

1. QUANTUM CRYPTOGRAPHY AND DENSE CODING PROTOCOLS

1.1. **Quantum Cryptography.** The idea is simple:

A wants to send:	1001101
uses the key:	0111010
transmits:	1110111
B decodes by the key:	0111010
original results:	1001101

The key to making quantum cryptography work is randomly generating the keys in sync for both A and B. A creates a pair of particles with total spin 0 in some entangled state; 1 particle is sent to B. Both A and B randomly pick a direction $(\vec{x}, \vec{y}, \vec{z})$, measure the spin, and record the value. Then they communicate on an unencrypted line which directions they measured in which experiment and disregard experiments when they measured in different directions. From this now restricted list of results, they again check results to make sure there has been no interference, if everything is good, they use the remaining results to encrypt data that they send between each other.

If there was an eavesdropper who observed the original particles, then A and B would discover this in the last phase when they check a number of their answers.

1.2. **Dense Coding.** We begin with 2 spin 1/2 particles prepared such that they are entangled. B (Bob) has both particles and sends one to A (Alice). Alice makes a rotation, encoding some information and send it back to Bob. Bob performs a measurement on the particles. At first it may seem that Alice can only send 1 bit of information, however she can actually send 2 bits to Bob.

We are given some original state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$$

Alice, then performs 1 of 4 actions: a rotation around the x, y, or z axis or nothing. These correspond to the following matrices.

action	matrix
nothing	1
x-axis	$\sigma_{1,x}$
y-axis	$\sigma_{1,y}$
z-axis	$\sigma_{1,z}$

What should Bob measure? Consider that $\{(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle), (|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle), (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle), (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)\}$ form an ONB and so there exists a self-adjoint operator X such that these vectors are eigenvectors of X with different eigenvalues. By measuring these values you can determine the sent value. Since we have 4 possible outcomes, this is identical to sending 2 bits ($2^2 = 4$ options).

2. EPR

2.1. Background and Initial Formulation. The Einstein-Podolsky-Rosen (EPR) paradox is a thought experiment that began in the hopes of disprove quantum physics. In quantum physics, there's some uncertainty even if we know all the variables. EPR wanted to show that the even on the quantum level, everything was still in fact deterministic.

Take a decaying particle that splits into two particles A and B. Quantum physics says that momentum and position should be described operators that don't commute and they can't be measured jointly. So you could disprove quantum physics if you gave an experiment where you measured both position and momentum simultaneously with arbitrary precision. Of course designing such an experiment was difficult. However, due to conservation of momentum, we can find position and momentum of particle A by measuring position of A and the momentum of B (momentum of A = -momentum of B).

{perhaps explanation about in space time causal connection between two events X and Y. Question can X cause Y, or vice versa? A causal connection exists only if for all observers X happens before Y (absolute future, past, spatial to X and Y)}

2.2. Reformulation with spin-systems. You can look at the EPR with spins in different directions. We will examine this reformulation and the results. We have a spin-0 particle that decays into two spin-1/2 particles. Once they have reached some distance from each other, we measure each particle in a random choice of 3 directions, A, B, and C on a plane separated by 120 degrees. Classically we can represent the possible outcomes by 8 tables with an some assigned frequency.

	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
A	+	+	+	+	-	-	-	-
B	+	+	-	-	+	+	-	-
C	+	-	+	-	+	-	+	-

For example, if we measure the first particle in direction A and find that it's "+" and we measure the second particle in the direction B and get a "-", then according to the classical hypothesis, we have seen either t_1 or t_2 . We can formulate this as:

$$p("1, \vec{A} = +" \wedge "2, B = -") = \text{freq}(t_1) + \text{freq}(t_2).$$

However, from quantum physics and experiment, we know this value to be:

$$\dots = \frac{1}{4}(1 - \cos(\theta))$$

By evaluating at a number of different combinations we get the following tables. Theoretically, we should be able to solve for the frequencies of t_1, t_2, \dots, t_8 . However, no solution exists.

Consider the equations resulting from examining 1, \vec{A} and 2, \vec{B} :

(1) $t_3 + t_4 = 3/8$

(2) $t_1 + t_2 = 1/8$

(3) $t_7 + t_8 = 1/8$

(4) $t_5 + t_6 = 3/8$

Consider the equations resulting from examining 1, \vec{C} and 2, \vec{B} :

(5) $t_3 + t_7 = 3/8$

(6) $t_1 + t_5 = 1/8$

$$(7) \quad t_4 + t_8 = 1/8$$

$$(8) \quad t_2 + t_6 = 3/8$$

Also consider the equations resulting from $1, \vec{C}$ and $2, \vec{A}$:

$$(9) \quad t_5 + t_7 = 3/8$$

$$(10) \quad t_1 + t_3 = 1/8$$

$$(11) \quad t_6 + t_8 = 1/8$$

$$(12) \quad t_2 + t_4 = 3/8$$

(2) and (10) imply that $t_2 = t_3$ and also that $t_2 \leq 1/8$. Now consider (16), this implies that $t_4 \geq 1/2$. But (7) indicates that $t_4 \leq 1/8$. So there are no solutions.

This proves that there are probabilities based on inherent uncertainty within the system not simply on unknowns.

3. SYMMETRY OPERATIONS, WIGNER'S THEOREM, AND THE 'NO CLONE' THEOREM

Definition 3.1. $\alpha : \Pr(\mathcal{H}) \rightarrow \Pr(\mathcal{H})$, α takes an event to an event. α is a **symmetry** if it's a bijection and satisfies:

- (1) $P \leq Q \Rightarrow \alpha(P) \leq \alpha(Q)$
- (2) $P = \neg Q \Rightarrow \alpha(P) = \neg\alpha(Q)$

In other words, a symmetry is a map that does not change the relation between events.

Theorem 3.1. (Wigner, 1931) $\dim(\mathcal{H}) > 2$. If α is a symmetry, then either

- $\exists U$ unitary: $\alpha(\cdot) = U \cdot U^{-1}$
- $\exists V$ anti-unitary: $\alpha(\cdot) = V \cdot V^{-1}$.

U and V are unique up to scalar multiples.

Wigner's theorem gives us the result that for any symmetry operation can be represented by a unitary or anti-unitary operator. Moreover, if performed on entangled particles these operations do not ruin the entanglement. Also, note that the converse of Wigner's theorem is true (trivially): if $U \in B(\mathcal{H})$ is unitary, the $\alpha(\cdot) := U \cdot U^*$ is a symmetry.

Theorem 3.2. (No-Clone Theorem, 1982) We have two identical systems in the states D and D_0 respectively. Putting the two together we get a larger system in the state $D \otimes D_0$. It is not possible to make a physical operation that given any D and D_0 always yields the new state $D \otimes D$.

Proof. Take e_1, e_2, \dots, e_n an ONB in (H) with $n \geq 2$. Consider a density operator:

$$\tilde{D} := \frac{1}{n} \sum_1^n |e_k\rangle\langle e_k|$$

Combine this system with another identical system in the state D_0 . We know that $|e_k\rangle\langle e_k| \otimes D_0 \rightarrow |e_k\rangle\langle e_k| \otimes |e_k\rangle\langle e_k|$. So

$$\tilde{D} \otimes D_0 \rightarrow \frac{1}{n} \sum_1^n |e_k\rangle\langle e_k| \otimes |e_k\rangle\langle e_k|$$

However, $\sum |e_k\rangle\langle e_k| = 1$, independent of basis.

□

Although, we cannot clone perfectly, we can do so with some errors and we can also copy the first one, but in so doing we destroy the first. The underlying reason is the inability to truly measure the entangled states that the particles may be in without ruining their entanglement.

4. GLEASON'S THEOREM AND IMPORTANCE

The conclusion of quantum mechanics is that there are no hidden variables in the system, instead there is some hesitancy. In the 1950's and 1960's there was a flurry of academic activity that tried to both mathematically substantiate the claim, and also those that tried to argue the opposite. The first milestone in establishing the validity of quantum mechanics was a theorem by Von Neumann. In addition to helping prove that there were no hidden variables in the system, he did a lot to help formalize the mathematics representing the physical operations already being done.

Theorem 4.1. (Von Neumann) *Expected value maps a quantity to a value such that it is:*

(1) *linear*

(2) *positive if A is a real-valued physical quantity. In other words the expected value: $E(A^2) \geq 0$.*

If $\phi : B(\mathcal{H}) \rightarrow \mathbb{R}$, where $\phi(A^2) \geq 0$ and $\phi(\infty) = 1$, then there exists a unique density operator D such that $\phi(A) = \text{Tr}(DA)$ for all A .

Von Neumann's proof was correct mathematically, but it doesn't quite make sense since the linear assumption is wrong. The assumption is that $\phi(A+B) = \phi(A) + \phi(B)$. There are many cases where $A+B$ is not defined - particularly in the case where the two physical quantities cannot be measured together. Mackey noted linearity should hold only if the operators corresponding to the physical quantities commute. Gleason proved this proposition in 1957, proving von Neumann's result without assuming that the expectation function is linear.

Theorem 4.2. (Gleason's Theorem) *If $\dim \mathcal{H} \neq 2$ and $p : Pr(\mathcal{H}) \rightarrow [0, 1]$ is a probability law, then there exists D a density operator such that $D = \phi_D$.*

If P and Q are exclusive then $p(P \vee Q) = p(P) + p(Q)$.

Gleason's theorem shows that the formalism of quantum mechanics gives no space for hidden variables. So either quantum mechanics is wrong, or there are no hidden variables in the real world system. The EPR paradox provides a solution to this problem.