GEOMETRIC ALGEBRA:

Parallel Processing for the Mind

Timothy F. Havel (Nuclear Engineering)

LECTURE 4

On spin & spinors:

The operators for the x, y & z components of the angular momentum of a spin 1/2 particle (in units of $\hbar$) are usually represented by one half the **Pauli matrices**:

$$\underline{\sigma}_1 \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \underline{\sigma}_2 \equiv \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} \qquad \underline{\sigma}_3 \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

These are easily seen to anticommute & square to the identity, and hence correspond to orthonormal vectors in a *matrix representation* for $\mathcal{G}(3)$.

The state of a spin is more commonly specified by a **spinor** (unit vector) $|\psi\rangle$ in a 2-D Hilbert space $\mathcal{H}$ over $\mathcal{C}$, in which case the expected components of the angular momentum are

$$\tfrac{1}{2}\langle\psi|\underline{\sigma}_k|\psi\rangle = \tfrac{1}{2}tr(\underline{\Psi}\underline{\sigma}_k) = \tfrac{1}{4}tr(\underline{\Psi}\underline{\sigma}_k + \underline{\sigma}_k\underline{\Psi}) = \tfrac{1}{2}tr((\Psi\bullet\sigma_k)\underline{\mathbf{1}}) = \Psi\bullet\sigma_k$$

where $\underline{\Psi} \equiv |\psi\rangle\langle\psi|$, i.e. the inner product of $\Psi, \sigma_k \in \mathcal{G}(3)$!

Since $\Psi \bullet \sigma_k$ is a scalar, Ψ itself must be the sum of a scalar & a vector, and the scalar part is $\langle \Psi \rangle_0 \equiv \frac{1}{2} tr(\underline{\Psi}) = \frac{1}{2}\langle \psi | \psi \rangle = \frac{1}{2}$. Using the fact that the angular momentum is quantized along its own axis to $1/2$, the vector part can be written as $\frac{1}{2}\boldsymbol{R}\sigma_3\tilde{\boldsymbol{R}}$, i.e. as a rotation of σ_3 by some spinor $\boldsymbol{R} \in \mathcal{G}^+(3)$. It follows that $\Psi = \boldsymbol{R}(\frac{1}{2}(1+\sigma_3))\tilde{\boldsymbol{R}}$ or, using the correspondence between $\mathcal{G}^+(3)$ and $\mathrm{SU}(2)$ matrices:

$$\underline{\Psi} = \begin{bmatrix} a & -b^* \\ b & a^* \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a^* & b^* \\ -b & a \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}\begin{bmatrix} a^* & b^* \end{bmatrix} = \begin{bmatrix} |a|^2 & ab^* \\ ba^* & |b|^2 \end{bmatrix} = |\psi\rangle\langle\psi|$$

Thus we can identify $|\psi\rangle$ with $\psi \equiv \boldsymbol{R}\boldsymbol{E}_+$, where $\boldsymbol{E}_+ \equiv \frac{1}{2}(1+\sigma_3)$ is an **idempotent** ($\boldsymbol{E}_+^2 = \boldsymbol{E}_+$). In fact, since the 2nd column of $\mathrm{SU}(2)$ matrices is determined by the first, we can just use $\boldsymbol{R}$!

Another big advantage of representing states by sums of scalars & vectors is that this representation extends directly to *statistical ensembles* $\{\Psi\}$ of spin states, as follows:

$$\overline{\Psi} = \frac{1}{M}\sum_{i=1}^{M}\Psi_i = \frac{1}{2} + \frac{1}{2M}\sum_{i=1}^{M}\boldsymbol{R}_i\sigma_3\tilde{\boldsymbol{R}}_i \underset{M\to\infty}{\longrightarrow} \frac{1}{2} + \oint \boldsymbol{R}\,\sigma_3\tilde{\boldsymbol{R}}\,dP(\boldsymbol{R})$$

We may write this (dropping the bar) as $\Psi = (1+\boldsymbol{s})/2$, where $s \equiv \|\boldsymbol{s}\| \le 1$ is the ensemble's **polarization**. The "operator" $\overline{\Psi}$, called the **density operator**, yields the *ensemble average expectation value* of any observable $\boldsymbol{A}$ via:

$$\overline{\langle\psi|\underline{\boldsymbol{A}}|\psi\rangle} = M^{-1}\sum_{i=1}^{M}\langle\psi|\underline{\boldsymbol{A}}|\psi\rangle = 2M^{-1}\sum_{i=1}^{M}\langle \boldsymbol{A}\Psi_i\rangle_0 = 2\langle \boldsymbol{A}\overline{\Psi}\rangle_0$$

Spins from Space-Time (sic)

The spin vector $\boldsymbol{s}$ is the net angular momentum (in units of $\hbar$), which for a classical spinning particle of charge e leads to a magnetic moment of $s\mu_0 \equiv se/(2m)$ $(c = 1)$, where μ_0 is the **Bohr magneton**. The spatial vector $\boldsymbol{s}$ corresponds to a *space-time bivector* $\boldsymbol{s} = \mathbf{s}\gamma_0$, where γ_0 defines its inertial frame. In a co-moving frame, this evolves according to the covariant form of Lorentz equation (**Lecture 3**) as $\dot{\boldsymbol{s}} =$

$$2\mu_0(\mathbf{F} \bullet (\boldsymbol{s}\gamma_0)) \wedge \gamma_0 = 2\mu_0((\boldsymbol{E} \bullet \boldsymbol{s} + (\imath\boldsymbol{B}) \bullet \boldsymbol{s})\gamma_0) \wedge \gamma_0 = 2\mu_0 \boldsymbol{s} \times \boldsymbol{B},$$

where we have used the facts that γ_0 anticommutes with $\boldsymbol{s}$, $\boldsymbol{E}$, $\boldsymbol{B}$ and $\imath$, while $\boldsymbol{E} \bullet \boldsymbol{s}$ is a scalar but $(\imath\boldsymbol{B}) \bullet \boldsymbol{s}$ is a spatial vector. The lack of response to the electric field is a result of choosing a co-moving frame. Thus the magnetic moment of the electron, which is very nearly $2\mu_0$, can be explained by a simple *classical* model. Like the magnetic field itself, however, spin behaves under inversion like a spatial bivector $\imath\boldsymbol{s}$.

MULTIPARTICLE ALGEBRA

More than the Sum of Its Parts?

To model a system of N particles:

- Take as usual the direct sum of their states (vectors);
- Consider the corresponding *joint* Clifford algebra, i.e. $(\mathcal{G}(1,3))^N \approx \mathcal{G}(N,3N)$;
- This algebra has dimension 2^{4N} (*exponential* in N!).

Assuming there exists a *common* frame of reference, i.e. a natural choice of time-like γ_0^m in every particle space, then:

- The even subalgebras $\mathcal{G}^+(1,3)$ of different particle spaces *commute*, since for $1 \le i, j \le 3$ and $1 \le k < l \le N$

$$\sigma_k^m \sigma_l^n \leftrightarrow (\gamma_k^m \gamma_0^m)(\gamma_l^n \gamma_0^n) = (\gamma_l^n \gamma_0^n)(\gamma_k^m \gamma_0^m) \leftrightarrow \sigma_l^n \sigma_k^m$$

  where the superscripts are particle indices.

- Thus one has an isomorphism with the **tensor product** of the corresponding 3-D Euclidean geometric algebras:

$$(\mathcal{G}^+(1,3))^N \approx (\mathcal{G}(3))^{\otimes N};$$

- This algebra has dimension 2^{3N} (still *exponential*!).

PRODUCT OPERATORS

The usual nonrelativistic theory of N spin 1/2 particles relies entirely upon the algebra of $2^N \times 2^N$ matrices over $\mathcal{C}$, which has dimension only 2^{2N+1}. The extra degrees of freedom in the algebra $(\mathcal{G}^+(1,3))^N$ are due to the fact that it contains a different imaginary unit $\imath^m$ for every particle m.

These extra degrees of freedom can be removed can be removed by multiplication by the **correlator idempotent**:

$$\boldsymbol{C} \equiv \frac{1}{2}\left(1 - \imath^1\imath^2\right)\frac{1}{2}\left(1 - \imath^1\imath^3\right) \cdots\cdots \frac{1}{2}\left(1 - \imath^1\imath^N\right)$$

This projects everything onto an "ideal" of the correct dimension, in which all these different imaginary units have been identified. In addition, since $\boldsymbol{C} = \boldsymbol{C}^2$ is easily seen to commute with everything in the algebra, multiplication by it is trivially a homomorphism onto this ideal (subalgebra).

Henceforth we shall drop the implicit factor of $\boldsymbol{C}$ from all our expressions, and use the single imaginary unit

$$\imath \equiv \imath^1\boldsymbol{C} = \ldots = \imath^N\boldsymbol{C}.$$

Note the correlated product of the even subalgebras in each particle space, $(\mathcal{G}^+(3))^{\otimes N}/\boldsymbol{C}$, is a subalgebra of dimension 2^{2N} (the same as that of the subspace of Hermitian matrices), which has *never* been recognized in the matrix algebra!

MULTIPARTICLE SPINORS

Just as in the one-particle case, multi-particle spinors (state vectors) $|\psi\rangle$ in the 2^N-D complex Hilbert space correspond to elements of a left-ideal obtained by multiplying through by an idempotent:

$$\boldsymbol{EC} \equiv \boldsymbol{E}_+^1 \ldots \boldsymbol{E}_+^N \boldsymbol{C} \qquad (\boldsymbol{E}_\pm^m \equiv \tfrac{1}{2}(1 \pm \sigma_3^m)).$$

This ideal corresponds, as before, to matrices whose columns are all zero save for their left-most, and provides a carrier space for the products of all possible 3-D rotations.

Similarly, multiparticle density operators may now be written (omitting now the $\boldsymbol{C}$) as

$$\Psi = \frac{1}{M}\sum_{i=1}^{M} \Psi_i = \frac{1}{M}\sum_{i=1}^{M} \psi_i \tilde{\psi}_i = \frac{1}{M}\sum_{i=1}^{M} \boldsymbol{R}_i \boldsymbol{E} \tilde{\boldsymbol{R}}_i,$$

where $\boldsymbol{R}_i \in (\mathcal{G}^+(3))^{\otimes N}/\boldsymbol{C}$. Note however that $\boldsymbol{R}_i$ may not be *factorizable* into one particle rotations $\boldsymbol{R}_i^1 \cdots \boldsymbol{R}_i^N$, in which case the corresponding spinor $\psi_i = \boldsymbol{R}_i \boldsymbol{E}$ cannot be expressed as a product of one-particle spinors $\psi_i^1 \cdots \psi_i^N$ and so is termed **entangled**. It may also happen that the individual terms in this sum can be factorized as $\boldsymbol{R}_i^m \boldsymbol{E}_+^m \tilde{\boldsymbol{R}}_i^m$, but the overall sum is *not* factorizable. In this case the density operator describes a correlated, but not an entangled, statistical ensemble.

The Basics of Quantum Information Processing

Binary information can be stored in an array of two-state quantum systems (e.g. spin 1/2) *relative to* a fixed **computational basis** of $\mathcal{H}(2^N)$ (or ideal in $(\mathcal{G}(3))^{\otimes N}/\boldsymbol{C}$):

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \leftrightarrow \quad |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \leftrightarrow \quad \boldsymbol{E}_+ = \frac{1}{2}(1 + \sigma_3)$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \leftrightarrow \quad |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad \leftrightarrow \quad \boldsymbol{E}_- = \frac{1}{2}(1 - \sigma_3)$$

Each such **qubit** can be placed into a **coherent superposition** over these two basis states, which for $\alpha, \beta \in \mathcal{C}$ can be written in the following equivalent ways:

$$\alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \leftrightarrow$$

$$(\alpha|0\rangle + \beta|1\rangle)(\tilde{\alpha}\langle 0| + \tilde{\beta}\langle 1|) = \begin{bmatrix} |\alpha|^2 & \alpha\tilde{\beta} \\ \tilde{\alpha}\beta & |\beta|^2 \end{bmatrix} \quad \leftrightarrow$$

$$(\alpha + \beta\sigma_1)\boldsymbol{E}_+(\tilde{\alpha} + \tilde{\beta}\sigma_1) = \frac{1}{2}\Big(1 + \Re(\tilde{\alpha}\beta)\sigma_1 + \Im(\tilde{\alpha}\beta)\sigma_2 + (|\alpha|^2 - |\beta|^2)\sigma_3\Big)$$

A superposition over all qubits individually *expands* to a superposition over all integers in $\{0, \ldots, 2^N - 1\}$, e.g.

$$|\Omega\rangle = 2^{N/2} \underbrace{(|0\rangle + |1\rangle)\ldots\ldots(|0\rangle + |1\rangle)}_{N} = 2^{N/2} \sum_{j=0}^{2^N - 1} |j\rangle ,$$

($|j\rangle \equiv |01\ldots0\rangle$ is obtained by *binary* expansion of the integer j).

By the linearity of quantum mechanics, any unitary operation $\boldsymbol{U}$ on such a superposition operates on every term of its expansion *in parallel*, i.e.

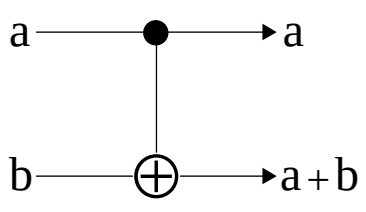
$$\underline{\boldsymbol{U}}|\Omega\rangle = 2^{N/2} \sum_{j=0}^{2^N - 1} \underline{\boldsymbol{U}}|j\rangle$$

(in $(\mathcal{G}^+(3))^{\otimes N}/\boldsymbol{C}$, $\boldsymbol{U}$ acts as $\underline{\boldsymbol{U}}|\Omega\rangle\langle\Omega|\tilde{\underline{\boldsymbol{U}}}$, which is also linear). Moreover, there exists a polynomially-bounded basis for the unitary group $\mathrm{U}(2^N)$ (i.e. one that is **unitarily universal**).

Example: All one-qubit operations, including those mapping one qubit states to superpositions, e.g. the **Hadamard gate**

$$\underline{\boldsymbol{R}}_{\mathrm{H}}|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \qquad \underline{\boldsymbol{R}}_{\mathrm{H}}|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2} ,$$

together with the c-NOT (**controlled-NOT**) logic gate which computes the XOR of its inputs (see right). Note that this operates on bit b conditional on bit a.

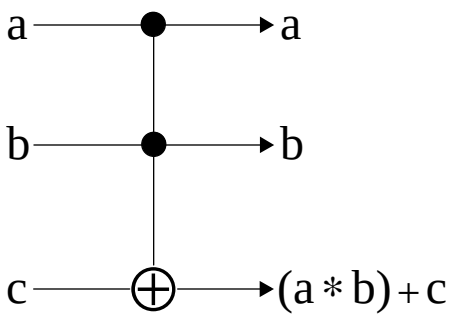


There exists a subgroup of $\mathsf{U}(2^N)$ which:

- Maps single states $|j\rangle$ to single states.
- Admits a polynomially bounded basis for the symmetric group $\mathsf{S}(2^N)$ (i.e. that is computationally **universal**).

This is nontrivial, since unitary operations are necessarily *reversible* (i.e. each output corresponds to a single input).

Example: The **Toffoli gate** has three input and three output bits. It copies the a & b bits, but takes the NOT of the c bit if the other two are both 1 (see right). Setting the c bit to 1 thus takes the NAND of the other two.



Some of the hardest and most interesting computational problems (e.g. NP-complete) are **decision problems**:

> **Given a boolean function $f : \{0,1\}^N \longrightarrow \{0,1\}^M$ and an integer $0 \le j \le 2^M - 1$, decide if the *set* $\{i \mid f(i) = j\}$ has some global property (e.g. is nonempty, periodic, etc.).**

One might think such problems could be efficiently solved on a quantum computer by applying a unitary transformation $\boldsymbol{U}_f$ (which computes the function f) to a superposition,

$$\underline{U}_f(|\Omega\rangle|\mathbf{0}\rangle) = 2^{N/2}\sum_{i=0}^{2^N-1}|i\rangle|f(i)\rangle,$$

followed by measurement of the output qubit's state. But according to von Neumann's **measurement postulate**:

> **The result of a measurement on a quantum system in a superposition is a random term in the superposition, each with probability equal the modulus of its coefficient.**

For $|\Omega\rangle|\mathbf{0}\rangle$, this implies the chance of observing a given $|j\rangle$ is

$$Pr(i\,|\,f(i)=j) = |\{i\,|\,f(i)=j\}|/2^N,$$

which may be *exponentially* small. Even if it is not small, some properties of $\{i\,|\,f(i)=j\}$ (e.g. periodicity) can only be found by enumeration all or most of it.

There is a way around this: If one adjusts the *phases* of the terms of the input superposition appropriately, an additional transformation can be found that will *amplify* the magnitude of the coefficients associated with the solution(s), such that the probability of *finding* the solution upon making a measurement becomes appreciable. Because of an analogy with light diffraction, this is usually called **interference**.

Example: The Deutsch-Jozsa algorithm.

Suppose we are given a function $f:\{0,1\}\to\{0,1\}$, and ask:

- Is f a **constant** function, i.e.
  $(|\{i\,|\,f(i)=0\}|=0)$ or $(|\{i\,|\,f(i)=1\}|=0)$, **or**:
- Is f a **balanced** function, i.e.
  $|\{i\,|\,f(i)=0\}| = |\{i\,|\,f(i)=1\}|$ **??**

(two of the four possible functions $f:\{0,1\}\to\{0,1\}$ are constant, while the other two are balanced). This can be determined classically only by evaluating f on *both* inputs.

1) Starting with $|01\rangle\equiv|0\rangle|1\rangle$, apply the Hadamard gates:

$$|\psi_1\rangle\equiv\left(\underline{\boldsymbol{R}}_{\mathrm{H}}^{1}\underline{\boldsymbol{R}}_{\mathrm{H}}^{2}\right)|01\rangle\equiv(\underline{\boldsymbol{R}}_{\mathrm{H}}|0\rangle)(\underline{\boldsymbol{R}}_{\mathrm{H}}|1\rangle) = \tfrac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)$$

2) Evaluate f via its unitary transformation $\boldsymbol{U}_f$:

$$|\psi_2\rangle\equiv\underline{\boldsymbol{U}}_f|\psi_1\rangle = \tfrac{1}{2}(\underline{\boldsymbol{U}}_f|0\rangle|0\rangle+\underline{\boldsymbol{U}}_f|1\rangle|0\rangle-\underline{\boldsymbol{U}}_f|0\rangle|1\rangle-\underline{\boldsymbol{U}}_f|1\rangle|1\rangle)$$

$$= \tfrac{1}{2}(|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle-|0\rangle|\bar{f}(0)\rangle-|1\rangle|\bar{f}(1)\rangle)$$

where $\bar{f}=1-f$ is the **complement** (or **negation**) of f.

3) Using the fact that

$$|f(i)\rangle-|\bar{f}(i)\rangle = \left\{\begin{matrix}|0\rangle-|1\rangle & \text{if } f(i)=0\\ |1\rangle-|0\rangle & \text{if } f(i)=1\end{matrix}\right\} = (-1)^{f(i)}(|0\rangle-|1\rangle)$$

we can rewrite this as follows:

$$|\psi_2\rangle = \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)(|0\rangle - |1\rangle)$$

4) Now apply the same pair of Hadamard gates again:

$$|\psi_3\rangle \equiv \left(\underline{\boldsymbol{R}}_{\mathrm{H}}^{1}\underline{\boldsymbol{R}}_{\mathrm{H}}^{2}\right)|\psi_2\rangle \qquad (\text{since } \underline{\boldsymbol{R}}_{\mathrm{H}}(|0\rangle - |1\rangle) = \sqrt{2}|1\rangle)$$

$$= \frac{1}{2}\Big((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)\Big)|1\rangle$$

5) This in turn may be rewritten as

$$|\psi_3\rangle = \begin{cases} (-1)^{f(0)}|0\rangle|1\rangle & \text{if } f(0) = f(1) \\ (-1)^{f(0)}|1\rangle|1\rangle & \text{if } f(0) = \bar{f}(1) \end{cases}$$

showing the concentration of coherence via interference.

6) Thus measurement of the "input" (left-most) qubit gives $|0\rangle$ if f is *constant* and $|1\rangle$ if f is *balanced*.

The remarkable thing is that this took only a *single* evalua-tion of the function f. This algorithm was the first hint that quantum computers are more powerful than classical.

NB: A general quantum search algorithm is known which is quadratically faster than classical linear search, but *very* few quantum algorithms are known that are exponentially faster.

The Geometry Behind the Logic

The Hadamard Gate Revisited

Recall the action of the Hadamard gate on basis states:

$$\underline{\boldsymbol{R}}_{\mathrm{H}}|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \qquad \underline{\boldsymbol{R}}_{\mathrm{H}}|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\ ,$$

The idempotents corresponding to the resulting states are:

$$\underline{\boldsymbol{R}}_{\mathrm{H}}\underline{\boldsymbol{E}}_{+}\tilde{\underline{\boldsymbol{R}}}_{\mathrm{H}} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \leftrightarrow \quad \boldsymbol{G}_{+} \equiv (1+\sigma_1)/2$$

$$\underline{\boldsymbol{R}}_{\mathrm{H}}\underline{\boldsymbol{E}}_{-}\tilde{\underline{\boldsymbol{R}}}_{\mathrm{H}} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \quad \leftrightarrow \quad \boldsymbol{G}_{-} \equiv (1-\sigma_1)/2$$

We can also show that

$$\begin{aligned} \underline{\boldsymbol{R}}_{\mathrm{H}}(|0\rangle + \imath|1\rangle)/\sqrt{2} &= ((|0\rangle + |1\rangle) + \imath((|0\rangle - |1\rangle)))/2 \\ &= ((1+\imath)|0\rangle + (1-\imath)|1\rangle)/2 \end{aligned}$$

which becomes $(|0\rangle - \imath|1\rangle)/\sqrt{2}$ on multiplying thru by the phase factor $(1-\imath)/\sqrt{2}$. The corresponding idempotents are:

$$(|0\rangle \pm \imath|1\rangle)(\langle 0| \pm \imath\langle 1|) = \frac{1}{2}\begin{bmatrix} 1 & \mp\imath \\ \pm\imath & 1 \end{bmatrix} \quad \leftrightarrow \quad \boldsymbol{F}_{\pm} \equiv (1 \pm \sigma_2)/2$$

Since $(\boldsymbol{R}_{\mathrm{H}})^2 = 1$ and maps $\boldsymbol{x} \leftrightarrow \boldsymbol{z}$ & $\boldsymbol{y} \leftrightarrow -\boldsymbol{y}$, it follows that $\boldsymbol{R}_{\mathrm{H}}$ is just a *rotation* by π about the axis $\boldsymbol{h} = (\sigma_1 + \sigma_3)/\sqrt{2}$!

Recall such rotations can be written in exponential form as

$$\exp(-\imath(\pi/2)\boldsymbol{h}) = -\imath\boldsymbol{h} \quad \text{(since } \boldsymbol{h}^2 = 1\text{)}.$$

It may be observed that $(-\imath\boldsymbol{h})^2 = -1$, due to a geometrically irrelevant global phase (a **gauge** degree of freedom); the phase corrected Hadamard gate is

$$\boldsymbol{R}_{\mathsf{H}} = \exp(\imath(\pi/2)(1-\boldsymbol{h})) = \boldsymbol{h}\ ; \quad \text{similarly,}$$

the NOT operation $\boldsymbol{N}$ is a rotation by π about σ_1, i.e. $\boldsymbol{N} = \sigma_1$.

The c-NOT Gate Revisited

Recall that the c-NOT gate takes the NOT of one qubit if the other is $|1\rangle$, e.g.

$$\underline{\boldsymbol{S}}^{2|1}|00\rangle = |00\rangle \qquad \underline{\boldsymbol{S}}^{2|1}|01\rangle = |01\rangle$$

$$\underline{\boldsymbol{S}}^{2|1}|10\rangle = |11\rangle \qquad \underline{\boldsymbol{S}}^{2|1}|11\rangle = |10\rangle$$

Using the nilpotent **transition operators** $|0\rangle\langle 1|$ & $|1\rangle\langle 0|$, we can write this as

$$\begin{aligned}
\underline{\boldsymbol{S}}^{2|1} &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\
&= |00\rangle\langle 00| + |01\rangle\langle 01| + \underline{\sigma}_1^2(|10\rangle\langle 10| + |11\rangle\langle 11|) \\
&= (|0\rangle\langle 0|)(|0\rangle\langle 0| + |1\rangle\langle 1|) + \underline{\sigma}_1^2(|1\rangle\langle 1|)(|0\rangle\langle 0| + |1\rangle\langle 1|) \\
&= |0\rangle\langle 0| \otimes \mathbf{1} + (|1\rangle\langle 1| \otimes \mathbf{1})\underline{\sigma}_1^2 \quad \leftrightarrow \quad \boldsymbol{E}_+^1 + \boldsymbol{E}_-^1\sigma_1^2
\end{aligned}$$

This has an interesting ideal-theoretic interpretation:

Rotate qubit 2 by π in the left-ideal defined by $\boldsymbol{E}_-^1$, but leave it alone in the complementary ideal defined by the annihilating idempotent $\boldsymbol{E}_+^1$.

Using a well-known formula for the exponential of any-thing times a commuting idempotent, this may be written as

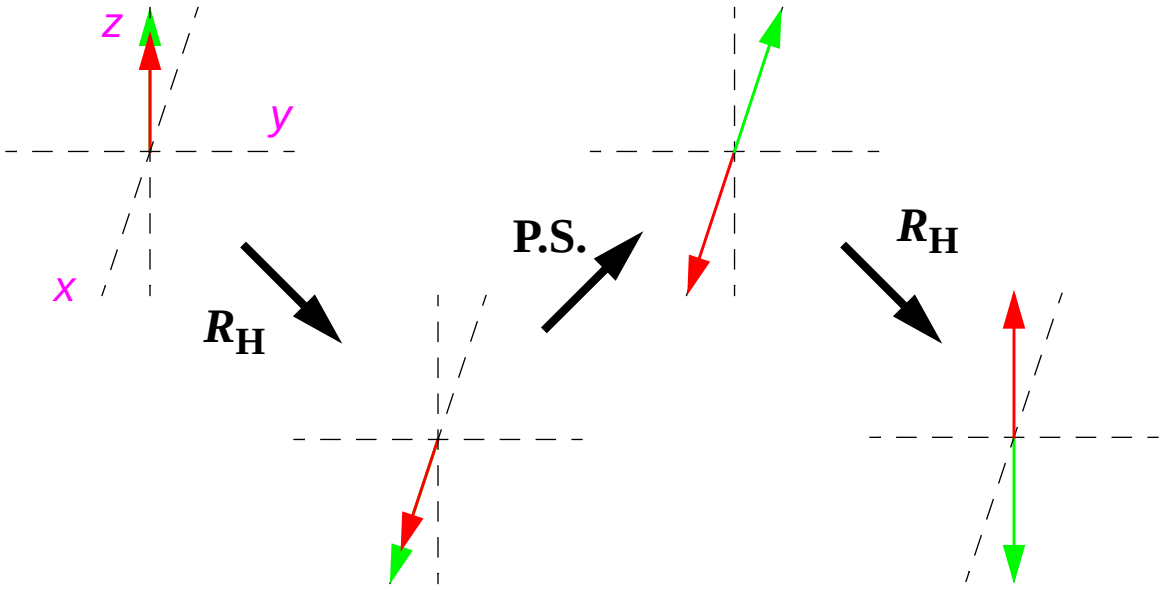
$$\exp(\imath(\pi/2)\boldsymbol{E}_-^1(1-\sigma_1^2)) = (1-\boldsymbol{E}_-^1)+\boldsymbol{E}_-^1\exp(-\imath(\pi/2)(1-\sigma_1^2))$$
$$= \boldsymbol{E}_+^1+\boldsymbol{E}_-^1\sigma_1^2 = 1-2\boldsymbol{E}_-^1\boldsymbol{G}_-^2 \ .$$

More generally, a **conditional rotation** is a rotation of a qubit in the left-ideal generated by the idempotents of the given states of one or more other qubits.

Noting that $\imath\sigma_3\boldsymbol{E}_\pm = \pm\imath\boldsymbol{E}_\pm$ so that rotations about σ_3^1 in the ideal generated by $\boldsymbol{G}_-^2$ are also conditional phase shifts, the form $1-2\boldsymbol{E}_-^1\boldsymbol{G}_-^2$ makes it clear that $\boldsymbol{S}^{2|1}$ can alternatively be viewed as a phase shift of the first qubit conditional on the second being along $-\boldsymbol{x}$. We can therefore write $\boldsymbol{S}^{2|1}$ as a phase shift conditional on both qubits being along $-\boldsymbol{z}$, sandwiched between two Hadamards, as follows:

$$\boldsymbol{R}_{\mathsf{H}}^2\exp(-\imath\pi\boldsymbol{E}_-^1\boldsymbol{E}_-^2)\boldsymbol{R}_{\mathsf{H}}^2 = \exp(-\imath\pi\boldsymbol{E}_-^1\boldsymbol{R}_{\mathsf{H}}^2\boldsymbol{E}_-^2\boldsymbol{R}_{\mathsf{H}}^2) = \exp(-\imath\pi\boldsymbol{E}_-^1\boldsymbol{G}_-^2)$$

Using **green** & **red** arrows for the qubit projected onto the E^1_- & E^1_+ ideals, this can be represented by vector diagrams as follows:



This is actually rather close to how $S^{2|1}$ is implemented in NMR spectroscopy, which also makes common use of such dia-grams without recognizing their ideal-theoretic connection.

The Deutsch-Jozsa Algorithm Revisited

The initial superposition in the Deutsch-Jozsa algorithm is

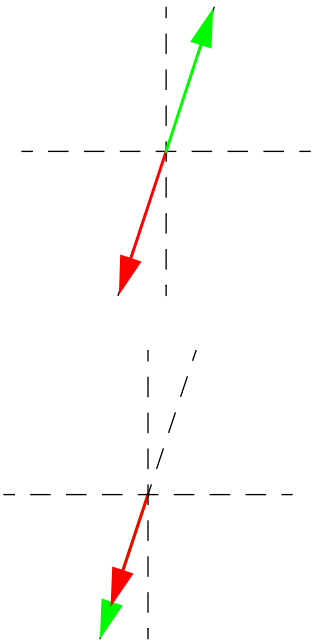
$$|\psi_1\rangle\langle\psi_1| = G^1_+ G^2_- = \tfrac{1}{4}(1 + \sigma^1_1 - \sigma^2_1 - \sigma^1_1\sigma^2_1)$$

If $f(0) = f(1) = 0$, $U_f = 1$ and so the final Hadamards just transform this back to $E^1_+ E^2_-$, telling us it's constant.

Now suppose we have the function $f(0) = 0,\ f(1) = 1$. Then $\boldsymbol{U}_f = \boldsymbol{S}^{2|1}$, i.e. the output qubit is flipped from $|0\rangle$ to $|1\rangle$ when the input bit is $|1\rangle$. How does this act on the product operators in the initial state? To answer that question by geometric reasoning only, let us go into the ideals generated by $\boldsymbol{G}^2_-$ and $\boldsymbol{G}^2_+$, where we find that

$$\sigma^1_1\sigma^2_1 = \sigma^1_1\sigma^2_1(\boldsymbol{G}^2_+ + \boldsymbol{G}^2_-) = \sigma^1_1\boldsymbol{G}^2_+ - \sigma^1_1\boldsymbol{G}^2_-.$$

This shows that this state is that shown on the right, i.e. the two components of the first qubit point in opposite directions along $\boldsymbol{x}$. We know that $\boldsymbol{S}^{2|1} = 1 - 2\boldsymbol{E}^1_-\boldsymbol{G}^2_-$ will rotate the green one by π about $\boldsymbol{z}$ to give us the state:



$$\sigma^1_1\boldsymbol{G}^2_+ + \sigma^1_1\boldsymbol{G}^2_- = \sigma^1_1.$$

Thus the net effect of $\boldsymbol{S}^{2|1}$ is to do a swap,

$$\sigma^1_1 \quad \leftrightarrow \quad \sigma^1_1\sigma^2_1 \quad ;$$

applied to $|\psi_1\rangle\langle\psi_1|$, it swaps the signs of these terms (while it commutes with & hence has no effect on σ^2_1), so we get:

$$\boldsymbol{S}^{2|1}|\psi_1\rangle\langle\psi_1|\boldsymbol{S}^{2|1} = \tfrac{1}{4}(1 - \sigma^1_1 - \sigma^2_1 + \sigma^1_1\sigma^2_1) = \boldsymbol{G}^1_-\boldsymbol{G}^2_-$$

The final Hadamards convert this to $\boldsymbol{E}^1_-\boldsymbol{E}^2_-$ as expected.

CLOSING REMARKS

The Future of Quantum Computing

1) To date, computers have done more than theory has in enabling us to deal with *complexity* in the natural sciences (and elsewhere), because very simple local dynamics can model arbitrarily complex global behavior.

2) The situation in *multiparticle quantum systems* is similar: Simple (indeed linear) local dynamics can lead to very complex large-scale behavior, including the apparent non-linearities of the classical world.

3) Quantum computers may yield only modest advantages in combinatorial problems, but they will certainly provide a powerful means of simulating *general* quantum systems.

4) Thus the advent of quantum computers will greatly extend the reach of *fundamental physics* to the complex systems found in *chemistry* and *molecular biology*.

5) Meanwhile, there is much to be learned about how simple quantum dynamics leads to classical complexity (even chaos), which is the subject of the theory of *decoherence*.

6) By computing with *homomorphic images* in Clifford algebras, this may even enable theorems to be "proved" by experiment (for CaF_2, a dimension of $2^{10^{11}}$ has been reached).