segunda parte estará enfocada a la recta proyectiva sobre una cuerpo finito y sus conexiones con la combinatoria, la teoría de códigos correctores de errores (de bloques y convolucionales) y la criptografía pos-cuántica.

Dedicada a la memoria de José María Muñoz-Porras, cuya sapiencia, ingenio y entusiasmo siempre presidieron las innumerables discusiones sobre estos y muchos otros temas en cualquier parte donde coincidimos.

Index

- $\mathbf{P}^1_{\mathbf{C}} \overset{\alpha}{\simeq} \hat{\mathbf{C}} \overset{\sigma}{\simeq} S^2$ and the Hopf fibration
- Pauli's model of the electron spin
- Quantum computing
- $\mathbf{P}^1_{\mathbb{F}_q}$, McEliece cryptography, coding theory
- Post-quantum cryptography—the resilience of mathematics
- Can classical computation certify quantum computers?
- *In memoriam*.

$\mathbf{P}^1_{\mathbf{C}} \overset{\alpha}{\simeq} \hat{\mathbf{C}} \overset{\sigma}{\simeq} S^2$ and the Hopf fibration

Pauli spinors, $\pi : S^3 \to \mathbf{P}^1_{\mathbf{C}}$, $\mathbf{P}^1_{\mathbf{C}} \overset{\alpha}{\simeq} \hat{\mathbf{C}}$

The spinor involution $\perp$

Stereographic projection

The Hopf fibration

- In $\mathbf{P}^1_K$ (K a field, possibly non-commutative), $[\xi_0, \xi_1] = [1, \xi_0^{-1}\xi_1]$ if $\xi_0 \neq 0$, $= [0, 1]$ otherwise. In sum,

$$\mathbf{P}^1_K = \{[1, \xi]\}_{\xi \in K} \sqcup \{[0, 1]\} \overset{\alpha}{\simeq} K \sqcup \{\infty\} = \hat{K}.$$

In particular, $\mathbf{P}^1_{\mathbf{C}} \overset{\alpha}{\simeq} \hat{\mathbf{C}}$.

- In $\mathbf{C}^2$ we have the Hermitian metric

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

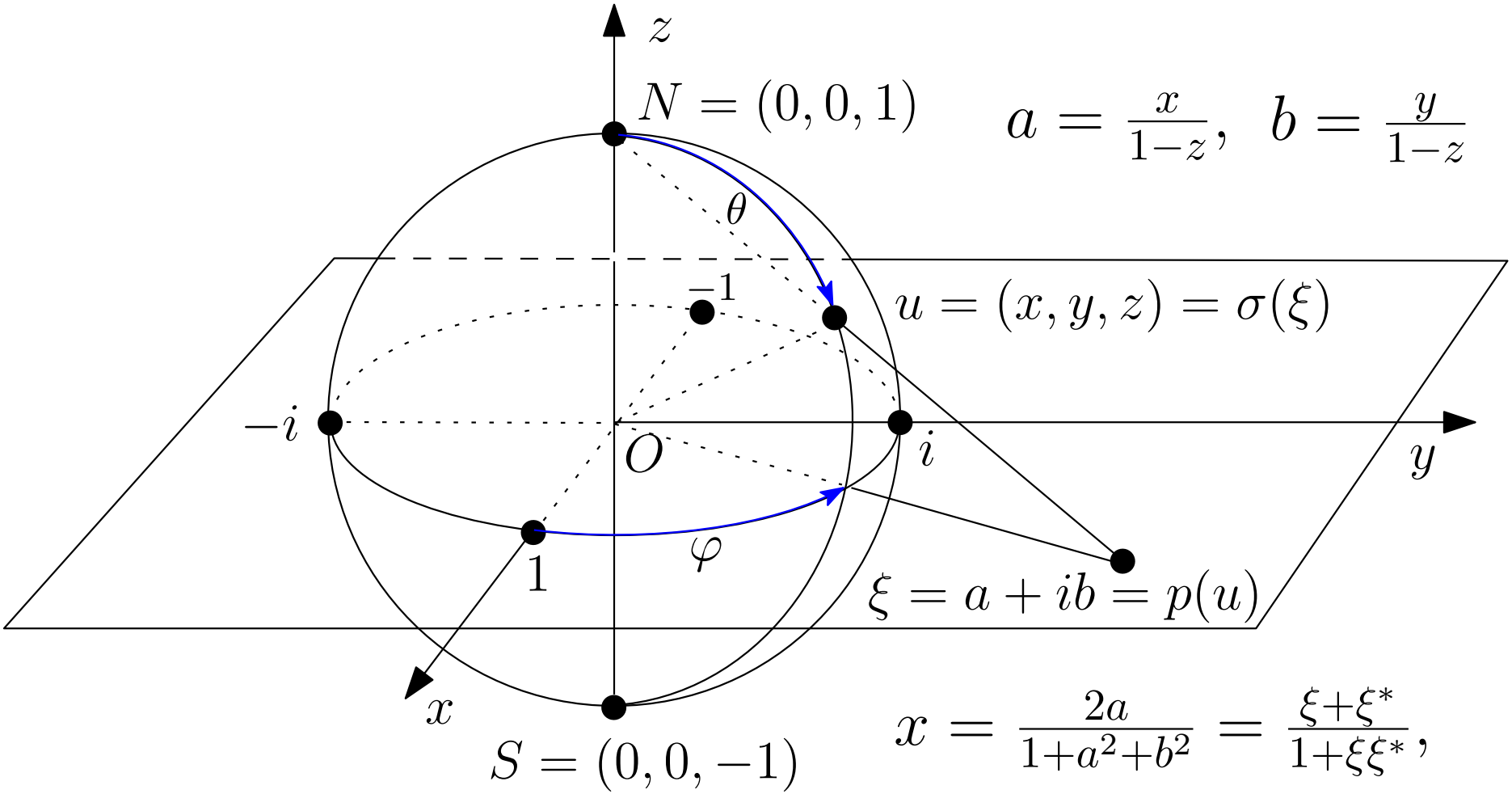
- If $\psi = (\psi_0, \psi_1) \in \mathbf{C}^2$, $|\psi|^2 = \langle \psi | \psi \rangle = |\psi_0|^2 + |\psi_1|^2$ defines the *Hermitian norm* $|\psi|$ of ψ.
- $\{\psi \in \mathbf{C}^2 : |\psi| = 1\} = S^3 \subset \mathbf{C}^2 \simeq \mathbf{R}^4$ (*Pauli spinors*).
- The map $\pi : S^3 \to \mathbf{P}^1_{\mathbf{C}}$, $\psi \mapsto [\psi]$, is surjective and the fibers are isomorphic to $S^1 = \{e^{2\pi i t} : 0 \leqslant t < 1\}$. In fact, $[\psi'] = [\psi]$ if and only if $\psi' = e^{2\pi i t}\psi$ for some (unique) t.

- Given $\psi = (\psi_0, \psi_1) \in \mathbf{C}^2$, define $\psi^\perp = (\bar{\psi}_1, -\bar{\psi}_0)$, so that $\langle \psi^\perp | \psi \rangle = 0$. The map $\psi \mapsto \psi^\perp$ is an *antilinear involution* that satisfies $|\psi| = |\psi^\perp|$. Thus $\psi, \psi^\perp$ form an *orthogonal basis* of $\mathbf{C}^2$ *if* ψ *is non-zero*, hence and *orthonormal basis* if ψ is *unitary*.
- The involution $\perp$ descends to an involution in $\mathbf{P}^1_{\mathbf{C}}$ that we will denote with the same symbol:

$$[\psi_0, \psi_1]^\perp = [\bar{\psi}_1, -\bar{\psi}_0] = [-\bar{\psi}_1, \bar{\psi}_0].$$

- $\perp$ maps the fiber of $S^3 \to \mathbf{P}^1_{\mathbf{C}}$ over $[\psi]$ to the fiber over $[\psi]^\perp$.

For example, the fiber over ∞ is $\{(0, e^{2\pi i t}) : 0 \leqslant t < 1\}$, the fiber over $[1, 0] = \infty^\perp$ is $\{(e^{2\pi i t}, 0) : 0 \leqslant t < 1\}$, and $(0, e^{2\pi i t})^\perp = (e^{2\pi i t}, 0)$.



$$a = \frac{x}{1-z}, \quad b = \frac{y}{1-z}$$

$$x = \frac{2a}{1+a^2+b^2} = \frac{\xi+\xi^*}{1+\xi\xi^*},$$

$$y = \frac{2b}{1+a^2+b^2} = -i\frac{\xi-\xi^*}{1+\xi\xi^*},$$

$$z = \frac{1-a^2-b^2}{1+a^2+b^2} = \frac{\xi\xi^*-1}{\xi\xi^*+1}$$

$$u = u_{\varphi,\theta} =$$

$$(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$$

- The *Hopf fibration* is the map $h : S^3 \to S^2$ defined by the composition

$$S^3 \xrightarrow{\pi} \mathbf{P}^1_{\mathbf{C}} \xrightarrow{\alpha} \hat{\mathbf{C}} \xrightarrow{\sigma} S^2,$$

where $u = \sigma(\xi)$ is the inverse of the stereographic projection $S^2 \xrightarrow{p} \hat{\mathbf{C}}$, $\xi = p(u)$ (see page 7).

- $h(\psi) = \left(\psi_1\bar{\psi}_0 + \bar{\psi}_1\psi_0, -i(\psi_1\bar{\psi}_0 - \bar{\psi}_1\psi_0), \psi_1\bar{\psi}_1 - \psi_0\bar{\psi}_0\right)$.
- Let $\psi_{\varphi,\theta} = (e^{-i\varphi/2}\sin\frac{\theta}{2}, e^{i\varphi/2}\cos\frac{\theta}{2})$ $(0 \leqslant \phi < 2\pi,\ 0 \leqslant \theta \leqslant \pi)$. Then

$$h(\psi_{\varphi,\theta}) = u_{\varphi,\theta},$$

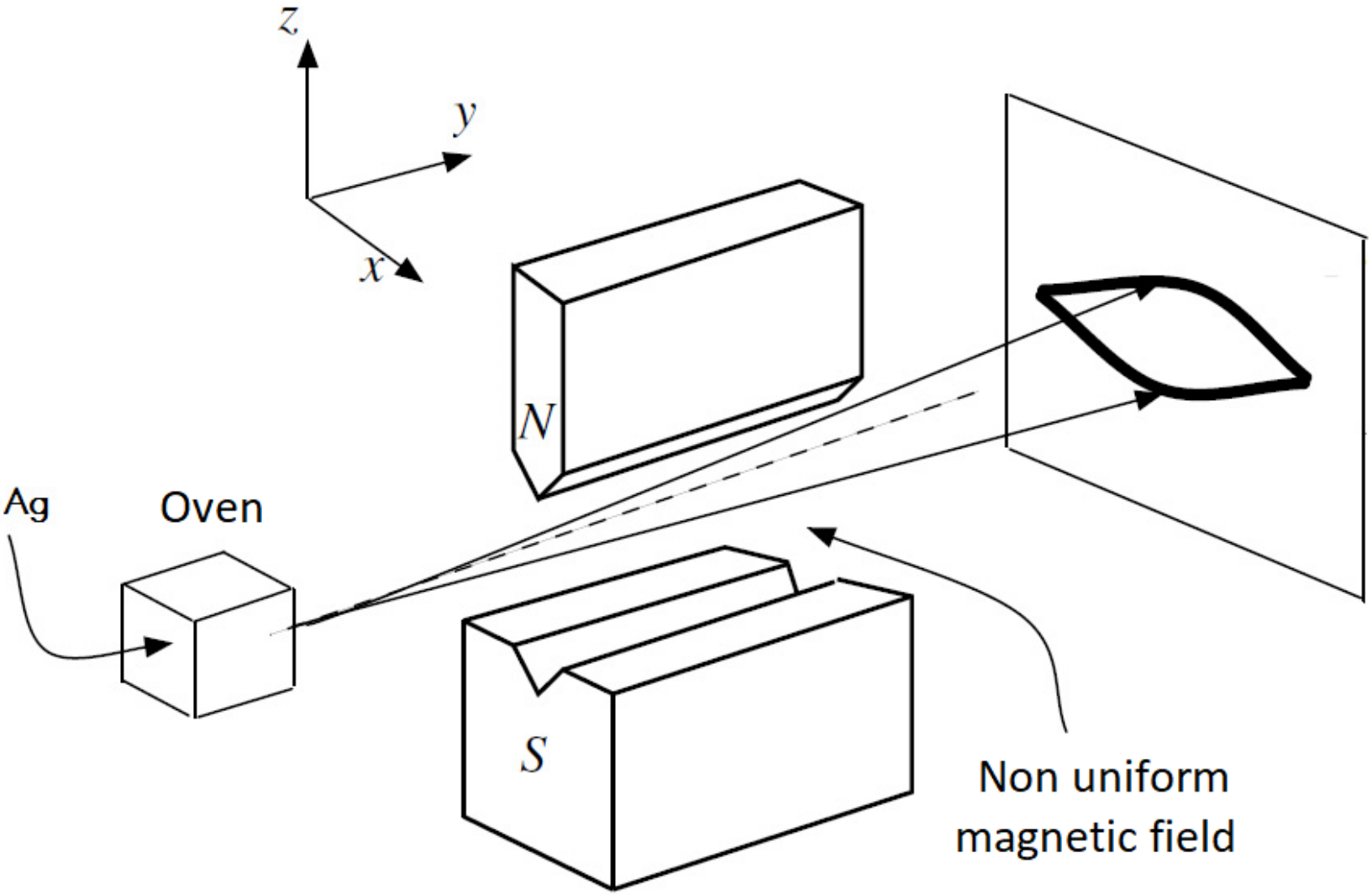
where $u_{\varphi,\theta} \in S^2$ is the point whose spherical coordinates are φ, θ (in the sense explained on page 7).

- $h(\psi^{\perp}) = -h(\psi)$. Thus the involution $\perp$ on S^3 induces the *antipodal involution* of S^2.

(cf.[1], *Spinoranalyse*).

Pauli's model of the electron spin

The quantum nature of spin: Stern Gerlach (SG) experiments. q-bits (or qubits). The Bloch sphere. q-measurements.



Stern-Gerlach experiment, which uncovered the quantum nature of the electron *spin*. It suggests that the space of spin states is S^2.

- To move from classical to quantum computation, replace $B = \{0, 1\}$, the set of classical bits, by all their 'superpositions' (linear combinations with complex coefficients), i.e. by the complex space $E = E^{(1)}$ generated by B.

Remark. Superpositions of waves occur in classical physics, particularly in many wave phenomena, and in the related notion of *polarization states of electromagnetic waves*. Its general validity in the context of quantum physics is one of the main tenets of this theory, which is strongly backed experimentally.

Thus the elements of E have the form $\psi = \psi_0 e_0 + \psi_1 e_1$, where e_0 and e_1 is the basis corresponding to 0 and 1 and $\psi_0, \psi_1 \in \mathbf{C}$. In the formalism of the preceeding section, we may take $e_0 = (1, 0)$ and $e_1 = (0, 1)$.

The Pauli spinors ψ form the sphere $S^3 \subset E^{(1)} \simeq \mathbf{R}^4$.

A Pauli spinor $\psi \in S^3 \subset E^{(1)} \simeq \mathbf{R}^4$ defines the *state* $|\psi\rangle = h(\psi) \in S^2$ (*Dirac notation*).

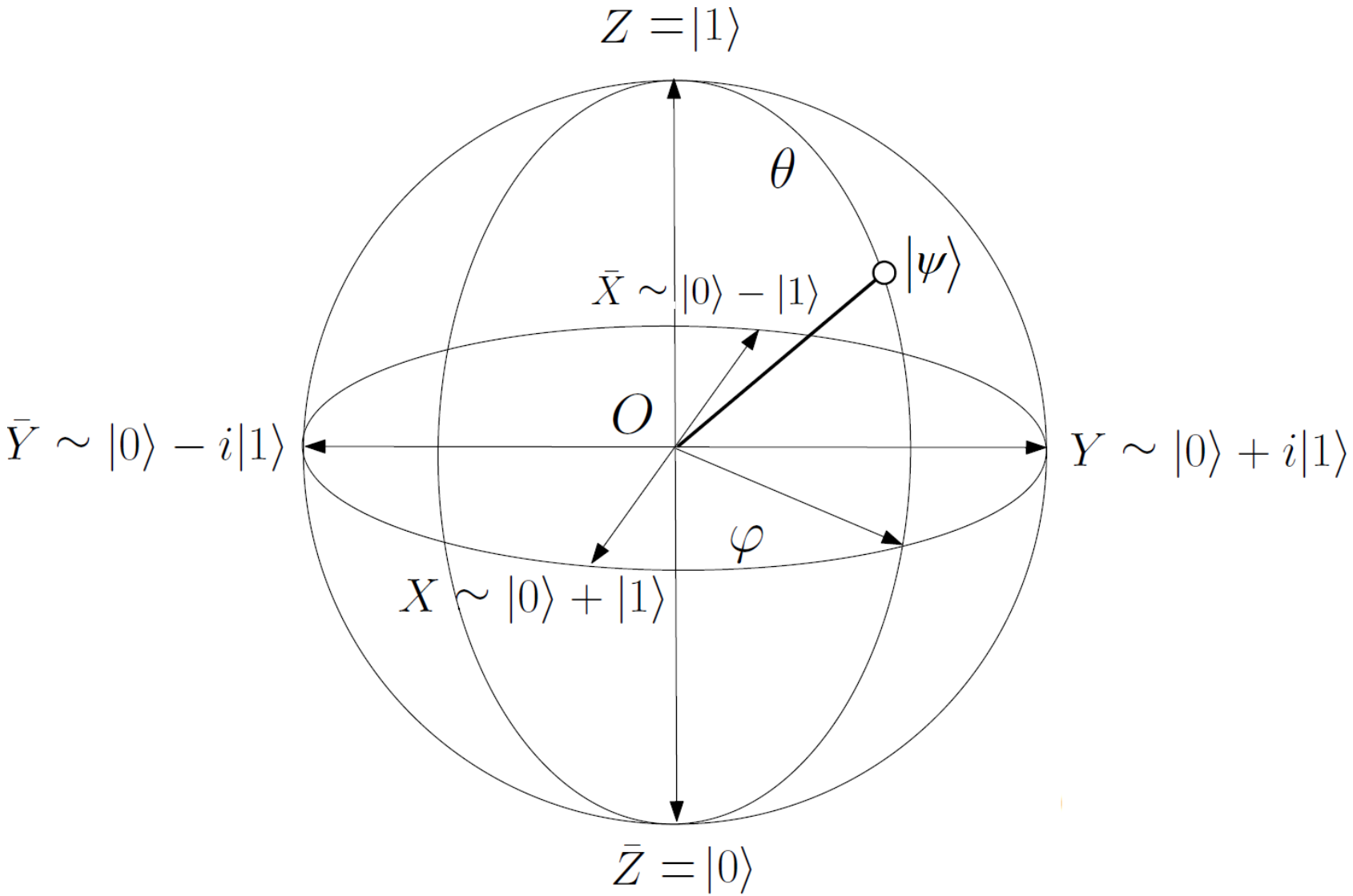
In the common parlance of quantum mechanics, the space of (pure) *spin states* is S^2 (as suggested by the SG experiments) and the Pauli spinors are the *state vectors*. The state vector of a state is defined up to a *phasor* factor ($e^{2\pi i t}$).

- As seen before, if $\psi_{\varphi,\theta} = e^{-i\varphi/2} \sin\frac{\theta}{2}\, e_0 + e^{i\varphi/2} \cos\frac{\theta}{2}\, e_1$,

$$|\psi_{\phi,\theta}\rangle = u_{\varphi,\theta}$$

the state at longitude ϕ and colatitude θ. In particular,

$$\pm X = (\pm 1, 0, 0) = |\tfrac{\sqrt{2}}{2}(e_0 \pm e_1)\rangle,$$
$$\pm Y = (0, \pm 1, 0) = |\tfrac{\sqrt{2}}{2}(e_0 \pm i e_1)\rangle,$$
$$-Z = |e_0\rangle = |0\rangle = (0, 0, -1) = S \text{ (South pole)},$$
$$+Z = |e_1\rangle = |\infty\rangle = (0, 0, 1) = N \text{ (North pole)}.$$



$$\psi = e^{-i\varphi/2} \sin\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi/2}\cos\left(\frac{\theta}{2}\right)|1\rangle$$

- The q-*measurement* of a q-bit that is in the state $u = u_{\phi,\theta}$, which corresponds to the *reading* of a classical bit, produces the state $|e_1\rangle = N = \uparrow$ or the state $|e_0\rangle = S = \downarrow$, and this result is a random event with *probabilities* $p_u(\downarrow) = \sin^2 \frac{\theta}{2}$ and $p_u(\uparrow) = \cos^2 \frac{\theta}{2}$.

These states $\uparrow$ and $\downarrow$ are classical, in that $p_\uparrow(\uparrow) = p_\downarrow(\downarrow) = 1$ (in agreement with the Stern-Gerlach findings), and they are the only states having this property.

For states u on the equator ($\theta = \pi/2$), $\uparrow$ and $\downarrow$ are equiprobable, and they are the only ones having this property.

Quantum computing

q-registers. q-computations. q-gates. q-algorithms. Shor's factoring q-algorithm. Grover's searching q-algorithm. The power of q-computing.

- More generally, the model of a *q-register of length n*, Q_n, is based on replacing B^n (the space of n-bit strings) by $E^{(n)} = \langle B^n \rangle_{\mathbf{C}}$, the complex vector space with basis B^n, represented as the tensor product (*q-entanglement* of the q-bits in the q-register) of $E^{(1)}$ with itself n times.

  So the vectors of $E^{(n)}$ have the form $\psi = \sum_{b \in B^n} \psi_b e_b$, where $e_b = e_{b_1} \otimes \cdots \otimes e_{b_n} \equiv e_{b_1} \cdots e_{b_n}$. A vector ψ is *normalized* if $|\psi|^2 = \sum_{b \in B^n} |\psi_b|^2 = 1$.
- Each normalized vector ψ defines a state $|\psi\rangle$ in the *state space* Σ_n of a Q_n, with the rule that $|\psi\rangle = |\psi'\rangle$ if and only if $\psi' = \xi\psi$ for some unit complex number ξ. Again, we denote this relation by $\psi \sim \psi'$.

  As we have seen, $\Sigma_1 = S^2$.
- The *measuring* of Q_n in the state $S = |\psi\rangle$ returns one of the basis states $|e_b\rangle \equiv |b\rangle$ at random with probabilities $|\psi_b|^2$.

- The notion of a classical (reversible) computation on n bits is replaced by a unitary matrix U of order 2^n, which can be viewed as a unitary transformation $U : E^{(n)} \to E^{(n)}$.
- To any classical computation $f : B^n \to B^n$ we can associate the q-computation $U_f : E^{(n)} \to E^{(n)}$ defined by $e_b \mapsto e_{f(b)}$. It is a permutation matrix.
- In particular we can regard the logical gates CNOT and TOFFOLI as *quantum gates*. Thus, for instance, CNOT(1,4) leaves e_b fixed if $b_1 = 0$ and changes it to $e_{b'}$ if $b_1 = 1$, where $b'_4 = 1 + b_4$ and otherwise $b'_i = b_i$. Similarly, TOFFOLI(1,3,7) does nothing on e_b if $b_1 b_3 \neq 1$, and otherwise just negates b_7.

- For a q-bit, the *Hadamard gate*, H, is defined by $e_0 \mapsto \frac{\sqrt{2}}{2}(e_0 + e_1)$, $e_1 \mapsto \frac{\sqrt{2}}{2}(e_0 - e_1)$:

$$H = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

This is a genuine q-gate, as the states $\pm X$ defined by $H(e_0)$ and $H(e_1)$ are not classical.
In the case of Q_n, H can be applied to any q-bit, or to all, in which case we will denote it by $H^{(n)}$. For example:

$$H^{(2)}e_{00} = \tfrac{1}{2}(e_0 + e_1)(e_0 + e_1) = \tfrac{1}{2}(e_{00} + e_{01} + e_{10} + e_{11}).$$

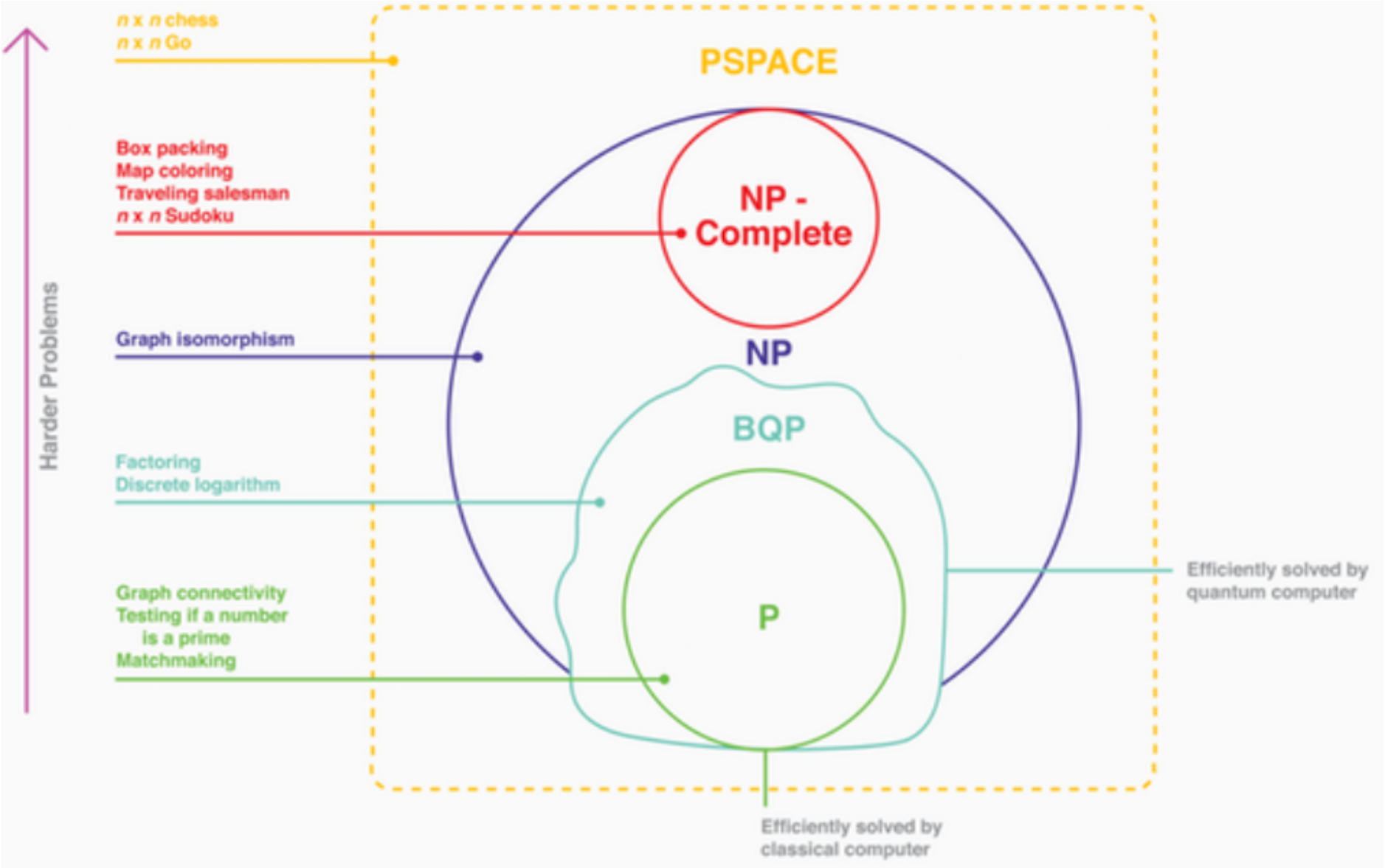
Thus, on measuring, the four possible results 00, 01, 10, 11 are equiproblable.
In general, $H^{(n)}e_{0\ldots0} = \left(\frac{\sqrt{2}}{2}\right)^n \sum_{b\in B^n} e_b$, a superpostion for which all states $|b\rangle$ are equiprobable. This embodies the so-called *quantum parallelism*.

- A *q-algorithm* is a sequence of Hadamard and Toffoli gates, followed by a measurement of the final state, which is the (classical) bit string returned by the algorithm.

Example. Initialize Q_3 in the state $|000\rangle$. Apply $H^{(3)}$. End by a measuring operation. This q-algorithm yields a uniform random string of three bits. The generalization to Q_n is obvious.

- *Shor's q-algorithm factors integers in polynomial time*.
- *Grover's q-algorithm searches an item in a list of size N in time* $\sqrt{N}$.

For a systematic introduction to q-computing, including a discussion of these and other algorithms, see [2], and also the references therein.



An excellent discussion about the complexity theory issues is provided by Scott Aaronson' book [3] (*Quantum computing since Democritus*).

$\mathbf{P}^1_{\mathbb{F}_q}$, McElice cryptography, coding theory

Ingredients of a McECS. Encryption. Decryption. Construction of McECS. Security analysis.

- $F = F_q$, a finite field of cardinal q (*base field*). The most important case will be $F = \mathbf{Z}_2$.
- k a positive integer. The vectors of F^k are called *information vectors*, or *messages*.
- $n > k$ an integer. The vectors of F^n are called *transmission vectors*.

Notations

If $\mathbf{x} \in F^n$, we let $|\mathbf{x}|$ denote the number of non-zero components of $\mathbf{x}$ and we say that it is the *weight* of $\mathbf{x}$.

$F(r, s)$ denotes the space of matrices of type $r \times s$ with entries in F and $F(r) = F(r, r)$.

A receiving user needs the following data:

- $G \in F(k, n)$ such that $\text{rank}(G) = k$;
- $S \in F(k)$ invertible and chosen uniformly at random;
- $P \in F(n)$ a random permutation matrix;
- t, a positive integer; and
- $g : X \to F^k$, $X \subseteq F^n$, such that for any $\boldsymbol{u} \in F^k$ and all $\boldsymbol{e} \in F^n$ with $|\boldsymbol{e}| \leqslant t$,

$$\mathbf{x} = \boldsymbol{u}G + \boldsymbol{e} \in X \quad \text{and} \quad g(\mathbf{x}) = \boldsymbol{u}. \tag{1}$$

The map g is called an *t-error-correcting G-decoder*, or simply *decoder*, and the vectors of X are said to be *g-decodable*.

- **Private key**: $\{G, S, P\}$.
- **Public key**: $\{G', t\}$, where $G' = SGP$.

Encryption protocol

The protocol that a user has to follow to encript and send a message $\boldsymbol{u}$ to the user whose public key is $\{G', t\}$ consists of two steps:

- Random generation of a transmission vector $\boldsymbol{e}$ of weight t;
- Sending the vector $\mathbf{x} = \boldsymbol{u}G' + \boldsymbol{e} = \boldsymbol{u}SGP + \boldsymbol{e}$ to that user.

Decryption protocol

Consists of four steps that only use private data of the receiver and the vector $\mathbf{x}$ sent by the emitter:

- Set $\mathbf{y} = \mathbf{x}P^{-1}$, so that $\mathbf{y} = (\boldsymbol{u}S)G + \boldsymbol{e}P^{-1}$.
- Set $\mathbf{x}' = g(\mathbf{y})$. Since P is a permutation matrix, $|\boldsymbol{e}P^{-1}| = |\boldsymbol{e}| = t$, and hence $\mathbf{x}'$ is well defined, as g corrects t errors. The result is $\mathbf{x}' = (\boldsymbol{u}S)G$, which says that $\mathbf{x}'$ is the linear combination of the rows of G with coefficients $\boldsymbol{u}' = \boldsymbol{u}S$.
- Since G has rank k, $\boldsymbol{u}'$ is uniquely determined by $\mathbf{x}'$ and can be obtained by solving the system of linear equations $\mathbf{x}' = \boldsymbol{u}'G$, where $\boldsymbol{u}'$ is the unknown vector.
- Let $\boldsymbol{u} = \boldsymbol{u}'S^{-1}$, which agrees with the message sent by the emitter.

- $F = F_2$ (most constructions also for F_q, $q > 2$).
- $\bar{F} = F_{q^m}$, m a positive integer. If $\beta \in \bar{F}$, $[\beta]$ will denote the colum vector of its components with respect to a basis of $\bar{F}/F$.
- $\boldsymbol{\alpha} = \alpha_1, \ldots, \alpha_n \in \bar{F}$ distinct elements, so that $n \leqslant q^m$.
- $p \in \bar{F}[X]$ a polynomial of degree $r > 0$ such that $p(\alpha_j) \neq 0$ $(j = 1, \ldots, n)$.
- Set $h_j = 1/p(\alpha_j)$ $(j = 1, \ldots, n)$ and

$$\bar{H} = \begin{pmatrix} h_1 & \cdots & h_n \\ h_1\alpha_1 & \cdots & h_n\alpha_n \\ \vdots & & \vdots \\ h_1\alpha_1^{r-1} & \cdots & h_n\alpha_n^{r-1} \end{pmatrix} \in \bar{F}(r, n).$$

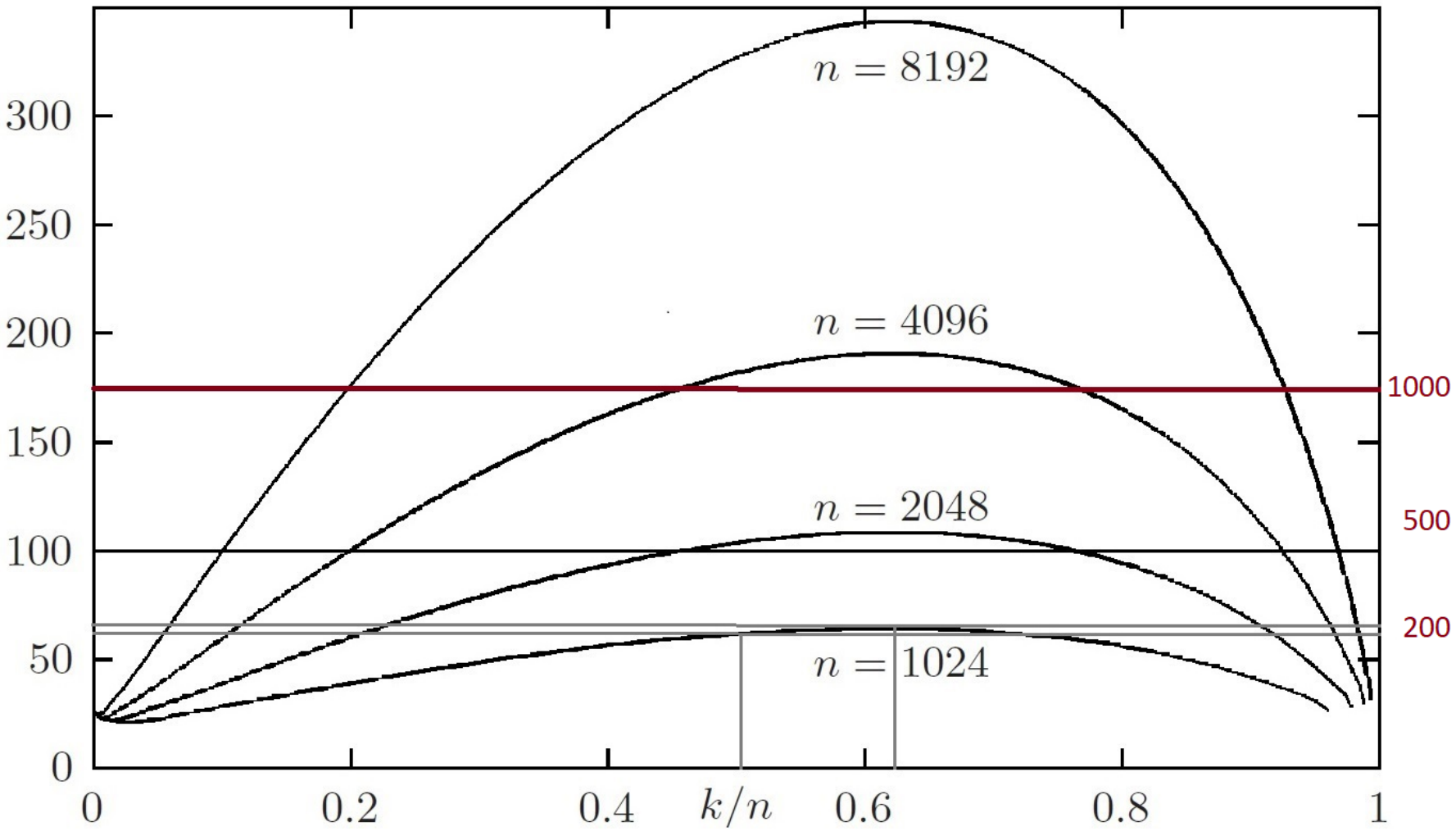
- Let $H \in F(r', n)$ be the result of replacing each entry β of $\bar{H}$ by $[\beta]$ (this yields a matrix $[H] \in F(mr, n)$), followed by deleting from $[H]$ any row that is in the span of the previous ones. Note that $r' \leqslant mr$. It also holds that $r \leqslant r'$, as the $\langle H \rangle_{\bar{F}} = \langle \bar{H} \rangle_{\bar{F}}$.
- Let $\Gamma = \Gamma(p, \alpha) = \{\mathbf{x} \in F^n : \mathbf{x}H^T = 0\}$. It is a **code** of type $[n, k = n - r']$. This code is called the *classical Goppa code* associated to p and $\boldsymbol{\alpha}$.
- We have $n - mr \leqslant k \leqslant n - r$.
- **Fact**: If $G \in F(k, n)$ is a generating matrix of Γ, *there is G-decoder that corrects r errors* ($r/2$ for $q > 2$) *provided p has no multiple roots in $\bar{F}$*. See, for example, [4, P.4.7]

Practical specification

- Let α be the set of elements of $\bar{F}$. Hence $n = 2^m$.
- Let $p \in \bar{F}[X]$ be a monic irreducible of degree $t > 1$. Then p has no roots in $\bar{F}$ and so a generating matrix G of $\Gamma(p, \alpha)$ *has a decoder g that corrects t errors*.

This ends the theoretical construction of a McECS with the following parameters:

- $n = 2^m$, where m is any posivive integer, and p is monic irreducible of degree t.
- $\bar{H} \in \bar{F}(t, n)$ and $G \in F(k, n)$, where $k = n - \text{rank}(H)$ $(n - tm \leqslant k \leqslant n - t)$.
- Original example: $m = 10$, $n = 1024$, $t = 50$, $k = 524$ (in this case $k = n - tm$, the minimum possible given m and t).



Horizontal axis $R = k/n$, WF curves for $n = 2^j$, $j = 10, \ldots, 13$. The red line represents the WF needed to break RSA with 1000-digit prime numbers. The similar 500-digit and 200-digit levels are also shown. The latter is comparable to the original McECS.

Post-quantum cryptography

Quantum threats to cryptographic protocols. McECS as a post-quantum system. Other post-quantum protocols. The NIST initiative for PQ protocols.

- q-computing poses a fundamental threat to widespread cryptographic systems like RSA.
- In principle, it does not pose a threat to McECS (unless P = NP), because the general problem of decoding linear codes is NP complete [8] (Berlekamp, McEliece and van Tilborg, 1978: *On the inherent intractability of certain coding problems*).

However, for the special codes used in McECS it could still exist an astute way of using their structure to crack them. But all the evidence collected in their study so far (see page 29) suggests it is a *post-quantum* protocol, in the sense that no computational power can crack it if the appropriate parameters are used.

In addition to the McEliece cryptosystem, there are other systems that may qualify as post-quantum cryptography:

- Hash-based cryptography;
- Code-based cryptography;
- Lattice-based cryptography;
- Multivariate-quadratic-equations cryptography.

See [9], particularly the introductory paper by D. J. Bernstein.

These, and variations on them, are being considered by NIST with the goal set at defining and standardize one or more post-quantum cryptography protocols. See `http://dx.doi.org/10.6028/NIST.IR.8105`.

In the first round, 26 algorithms were selected out of 69 submitted. The selection outcome of the second round should be known soon.

Can classical computation certify quantum computers?

The work of Urmila Mahadev

"Urmila Mahadev spent eight years in graduate school solving one of the most basic questions in quantum computation: How do you know whether a quantum computer has done anything quantum at all?" (article by Erika Klarreich, 8 October 2018, in Quantamagazine).

`https://www.quantamagazine.org/graduate-student-solves-quantum-verification-problem-20181008/`

See [10] (U. Mahadev, *Classical Verification of Quantum Computations*).

Another important paper of Urmila Mahadev: [11].

Abstract. We present the first protocol allowing a classical computer to interactively verify the result of an efficient quantum computation. We achieve this by constructing a *measurement protocol*, which enables a classical verifier to use a quantum prover as a trusted measurement device.
The protocol forces the prover to behave as follows: (1) the prover must construct an n qubit state of his choice, (2) measure each qubit in the *Hadamard* or standard basis **as directed by the verifier**, and (3) report the measurement results to the verifier.
The soundness of this protocol is enforced *based on the assumption that the learning with errors problem* [one of the post-quantum protocols] is computationally intractable for efficient quantum machines.

In memoriam

Codes 2001-2014. ArbolMat

MR1815719 (2002b:14041) 14H81 14H70 14L05 81T30

Muñoz Porras, J. M. (E-SALA); Plaza Martín, F. J. (E-SALA)

Automorphism group of $k((t))$: applications to the bosonic string.

Comm. Math. Phys. **216** (2001), *no.* 3, 609–634.

MR2142430 (2006e:94074) 94B15 14G50 94B27

Domínguez Pérez, J. A. (E-SALA); Muñoz Porras, J. M. (E-SALA); Serrano Sotelo, G. (E-SALA)

Convolutional codes of Goppa type.

Appl. Algebra Engrg. Comm. Comput. **15** (2004), *no.* 1, 51–61.

MR2238161 (2007c:94281) 94B27 14G50 94B10

Muñoz Porras, J. M. (E-SALA); Domínguez Pérez, J. A. (E-SALA); Iglesias Curto, J. I. (E-SALA); Serrano Sotelo, G. (E-SALA)

Convolutional Goppa codes.

IEEE Trans. Inform. Theory **52** (2006), *no.* 1, 340–344.

MR2401063 (2009c:94073) 94B10 14G50

Domínguez Pérez, J. A. (E-SALA); Iglesias Curto, J. I. (E-SALA); Muñoz Porras, J. M. (E-SALA); Serrano Sotelo, G. (E-SALA)

Algebro-geometric construction of convolutional codes. (Spanish)

Bol. Soc. Esp. Mat. Apl. SeMA No. 42 (2008), 163–169.

MR2509130 (2010j:94077) 94B27 14G50 94B10

Domínguez Pérez, J. A. (E-SALA); Muñoz Porras, J. M. (E-SALA); Serrano Sotelo, G. (E-SALA)

Algebraic geometry constructions of convolutional codes.

Advances in algebraic geometry codes, 391–417, *Ser. Coding Theory Cryptol.*, 5, *World Sci. Publ., Hackensack, NJ*, 2008.

MR2608186 (2011d:94073) 94B10 14G50 94B27

Muñoz Porras, José María (E-SALA); Iglesias Curto, José Ignacio (E-SALA)

Classification of convolutional codes.

Linear Algebra Appl. **432** (2010), *no.* 10, 2701–2725.

CÓDIGOS CONVOLUCIONALES Y GEOMETRÍA ALGEBRAICA

J.M. MUÑOZ PORRAS, J.A. DOMÍNGUEZ PÉREZ

Conferències FME, Volum V, Curs Riemann, 2007-2008, 199-209

MR3000507 94B10 14D06 14G50 94B25 94B27

Iglesias Curto, J. I. (E-SALA); Muñoz Porras, J. M. (E-SALA); Plaza Martín, F. J. (E-SALA); Serrano Sotelo, G. (E-SALA)

Convolutional Goppa codes defined on fibrations.

Appl. Algebra Engrg. Comm. Comput. **23** (2012), *no.* 3-4, 165–178.

MR3106850 94B10

Curto, José Ignacio Iglesias (E-SALA-IPM); Castañeda, Ángel Luis Muñoz (D-FUB-MI); Porras, José María Muñoz (E-SALA-IPM); Sotelo, Gloria Serrano (E-SALA-IPM)

Every convolutional code is a Goppa code.

IEEE Trans. Inform. Theory **59** (2013), *no.* 10, 6628–6641.

Métodos de Geometría Algebraica en Teoría de Códigos Convolucionales

Gloria Serrano Sotelo

Memoria presentada para optar al Grado de Doctora en Matemáticas bajo la dirección de los

Profesores Drs. D. J. M. Muñoz Porras y D. Francisco Plaza Martín

References I

[1] B. L. van der Waerden, "Spinoranalyse," *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, vol. 1929, pp. 100–110, 1929.

English translation by Guglielmo Pasa:
`https://arxiv.org/pdf/1703.09761.pdf`.

[2] J. Rué and S. Xambó-Descamps, "Introducció matemàtica a la computació quàntica," *Butlletí de la Societat Catalana de Matemàtiques*, vol. 28, no. 2, pp. 183–231, 2013.

English version:
`https://mat-web.upc.edu/people/sebastia.xambo/QC/qc.pdf`.

[3] S. Aaronson, *Quantum computing since Democritus*.

Cambridge University Press, 2013.

References II

[4] S. Xambó-Descamps, *Block error-correcting codes: a computational primer*. Univesitext, Springer, 2003.

[5] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography* (J. D. E. J. Buchanan, ed.), vol. 5299 of *Lecture Notes Computer Science*, pp. 31–46, Springer, 2008.

Proceedings of the Second PQCrypto international workshop, Cincinnati, OH, USA, October 17-19, 2008.
`https://cr.yp.to/codes/mceliece-20080807.pdf`.

[6] "Post-Quantum Cryptography 2018."
`https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`.

First PQC Standardization Conference organized by the NIST Computer Security Resource Center.

References III

[7] N. Sayols and S. Xambó-Descamps, "Computer Algebra Tales on Goppa Codes and McEliece Cryptography," *Mathematics in Computer Science*, pp. 1–13, 2019.

[8] E. R. Berlekamp, R. J. McEliece, and H. C. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions of Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[9] D. J. Bernstein, J. Buchmann, and E. D. (eds.), *Post-Quantum Cryptography*.

Springer, 2009.

ix+345 p.

References IV

[10] U. Mahadev, "Classical verification of quantum computations," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 259–267, IEEE, 2018.

`https://arxiv.org/pdf/1804.01082.pdf`.

[11] U. Mahadev, "Classical homomorphic encryption for quantum circuits," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 332–338, IEEE, 2018.

`https://arxiv.org/pdf/1708.02130.pdf`.