Algebraic Geometry Lecture 8 – Quantum Algebraic Geometry

Jon Allcock

In classical computing we work with *bits* (*bi*nary digi*ts*), i.e. elements from the set $\{0,1\}$. Here the state space is simply $\{0,1\}$. If we have n bits then our state space is $\{0,1\}^n$, which has size 2^n. So although our state space grows exponentially, the number of pieces of information we need in order to specify an element in the space only grows linearly. Obviously we can measure a given state: simply by looking at it we can see if the state is 0 or 1. These states can also be copied. That is there is a map $\{0,1\} \to \{0,1\}^2$ which copies whatever we input to the second coordinate.

Quantum mechanics.

In quantum mechanics a state is not a single number but rather a vector $|\psi\rangle \in \mathscr{H}$ for a complex Hilbert space $\mathscr{H}$. Here ψ is called a "state vector" or "wave function".

A quantum bit, or *qubit*, is a linear combination

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$ (normalisation). This can be written

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle.$$

So a general qubit can be identified with a point on the sphere, (whereas in classical computing the only two points allowed are the north and south poles).

Multiple qubits.

For more than one qubit we need the tensor product. If

$$\begin{cases} |\psi\rangle_A : \{|0\rangle_A, |1\rangle_A\} \\ |\psi\rangle_B : \{|0\rangle_B, |1\rangle_B\}, \end{cases}$$

then

$$|\psi\rangle_{AB} : \{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}.$$

To simplify the notation we write $|00\rangle$ for $|0\rangle \otimes |0\rangle$. Then, in general,

$$|\psi\rangle_{AB} = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle.$$

Measurement.

If we measure a given state we would expect

$$|0\rangle \xrightarrow{\text{measure}} 0$$
$$|1\rangle \xrightarrow{\text{measure}} 1$$

and, postmeasurement, we would still have $|0\rangle$ and $|1\rangle$ respectively. But for a general state vector we have:

$$\begin{array}{cccc} \text{Premeasurement} & & & \text{Postmeasurement} \\ \alpha|0\rangle + \beta|1\rangle & \xrightarrow{\text{measure}} & \begin{cases} 0 \text{ with probability } |\alpha|^2 \\ 1 \text{ with probability } |\beta|^2 \end{cases} & \begin{array}{c} |0\rangle \\ |1\rangle \end{array} \end{array}$$

This is called the collapse of the wave function.

Theoretically we can store arbitrarily much information in a qubit, say in the decimal expansion of α. But if we measure the qubit to recover this information then it collapses to either $|0\rangle$ or $|1\rangle$. So to get the information back we would have to copy the state vector many times and build up statistical information on α and β until we knew them with sufficient accuracy to recover the stored information. But can an arbitrary qubit be copied? This is answered by...

No cloning theorem.

For a unitary operator U we want our "copying machine" to map

$$\begin{aligned} U(|0\rangle_A \otimes |i\rangle_B) &= |0\rangle_A \otimes |0\rangle_B \\ U(|1\rangle_A \otimes |i\rangle_B) &= |1\rangle_A \otimes |1\rangle_B. \end{aligned}$$

But then

$$\begin{aligned} U\left((\alpha|0\rangle_A + \beta|1\rangle_A) \otimes |i\rangle_B\right) &= \alpha U(|0\rangle_A \otimes |i\rangle_B) + \beta U(|1\rangle_A \otimes |i\rangle_B) \\ &= \alpha|00\rangle + \beta|11\rangle \\ &\neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle). \end{aligned}$$

Entanglement.

Classical bits are always expressible as a product state, e.g. as an element of $\{0,1\} \times \{0,1\}$. So we could write an element of this space as 01 and we can split up the two parts: $0 \mid 1$. We can sometimes do this with qubits, for example:

$$|0\rangle_A \otimes |0\rangle_B = |0\rangle_A \,\big|\!\!\!\otimes |0\rangle_B.$$

Even in more complicated examples this is sometimes possible:

$$\begin{aligned} \frac{1}{\sqrt{2}}|0\rangle_A \otimes |0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A \otimes |0\rangle_B &= \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right) \otimes |0\rangle_B \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right) \big|\!\!\!\otimes |0\rangle_B. \end{aligned}$$

Some states simply cannot be split up like this though, for example:

$$\frac{1}{\sqrt{2}}|0\rangle_A \otimes |0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A \otimes |1\rangle_B.$$

This final example is thus called *entangled* (in this case it is maximally entangled). The unit of entanglement is the *ebit*, or entangled bit. Entanglement is denoted diagrammatically by $\bullet\!\!\sim\!\!\sim\!\!\bullet$.

Quantum entanglement allows "quantum teleportation". Suppose Andrew and Jon create an ebit and then go their separate ways. At some point in the future Andrew takes his entangled qubit, and a second qubit that he wants to "teleport" to Jon, say $|\psi\rangle$. He can measure the two qubits and he will get one of the four results

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Now Andrew can send his result to Jon and upon applying the inverse mapping Jon will have a copy of $|\psi\rangle$. So the qubit can be teleported using two classical bits and one ebit. This does not mean that the information is transferred faster than light, though, as Andrew still needs to communicate the two classical bits to Jon somehow.

Schmidt rank.

A general 2-qubit state can be written

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle.$$

Claim: We can always write the above in the form

$$|\psi\rangle_{AB} = \sum_i \lambda_i |e_i\rangle_A |f_i\rangle_B$$

where $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ form orthonormal qubit bases and λ_i are coefficients. E.g.

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle_A \otimes |0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A \otimes |1\rangle_B.$$

The number of nonzero λ_i is called the Schmidt rank. It is a measure of entanglement, but not a very good one since some states may be only just entangled, yet have the same Schmidt rank as a maximally entangled state.

We can write $|\psi\rangle$ as

$$\begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix}$$

then the Schmidt rank is the linear rank of this matrix. If the Schmidt rank is 1 then the determinant vanishes, which determines the variety

$$D : c_{00}c_{11} - c_{01}c_{10} = 0.$$

An $m \times n$ matrix has rank $< r$ if and only if all order-r minors vanish, which again gives a variety

$$D_r(d_a, d_B) : \text{determinantal variety}.$$

Now suppose that $|\psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then we have:

Theorem. *The maximum dimension of a subspace $S \subset \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ of Schmidt rank $\geqslant r$ is*

$$(d_a - r + 1)(d_B - r + 1).$$

The natural space to study this in is projective space since here the dimension formula tells us that if projective varieties V and W in $\mathbb{P}^d$ have $\dim V + \dim W \geqslant d$ then $V \cap W \neq \emptyset$, which doesn't hold in general for affine space.