CONTENTS

10 QUANTUM GAMES 3
10.1 Quantum Game 1: Bell 3
10.2 Quantum Game 2: CHSH 5
10.3 Quantum Game 3: GHZ 6
11 WHY QUANTUM MECHANICS? 9
11.1 Recap 9
11.2 Why Quantum Mechanics? 10
11.2.1 Well, why not? 10
11.2.2 Why complex numbers? 10
12 11
13 POSTULATE 3: MEASUREMENT 13
14 QUANTUM COMPUTATION 15
14.1 Quantum Computation: Introduction 15
14.1.1 Quantum Entanglement 15
14.1.2 Qubits 16
14.2 Quantum Cryptography 16

10

QUANTUM GAMES

10.1 QUANTUM GAME 1: BELL

Quantum Casino: Bell

Consider the following shell game:

There are three boxes (labeled left, middle, right (L,M,R for short)) within which is contained a single card that is either black or red. The house states that the cards are arranged such that:

If you reveal the left and middle (LM) boxes, or the right and middle (RM) the cards are always the same color.

If you reveal the left and right boxes (LR) the cards have opposite color.

Clearly we can not achieve this by having three independent cards (there does not exist a jpd), so two house employee's assist with the game. Your goal is to try to maximize the number of times that the above conditions are violated, while only revealing 2 (or 1) of the boxes. (You are not allowed to open all three.) The two employees (Alice and Bob) will try to maximize the conditions above.

Payouts:

The house and you are given an initial fixed amount of dollars (chips).

P1: If the conditions above are met, you pay the house \$1 (-\$1 to your balance).

P2: If the conditions above are not met, the house pays you \$2 (+\$2).

P3: : If each query the same box, and different outcomes result, house pays you $\$1 \times 10^{12}$ and goes out of business (game over).

Alice and Bob are not allowed to communicate during any single trial. They can use prearranged strategies.

Each round will occur as follows:

1) Contestant querying Alice to reveal the first box. Alice will state the outcome of the chosen box (red/black).

2) The contestant then queries Bob to reveal the second box (or the same). Bob states the outcome of the chosen box.

3) The dealer determines whether the conditions are met and performs the appropriate payment.

The contestant can end at any time, or until one of the parties runs out of money.

Classical probability analysis

Let's calculate the expectation for the contestant to win and see if this is a fair game.

We ignore the P3 outcome as that ends the game.

We have the correlations $\bar{L}M\rangle = \langle RM\rangle = +1, \langle LR\rangle = -1$.

Consider the case where results are all equiprobable (construct jpd).

L	M	R	satisfied	violated
b	b	b	LM, RM	LR
b	b	r	LR, LM	RM
b	r	b		LM, RM ,LR
b	r	r	LR, RM	LM
r	b	b	LR, RM	LM
r	b	r		LM, RM ,LR
r	r	b	LR, LM	RM
r	r	r	LM, RM	LR

As a potential prearranged strategy, the house can set the probability for (b,r, b) and (r, b,r) to o to gain an advantage as those outcomes always violate the conditions.

Examining the total number of outcomes, we see that in any round, there is at least

1/3 probability that the conditions are violated,

2/3 probability that the conditions are met.

Thus the expected gain for the contestant is, ($2)(1/3) + (-$1)(2/3) = $o.

This is a fair game as constructed.

Quantum analysis: "House always wins."

With classical resources (prearranged strategies) we see that this is a fair game. The question is, can the house tilt the odds in their favor? With quantum resources, yes! (Up to -$o.25 for the contestant.)

Here's how. As they are allowed to share resources in advance, but not allowed to communicate, they share an entangled pair of photons. Say they are in the state $|\psi\rangle = \frac{1}{\sqrt{2}}[|+-\rangle - |-+\rangle]$, where each have a qubit.

They now choose the following prearranged strategy to change the odds.

Alice:

Contestant C chooses:	Set polarization to	*Measure:*	If + return:	If - return:
L	$+30^o$		red	black
M	0^o		red	black
R	-30^o		red	black

Bob:

Contestant C chooses:	Set polarization to	*Measure:*	If + return:	If - return:
L	$+30^o$		black	red
M	0^o		black	red
R	-30^o		black	red

Let's check the payouts:

P3: First, let's check that the house never goes out of business:
If C chooses the same box, they are in the same basis and they always return the same result.

P1: If one of the choices includes M, notice that the angle between Alice and Bob is $|30^o|$. This gives the probability,

$$P(+-) = P(-+) = 3/8, \quad P(rr \text{ or } bb) = 3/4 \qquad \text{(details next page).}$$

P2: If C chooses LR, the bases are $|60^o|$ apart. This gives the probability,

$$P(+-) = P(+-) = 1/8, \quad P(rr \text{ or } bb) = 1/4.$$

The expected gain for C is now: ($2)(1/4) + (-$1)(3/4) = -$1/4 = -$o.25. The house has the advantage!

Quantum analysis 2:

Let's examine the details of calculating the probabilities.

The general form of the state takes this form in one of the three bases (L,M,R).

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|+-\rangle - |-+\rangle]$$

We want to find P(rr or bb), which corresponds to $P(+-\ or\ -+)$,

$$\begin{aligned} P(M+,L-) &= \frac{1}{2}\left|\langle M+|\langle L-|\left(|M+\rangle|M-\rangle - |M-\rangle|M+\rangle\right)\right|^2 \\ &= \frac{1}{2}\left|\langle M+||M+\rangle\langle L-||M-\rangle\right|^2 = \frac{1}{2}\left|\langle L-|M-\rangle\right|^2 = \frac{1}{2}\left|\cos^2 30^o\right|^2 = \frac{1}{2}\frac{3}{4} = \frac{3}{8} \end{aligned}$$

where the figure shows the projection.

When squared, we see this probability is 3/8. It is not hard to convince yourself that $P(-M,+L)$ also equals 3/8. Thus, $P(rr\ or\ bb) = 3/4$.

For this case, we want to find $P(rb\ or\ br)$, which corresponds to $P(++\ or\ --)$,

$$\begin{aligned} P(L+,R+) &= \frac{1}{2}\left|\langle L+|\langle R+|\left(|L+\rangle|L-\rangle - |L-\rangle|L+\rangle\right)\right|^2 \\ &= \frac{1}{2}\left|\langle R+|L-\rangle\right|^2 = \frac{1}{2}\left|\cos^2 30^o\right|^2 = \frac{1}{2}\frac{3}{4} = \frac{3}{8} \end{aligned}$$

Again, putting this altogether, the expected gain for C is:
($2)(1/4) + (-$1)(3/4) = -$1/4 = -$0.25.

10.2 QUANTUM GAME 2: CHSH

In this game we will represent inputs and outputs in binary form. In this game Alice and Bob are isolated from each other and each are given a random bit, Alice receives $x = 0, 1$ and Bob receives $y = 0, 1$, and their goal is to provide outputs, a and b, that maximize the following relation,

$$a \oplus b \quad = \quad xy.$$

You may recognize this as the defining relation for a PR box. If they satisfy this condition, they win $1 and if not, they lose $ 3. (We will see that for classical resources, this is a fair game.)

Classical analysis

The probability table representing the above relation is,

$(x,y)\|(a,b) \rightarrow$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$\frac{1}{2}$	0	0	$s\frac{1}{2}$
$(0,1)$	$\frac{1}{2}$	0	0	$\frac{1}{2}$
$(1,0)$	$\frac{1}{2}$	0	0	$\frac{1}{2}$
$(1,1)$	0	$\frac{1}{2}$	$\frac{1}{2}$	0

Thus, a simple (pre-established) strategy that Alice and Bob could employ is to simply always return 0. In this case, they win the game $\frac{3}{4}$ of the times. It can be proven that this is the maximal possible success probability in this game utilizing classical resources.

The expected gain in this scenario is,

$$\langle\$\rangle \quad = \quad (\$1)(\frac{3}{4}) + (-\$3)(\frac{1}{4}) = 0.$$

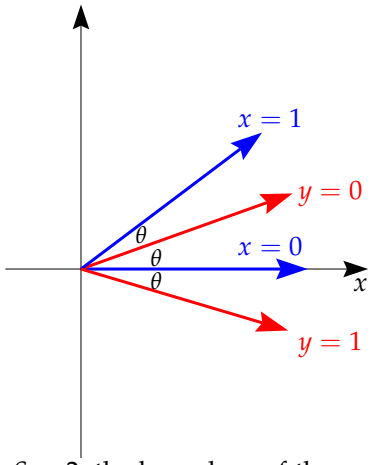
Thus, with only classical resources, this is a fair game.

The quantum edge

We now consider that Alice and Bob have access to quantum recourses, mainly entangled states. Thus, their prearranged strategy is as follows:

- They each obtain a photon in the entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle|0\rangle + |1\rangle|1\rangle]$.
- If Alice receives input $x = 0$, she simply measures her qubit. If she receives $x = 1$, she applies the unitary $\hat{U}(\frac{\pi}{4})$ to her qubit and then measures it. She outputs the outcome of her measurement.
- If Bob receives $y = 0$ he applies $\hat{U}(\frac{\pi}{8})$ and measures, for $y = 1$ he applies $\hat{U}(-\frac{\pi}{8})$

The figure shows the effect of $\hat{U}(\theta)$ on the H state. This algorithm yields the highest possible winning probability with quantum resources. It is left as an exercise to compute the maximum winning probability.



A little algebra will show that the maximum classical winning strategy corresponds to $S = 2$, the boundary of the local polytope, while the maximal quantum probability corresponds to $S = 2\sqrt{2}$. And of course, if Alice and Bob could share PR boxes, then they could win this game every time.

10.3 QUANTUM GAME 3: MERMIN SQUARE 1

We will preform the following two player game in class. There are two players, Alice and Bob (A & B) along with a referee (R). The procedure for the game is as follows:

There is a 3×3 board upon which Alice and Bob will be asked to fill with either $0, 1$. They are not allowed to communicate once the round has begun.

1. The referee picks a random row, $r \in \{1, 2, 3\}$ and a random column $c \in \{1, 2, 3\}$.
2. R sends the value r to Alice and c to Bob.
3. Alice fills the cells in row r with 0's and 1's and sends it to R. (Sent as a binary vector, r_i.)
4. Bob fills the cells in column c with 0's and 1's and sends it to R.
5. R checks that $r_1 \oplus r_2 \oplus r_3 = 0$.
6. R checks that $c_1 \oplus c_2 \oplus c_3 = 1$.
7. R checks that the cell where $r = c$ has the same value for Alice and Bob.
8. If items 5, 6, 7 are satisfied, Alice and Bob win, otherwise they lose.

Classical version of game

The first iteration of this game will be the classical version where Alice and Bob can devise strategies at the outset to satisfy the 3 constraints, but once the game begins, they can not communicate.

As a group, determine the maximal success rate for this version of the game.

Quantum version of the game

The rules are the same, however Alice and Bob may use an unlimited set of entangled particles (to keep it simple, let's restrict to bipartite two outcome entangled states -this is all you will need). Using entangled particles, what is the success probability now? What is the minimal number of entangled pairs do they need?

A potential strategy for the classical version of game

Now Alice and Bob can choose in advance how they will fill their rows and columns. This essentially asks the question whether we can fill the entire 3×3 satisfying all three constraints. A little exploration will see it is not possible. For one, every cell must be the same for Alice and Bob.

This reduces to the question can every row have even parity and every column have odd parity? By mapping to ± 1 values we can quickly see the answer. Each row must multiply to $+1$ while each column must multiply to -1. Considering the product of all terms, for Alice it must be $+1$, while for Bob it must be $-1 \times -1 \times -1 = -1$. Thus, it is not possible to fill the table in advance (i.e. there is no joint probability distribution over all possible outcomes).

What is left is to calculate the maximum probability in this scenario, clearly it can not be 1. It is not hard to see that if they try to make a deterministic strategy it is clear that the maximum success probability is $\frac{2}{3}$.

How would this be done? First, consider that Alice always fills every cell with a 0. This satisfies constraint 5 above. Now, Bob must have either one or three 1's in each column. To maximize the number of cells to be the same, he would obviously choose to have only a single 1 in each column. Thus constraints 5 and 6 are satisfied, with constraint 8 satisfied $\frac{2}{3}$ of the time. (Of course, what we are doing here is establishing a jpd which maximizes the success probability.)

A strategy for the quantum version of game

There is a, somewhat involved, algorithm to insure that Alice and Bob, with access to two pairs of entangled qubits, can win the game every time. We describe that below, but first we sketch the method.

First, Alice and Bob share two entangled pairs of qubits (1 & 2, and 3 & 4, with 1 and 3 going to Alice) in the following state:

$$|\Psi\rangle \quad = \quad \frac{1}{2}(|01\rangle - |10\rangle)_{12} \otimes (|01\rangle - |10\rangle)_{34} = \frac{1}{2}[|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle],$$

where the first two entries in the last term are qubits 1 and 3 (Alice's qubits) and the second two, 2 and 4, are Bob's qubits.

Alice applies one of three local unitary operations on her pair of quibits, (A_1, A_2, A_3) corresponding to the row which she is asked to fill in. Likewise, Bob has three, local, unitary operations (B_2, B_2, B_3) corresponding to which column he is asked to fill in. Once applied to the initial state, the three rules are satisfied. For example, consider $r = 1, c = 1$, in this case we have (up to phases which we just set to unity for clarity),

$$A_1 \otimes B_1|\Psi\rangle \quad = \quad \frac{1}{2\sqrt{2}}[|0000\rangle + |0001\rangle + |0100\rangle + |0101\rangle|1010\rangle + |1011\rangle + |1110\rangle + |1111\rangle].$$

This state builds in rule 7 (that the intersection of row and column yield the same result) as the first entry corresponds to Alice's entry into the first column of the first row, and the third entry is Bob's first entry of his column -the first and third entry are all the same. To satisfy rules 5 and 6 (Alice has even parity and Bob has odd parity) they simply set the last entry to satisfy the rule, given the first two entries. Explicitly, say the first measurement collapses to the 1110 case. Alice has entered two 1s in the first two entries of her row, to satisfy rule 5, she sets the third entry to 0. Likewise, Bob has filled his first two entries 10, thus he sets the third entry to 0 -all constraints have been met.

If either $r = 3$ or $c = 3$ is selected (or both), a transformed state can be created by local unitary transformations to satisfy the constraints. This state in the $r = 2, c = 3$ case looks as follow,

$$A_2 \otimes B_3|\Psi\rangle \quad = \quad \frac{1}{2\sqrt{2}}[|0000\rangle - |0010\rangle - |0101\rangle + |0111\rangle|1001\rangle + |1011\rangle - |1100\rangle - |1110\rangle].$$

The phases given here (and the form of the transformations to be given later) come from a paper by Brassard, Broadbent, and Tapp[1] Let's check one term 0111, verify that it works, and leave it as an exercise to show that the all terms satisfy the rules. Alice's first two entries are 01, thus, to satisfy rule 5, she sets her third entry as 1. Bob has entered 11 in the first two spots and, to satisfy rule 6, must enter a 1 in the last spot. Rule 7 has Alice's second entry, 1, equaling Bob's last.

1 G. Brassard, A. Brodbent, A. Tapp, "Quantum Pseudo-Telepathy" http://arxiv.org/abs/quant-ph/0407221v3 (2004).

Local unitary operators

The form of the operators that Alice and Bob apply during the game is a little tedious to work out, here we just state the result (as given by Brassard, et. al. in the previously mentioned paper).

$$A_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{pmatrix}, \quad A_2 = \frac{1}{2}\begin{pmatrix} i & 1 & 1 & i \\ -i & 1i & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & -i \end{pmatrix}, \quad A_3 = \frac{1}{2}\begin{pmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix},$$

$$B_1 = \frac{1}{2}\begin{pmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{pmatrix}, \quad B_2 = \frac{1}{2}\begin{pmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{pmatrix}, \quad B_3 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}.$$

These act (when tensored, e.g. $A_i \otimes B_j$) on the 16 dimensional Hilbert space with basis vectors ordered as follows (formed by tensoring the basis vectors together $|ij\rangle_{13} \otimes |kl\rangle_{24}$),

0000, 0001, 0010, 0011; 0100, 0101, 0110, 0111; 1000, 1001, 1010, 1011; 1100, 1101, 1110, 1111.

11

WHY QUANTUM MECHANICS?

11.1 RECAP

We have now established our three quantum postulates in a formal form,
QM Postulate 1: State
QM Postulate 2: Observables
QM Postulate 3: Measurement
QM Postulate 4: Time Evolution
We have explored several novel features that quantum mechanics introduces, some of these have been exploited to perform actions not possible with classical physics.

Superpositions

Classical physics consists of objects that have well-defined properties at all times. There exists states of quantum objects that do not have well defined properties. These objects have a probability to yield more than one result on a measurement of some property and thus before a measurement occurs it can not said to be in any one of the states possible. Such systems are described as *superpositions*, the simplest example being the following,

$$|\psi\rangle \quad = \quad \frac{1}{\sqrt{2}}\left[|\omega_1\rangle + |\omega_2\rangle\right].$$

An object that is in a superposition state of one observable may not be in a superposition of another observable. Thus, superposition is not a basis independent property -that is, if you change bases, you might find that it is not in a superposition (for polarization, there will always be a physical basis where the superposition becomes an eigenvector of some observable).

The physical phenomena of *interference* is evidence of a superposition state. Interference requires the possibility of the state being in a superposition of two or more outcomes.

Non-locality

When considering more than one quantum object, it is possible for the quantum state of the objects to entangled, that is, they can not be considered to be separate objects independent of each other prior to the first measurement. Entanglement is a resource that can be utilized to perform actions not possible with classical objects. It is a resource that is "used up" when a measurement occurs, the first measurement breaks the entangled state but establishes a correlation between the two outcomes. An example of the simplest maximally-entangled state of two objects can be expressed as (in terms of polarization),

$$|\psi\rangle_{1\,\&\,2} \quad = \quad \frac{1}{\sqrt{2}}\left[|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2\right].$$

When the first measurement occurs, the state collapses to the corresponding term in the superposition, which determines the state of the other particle at that time. An entangled state is defined as one that can not be factorized to to yield a product state, $|\psi\rangle_1|\phi\rangle_2$.

Violation of a Bell inequality (e.g. CHSH) informs us the system is not in a definite state, or that there does not exist a joint probability distribution (jpd).

Contextuality

The Kochen-Specker theorem discussed previously indicates, once again, that we can not ascribe predetermined values to measured values prior to measurement. What makes this differ from superposition is that even *compatible* measurements can not be said to be determined prior to a measurement. Explicitly it was shown that when measuring the sum of the squared outcomes of a spin 1 object simultaneously (allowable as the three squared observables commute), that it is not possible to assign predetermined values of 0 or 1 overall possible orientations, while adhering to the quantum constraint that the three outcomes add up to 2.

Physicists call this notion *contextuality* the outcomes of the third measurement in the spin 1 case depends on the *context* of the other two measurements (which direction they were measured in).

11.2 WHY QUANTUM MECHANICS?

11.2.1 *Well, why not?*

First of all, we have seen that classical physics can not explain all physical phenomena in our universe. Let's examine some variations , or deviations, from quantum mechanics. Scott Aaronson has said that quantum theory is nothing but an alternative theory of probability (I do not fully agree with this statement as there is a little more to it) so let's examine different possibilities.

Standard probability theory

In standard probability we have the probability state ω represented as a a real number and the probability norm is 1. This is another way to say that we simply add up the states to obtain the probability.

Quantum theory

Expressed in a similar manner, we consider the probability state (i.e. the quantum amplitude) to be a (possibly) complex number and probabilities are computed with a norm 2 measure (i.e. the Born probability rule),

$$p(x \; in \; \psi) \quad = \quad |\langle x|\psi\rangle|^2.$$

11.2.2 *Why complex numbers?*

One, mathematical, reason to possibly expect real numbers to represent the entirety of physical phenomena, is that they are not algebraically closed. That is, there are relations (i.e. equations) of real variables that do not have real solutions (e.g. $x^2 + 1 = 0$).

In comparison, complex numbers are closed algebraically. All mathematical relations can be expressed as complex numbers. This gives, at least a mathematical, reason to consider them as a means to represent all physical phenomena.

What about other fields? For example, quaternions

12

13

POSTULATE 3: MEASUREMENT

14

QUANTUM COMPUTATION

14.1 QUANTUM COMPUTATION: INTRODUCTION

In this course we have introduced the theory of quantum mechanics and explored the radical difference between it and classical physics. Often we stated properties in a negative tone, Ôyou can not think of trajectories, you can not think of it as being a definite state, there is no absolute determinism, etc.Õ. Even though we stated that quantum mechanics is arguably the most successful theory ever developed (though we do not have time to demonstrate how), it may seem that we have lost a lot in the end and people have a not-so-positive feeling for the subject. In this lecture we hope to stress some positives. We will introduce some of the cutting edge ideas to parlay the mysterious quantum entanglement that we have learned into new technologies. In fact, the arena of quantum information theory is a rapidly growing field that may someday revolutionize technology as a whole. Some claim the change in computing abilities from classical computers (like what you may use to view this document – even though it is utilizing some quantum aspects its core logic is classical) will be similar from the days prior to electronic computers to todayÕs computers. We will introduce four main quantum information technologies in some detail that have been theoretically devised and are becoming realized slowly in laboratories. They are,

Quantum Cryptography

Quantum Computing

Dense Coding

Quantum Teleportation

There are others, but we only have limited time. Hopefully you will agree that the future of quantum mechanics is filled with many fascinating avenues to pursue.

Not only are quantum phenomena important for these novel applications they will also become more important as traditional electronic technologies continue to shrink in scale. Even now quantum effects must be considered when designing computer chips and as the desire to make them smaller presses on, quantum mechanical effects will be more prevalent. We mentioned in the lecture on the Heisenberg Uncertainty Principle that the vacuum fluctuations which give rise to the Casimir force may become prominent in developing nanotechnological devices (the nano refers to nanometer scale objects which we have seen is wrought with quantum effects). We will not cover other areas like quantum gravity, though these attempts at uniting quantum mechanics and general relativity is at the center of theoretical physics research.

14.1.1 *Quantum Entanglement*

Recall that we discussed a pair of objects created from the decay of an object in the EPR gedankenexperiment. We discovered via BellÕs inequality that a local deterministic hidden variable theory could not explain all of the outcomes of an experiment. We found that the particles are truly in a superposition state prior to measurement and that measuring one instantaneously changed the state (wavefunction) of the other. These two objects must be treated as one extended wavefunction prior to a measurement. We say that these particles are entangled (other terms are EPR-pair, Bell state pair). It is possible to entangle many objects at the same time as well.

Recall that the state vector for the case of two entangled photons, created in an NLC, was expressed,, in the z basis and prior to measurement as,

14.1.2 *Qubits*

If we consider only one quantum two-state object that may be in one particular quantum state we can represent it as a vector in our Hilbert state space discussed previously. Such an object is the analog of the classical bit and is called a quantum bit or qubit. In most of what follows we discuss the manipulation of qubits, just as classical information theory deals in the manipulation of bits. (We now briefly return to representing our object as a polarization state). If the object is in a state of definite of HV polarization (either |1> or |0>) from previous discussions we know that it is not in a definite state of PM (or x) polarization, $|P\rangle = \frac{1}{\sqrt{2}}[|H\rangle + |V\rangle]$ or $|M\rangle = \frac{1}{\sqrt{2}}[|H\rangle - |V\rangle]$ nor is it in a definite state in the y basis. We can x2 x2 attempt to represent the arbitrary state of our qubit in (yet another) abstract three-dimensional space. This space is sometimes called a Bloch space and describes the state vector as a projection along the three basis directions.

This pictorial description will not be entirely necessary in what follows but it may provide a means to help visualize the coming discussion.

Notice that for a classical bit there are only two possible states, 0 and 1. For the qubit the state can be in an infinite number of different superpositions,

$$|\psi\rangle \quad = \quad \alpha|0\rangle + \beta|1\rangle, \qquad\qquad \text{with the constraint } \; |\alpha|^2 + |\beta|^2 = 1.$$

When a measurement is made on the qubit only a 0 or 1 results, thus you may be led to believe that the information content of one qubit is the same as for a classical bit. However, we know from our dealings with superpositions that the relative phases (α and β here) our important in quantum processes. Hence, the information content in one single qubit is much more than for a classical bit. This is one indication that a quantum computer may be able to process vastly more information than a classical computer. How all of that information is extracted, or processed, requires some work to figure out.

A simple calculation may shed some light on the differences. Consider 500 qubits, which can be represented physically as 500 atoms in one of two states or 500 polarized photons. The basis states of this system can be represented as,

$$|q_1 q_2 q_3 \cdots q_{500}\rangle \quad \equiv \quad |q_1\rangle|q_2\rangle|q_3\rangle \cdots |q_{500}\rangle, \qquad\qquad q_i = 0, 1.$$

A general quantum state in a superposition of these possible states can be expressed as,

$$|\psi\rangle \quad = \quad \alpha_{00000\cdots0}|00000\cdots0\rangle + \alpha_{00000\cdots1}|00000\cdots1\rangle + \cdots + \alpha_{11111\cdots1}|11111\cdots1\rangle.$$

with the normalization constraint, $|\alpha_{00000\cdots0}|^2 + |\alpha_{00000\cdots1}|^2 + \cdots + |\alpha_{11111\cdots1}|^2 = 1$. There are $2^{500} \sim 10^{150}$ complex phases in this expression. Attempting to represent this amount information in a classical memory would not be possible since the are fewer than 10^{150} atoms in the entire universe! Thus a linear superposition of a reasonable number of qubits has the potential to store an immense amount of information.

Now that we have a more grounded base for qubits, we begin to discuss how we can use the nature of quantum mechanics to our advantage to do some interesting things. The field of representing two-state quantum systems and manipulating them is at the heart of the field of quantum information, which may revolutionize the future of technology.

14.2 QUANTUM CRYPTOGRAPHY

For many years many thought that the nature of the special EPR entangled pairs was only related to discrimination between local deterministic theories and the orthodox interpretation of quantum mechanics. In 1970 Wiesner proposed that quantum entangled objects might be utilized to form an almost perfectly secure means of secret transmission of messages.

The history of cryptography (the study of sending secret messages) goes back many thousand years. Unfortunately, we do not have time to explore this fascinating history but will jump ahead to more modern methods of cryptography.

Classically, modern cryptographic methods rely on two schemes, public key distribution and private key distribution. We will discuss the latter only even though the former is prominent in current computer encryption methods. Private key distribution is a very intuitive way to send a secret message. Consider two spies Alice and Bob who work together to try to foil the attempts of their counterpart Eve. To do this they must be able to send secret messages to

each other that no one else will be able to understand. Private key distribution is simply the distribution of a secret key that both Alice and Bob share. This key allows them to encode and decode any message. The specifics are not necessary but we spell out a possible method anyway. It is more convenient for them to represent their messages in binary.

Alice wishes to send an encoded message to Bob and employs the key to, say, shift each binary bit of the message if the key is 1 and leave it as is if the key is 0. Explicitly,