INTRO TO QUANTUM COMPUTING

GLENN SUN
OLGA RADKO MATH CIRCLE ADVANCED 3

MAY 9, 2021

Today we will study quantum computation through a simple example known as the CHSH game. We will explore the standard model of quantum computing and see how it can be used to do something impossible in the classical world. At the end of the worksheet, there are also a bunch of extra problems. Some extra problems don't depend on lots of other things from the handout, so feel free to try them anytime.

1 The CHSH game

The CHSH game, first introduced in 1969 by the physicists Clauser, Horne, Shimony, and Holt, is a simple game that shows how quantum mechanics can be used to obtain advantages that are just not possible in the classical world.

Definition 1 (CHSH game)**.** Alice and Bob play the following game:

1. A referee chooses $x, y \in \{0, 1\}$ uniformly at random.
2. The referee gives Alice x and Bob y.
3. Alice responds with $a \in \{0, 1\}$ and Bob responds with $b \in \{0, 1\}$.

If $x = y = 1$, then Alice and Bob win when they output different responses. Otherwise, Alice and Bob win when they output the same response.

Problem 1. Play the CHSH game a few times. Find a good strategy.

It turns out that the best strategy for Alice and Bob only succeeds with probability 75%, using classical models of computation. If you want to prove this, see Extra Problem 1 in the back of this handout. It's doable without anything else from this worksheet, so you can give it a shot right now if you want.

Amazingly, the power of quantum mechanics allows them to do better! By the end of this handout, you will see a strategy involving quantum computing that allows them to succeed with significantly higher probability. This solution has in fact been experimentally verified, and gives strong evidence for the correctness of quantum mechanics.

2 The quantum mechanical model

A *vector* is a list of numbers. Vectors of the same length can be added componentwise, and any vector can be scaled by any regular number. For example,

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{and} \quad c(a_1, a_2) = (ca_1, ca_2).$$

First, we introduce a notation for some very special vectors.

Definition 2 (basis states)**.** Let $s_1 \dots s_n \in \{0,1\}^n$ be a binary string of length n, and let $i \in \{0, \dots, 2^n - 1\}$ be the value corresponding to the binary string. We define $|s_1 \dots s_n\rangle$ to be the vector of length 2^n that is 1 in the $(i+1)$th position and 0 everywhere else. Basis states are vectors of the form $|s_1 \dots s_n\rangle$. The notation $|\cdot\rangle$ is called ket notation.

Problem 2. Check your understanding of the previous definition. In particular:

1. Compute the basis states $|0\rangle$, $|1\rangle$, $|00\rangle$, $|11\rangle$, and $|101\rangle$.
2. Explain why $(a_1, a_2, a_3, a_4) = a_1|00\rangle + a_2|01\rangle + a_3|10\rangle + a_4|11\rangle$. Can you generalize the statement to longer vectors (of length 2^n)?

Before we jump into the quantum mechanical model, we need to emphasize the distinction between physics and mathematics. Physics stipulates assumptions that state something like "our universe behaves like these mathematical objects." Often times, we later discover that certain assumptions fail to predict real-life phenomena, and in some sense the ultimate goal of physics is to uncover what the correct assumptions should be.

However, the mathematical objects in those assumptions can be defined and studied independently of any physics. They are mathematical objects from which theorems can be rigorously proven, even though we give the objects suggestive names like "quantum state." This purely mathematical perspective is the view we will adopt for now, before we come back to the physics at the end of this section.

Definition 3 (quantum state)**.** A quantum state on n qubits is a vector

$$\vec{x} = x_{0\dots0}|0\dots0\rangle + \cdots + x_{1\dots1}|1\dots1\rangle = \sum_{S\in\{0,1\}^n} x_S|S\rangle$$

where the indices go through all binary strings of length n, and $\vec{x}$ satisfies

$$|x_{0\dots0}|^2 + \cdots + |x_{1\dots1}|^2 = 1.$$

The coefficients $x_{0\dots0}, \dots, x_{1\dots1}$ are generally complex numbers, but today we will focus on the case of real numbers.

As a convention, we'll use $\vec{x}, \vec{y}$ to denote states and $\vec{a}, \vec{b}$ to denote generic vectors. The components of all vectors from now on are denoted with subscripts from $0\dots0$ to $1\dots1$.

Problem 3. Check your understanding of the previous definition. In particular:

1. Why is every basis state a quantum state?
2. How many qubits are in the state $|00\rangle$? What about $|0000\rangle$?
3. A quantum state on 1 qubit is a vector $\vec{x} = x_0|0\rangle + x_1|1\rangle = (x_0, x_1)$. Supposing x_0 and x_1 are real numbers, how can you interpret the condition that $|x_0|^2 + |x_1|^2 = 1$ geometrically in the plane?
4. Find the positive real value c that makes $c|00\rangle + c|11\rangle$ into a valid quantum state.

The purpose of a quantum state is to store information, much like a computer's memory. (The word "qubit" is also suggestive.) Although the definition is a little mysterious right now, we'll soon see why it is natural. Because memory is only useful for computation when we can change it, we describe how to change quantum states before finally stating the model.

Definition 4 (quantum gate)**.** A quantum gate on n qubits is a function f that both takes in and outputs (generic) vectors with 2^n components, satisfying the following.

1. If $\vec{x}$ is a quantum state, then $f(\vec{x})$ is a quantum state. In other words, for all vectors $\vec{x}$, if $|x_{0\ldots0}|^2 + \cdots + |x_{1\ldots1}|^2 = 1$, then $|f(\vec{x})_{0\ldots0}|^2 + \cdots + |f(\vec{x})_{1\ldots1}|^2 = 1$.
2. For all generic vectors $\vec{a}, \vec{b}$ and all regular numbers c, we have $f(\vec{a}+\vec{b}) = f(\vec{a})+f(\vec{b})$ and $f(c\vec{a}) = cf(\vec{a})$.

A function satisfying (2) is called "linear."

Although it's clear why gates must satisfy the first condition, it's not as clear why we want gates to be linear. This motivation question will be resolved by the end of this section.

Problem 4. Check your understanding of the previous definition. In particular:

1. Are the following functions quantum gates on 1 qubit? (a) $f(\vec{a}) = \vec{a}$, (b) $f(\vec{a}) = 2\vec{a}$, (c) $f(\vec{a}) = |0\rangle$, (d) $f(a_0|0\rangle + a_1|1\rangle) = a_0|00\rangle + a_1|01\rangle$.
2. In the previous problem, we talked about interpreting 1-qubit states in the plane. Informally explain why reflecting across the x-axis (or y-axis) is a quantum gate.
3. Let f be a linear function that takes in and outputs vectors of length 2. Show that $f(a_0|0\rangle + a_1|1\rangle) = a_0 f(|0\rangle) + a_1 f(|1\rangle)$. How does this generalize?
4. Recall that the composition of two functions f and g is denoted $f \circ g$, and defined as $(f \circ g)(x) = f(g(x))$ (i.e. apply g then apply f). Check that if f and g are quantum gates on the same number of qubits, then $f \circ g$ is a quantum gate.

Now, let's finally discuss a physical interpretation of these definitions! We will use electrons. Although there are many other models of quantum computing, we will focus on the concrete case of electron spin to make things easier. It is a fact that electrons have a property called spin, which is "up" or "down" in traditional physics, but we will say "0" or "1" instead.

You can roughly think of an electron as a coin. If you flip a coin, you can talk about the probabilities of it landing heads or tails, but you can't say anything else until you look at it. You can only find out the orientation after looking at it, and the same is true for electron spin. We call discovering the spin of an electron *measurement*.

Recall that definition from probability theory that two events A and B are called independent if $\Pr[A \text{ and } B] = \Pr[A]\Pr[B]$. Informally speaking, independent events "don't affect each other," and hence in the below definition, isolated systems "don't affect each other."

Definition 5 (quantum system, isolated system)**.** A quantum system is an ordered collection of electrons $E = (e_1, \ldots, e_n)$. For all binary strings $S = s_1 \ldots s_n \in \{0,1\}^n$, write $E \to S$ to denote the event of measuring the electrons in E to have spins according to S (i.e. e_i has spin s_i for all i). Then a quantum system E is said to be isolated if for all other systems E' and all binary strings S, S' of appropriate length, the events $E \to S$ and $E' \to S'$ are independent.

Problem 5. Check your understanding of the previous definition. In particular:

1. Let e_1, e_2 be electrons with probabilities given by the following table.

		e_2	
		0	1
e_1	0	0.5	0
	1	0	0.5

   Is the system $E = (e_1)$ isolated (not including e_2 inside the system)?

2. Suppose you definitely know the spin of every electron in a system $E = (e_1, \ldots, e_n)$. Must such a system be isolated?

The reason for wanting isolated systems will come soon. First, we state the model.

Axiom 1. Let E be an isolated system of n electrons and let $\vec{x}$ be an n-qubit quantum state. We say that $\vec{x}$ describes E if for all binary strings $S \in \{0,1\}^n$,

$$\Pr[E \to S] = |x_S|^2.$$

Furthermore, we say that a quantum gate f describes a physical process if whenever E is an isolated system of electrons described by $\vec{x}$, the system obtained by applying the physical process to E is described by $f(\vec{x})$.

The axiom states that every isolated system is described by some quantum state, and that every physical process is described by some quantum gate. Conversely, the axiom also states that every quantum state describes some isolated system, and every quantum gate describes some physical process.

Problem 6. Check your understanding of the previous axiom. In particular:

1. Explain why the probability distribution in the axiom is valid, i.e. probabilities are non-negative and sum to 1.
2. Let $E = (e_1, e_2)$ be a system described by the state $\vec{x} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This system is called an *EPR pair* and will actually be important to us in our CHSH game solution. Compute $\Pr[E \to S]$ for all $S \in \{00, 01, 10, 11\}$.
3. Let $E = (e_1, \dots, e_n)$ be a system whose electrons have known spin according to $S = s_1 \dots s_n \in \{0,1\}^n$. Show that E is described by $|S\rangle$.
4. What is an example of a quantum gate that describes the physical process of doing nothing? (Mini challenge problem: can you come with another example?)

As a side remark, assuming that every quantum state describes some isolated system is a bit stronger than necessary, since it turns out that for any quantum state, we can construct a system described by it through applying an appropriate physical process to a system described by $|0 \dots 0\rangle$. This idea is explored a little bit in Extra Problem 2. Also, it turns out that assuming that every quantum gate describes some physical process is also stronger than necessary. We actually only need four gates to do (almost) all quantum computation, but that is a more advanced topic.

Problem 7. Let's slightly discuss why we wanted quantum gates to be linear.

1. More than one quantum state can describe the same isolated system. Show that if $\vec{x}$ describes E, then $c\vec{x}$ also describes E for all numbers c such that $|c| = 1$.
2. Let f be a quantum gate describing a physical process. Show that if $\vec{x}$ describes E, then both $f(c\vec{x})$ and $cf(\vec{x})$ describe the result of applying the physical process to E. This motivates half the definition of linearity.

We won't motivate the other half, but linear functions in general have an amazing theory that we'll reference in the next section, and those properties turn out to be essential.

3 Tensor product

Recall that we said the EPR pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ will be very important to our CHSH game solution. Here's a very general idea of how it will work. Alice and Bob form the electrons of an EPR pair and take one electron with them each. They then perform some physical processes on their electrons and use the final measurements to know what to respond with.

There are a lot of details and motivations that need to be made clear with this. What's so special about the EPR pair that allows us to do this? How do we mathematically capture the idea of applying a physical process on just one electron, when we only know how to describe the system as a 2-qubit state? And lastly, why were we always so concerned about isolated systems? We now answer these questions.

We'll follow the same approach as before of mathematically defining the concept first, thinking about it rigorously, then discussing how it is used in quantum computing. Tensor product is really cool! If you learned in school that you "can't" multiply vectors to get another vector, or that it's only possible in 3 dimensions, it turns out you actually can!

Definition 6 (tensor product of vectors)**.** Let $\vec{a} = (a_1, \dots, a_n)$ and $\vec{b} = (b_1, \dots, b_m)$ be vectors. The tensor product of $\vec{a}$ and $\vec{b}$ is the vector $\vec{a} \otimes \vec{b}$ of length nm, defined as the concatenation of $a_1\vec{b}, \dots, a_n\vec{b}$, that is, $(a_1b_1, a_1b_2, \dots, a_nb_{n-1}, a_nb_n)$.

Problem 8. Check your understanding of the previous definition. In particular:

1. Prove that for $s_1, s_2 \in \{0, 1\}$, we have $|s_1\rangle \otimes |s_2\rangle = |s_1s_2\rangle$. Generalize the claim.
2. Is tensor product of vectors commutative? Can you pull out constants, i.e. does $(c_1\vec{a}) \otimes (c_2\vec{b}) = c_1c_2(\vec{a} \otimes \vec{b})$?
3. Verify the distributive property for tensor product. That is,
$$(a_1|0\rangle + a_2|1\rangle) \otimes (b_1|0\rangle + b_2|1\rangle) = a_1b_1|00\rangle + a_1b_2|01\rangle + a_2b_1|10\rangle + a_2b_2|11\rangle.$$
This is the reason we have been insisting on writing $a_0|0\rangle + a_1|1\rangle$ instead of (a_0, a_1). It makes computing with tensor product extremely natural.
4. Check that if $\vec{x}$ and $\vec{y}$ are 1-qubit states, then $\vec{x} \otimes \vec{y}$ is a 2-qubit state. How about if $\vec{x}$ has n qubits and $\vec{y}$ has m qubits? (Hint: for regular numbers a, b, we have $|ab| = |a||b|$. Factor parts of the equation.)
5. Let $\vec{x}$ and $\vec{y}$ be n-qubit states and let $S_1, S_2 \in \{0, 1\}^n$ be binary strings. If S_1S_2 denotes the concatenation of the binary strings, what is $(\vec{x} \otimes \vec{y})_{S_1S_2}$?

Now, here's the physical interpretation of tensor product. Intuitively, the tensor product is the tool used to consider two systems as one.

Theorem 1. Let E_1 and E_2 be isolated systems described by $\vec{x}$ and $\vec{y}$ respectively. Then $\vec{x} \otimes \vec{y}$ describes the concatenation E_1E_2.

Problem 9. Prove Theorem 1. (Hint: Just check the definition of "describes"! The key is that the systems are isolated.)

The theorem reveals a very tight connection between systems being isolated and the tensor product. Let us explore this relationship a little further.

Problem 10. A quantum state is called *entangled* if it cannot be written as the tensor product of smaller states. Show that the EPR pair $\vec{x} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is entangled. (Hint: Assume for contradiction that we can factor it and equate coefficients of corresponding terms.) What does entanglement mean physically? (Hint: Problem 5.1.)

Next, we extend the notion of tensor product to functions. That is, how do we mathematically capture the idea of applying physical processes to subsystems of electrons?

Definition 7 (tensor product of linear functions)**.** Let f be a linear function that takes in and outputs vectors of length n, and let g be a linear function that takes in and outputs vectors of length m. Then the tensor product of f and g, denoted $f \otimes g$, is the unique linear function that takes in and outputs vectors of length nm and satisfies

$$(f \otimes g)(\vec{a} \otimes \vec{b}) = f(\vec{a}) \otimes g(\vec{b})$$

for all $\vec{a}$ of length n and $\vec{b}$ of length m.

Before proceeding with some understanding check questions, there's something that needs to be said here. This definition needs a proof! In particular, why does there exist a function satisfying that equation, and why should it be unique? This takes a bit of linear algebra to show, but is quite reasonable, so it is Extra Problem 3. For the rest of the worksheet, all you need to remember is the formula: apply component functions to component vectors.

Problem 11. Check your understanding of the previous definition. In particular:

1. Calculate $(f \otimes g)(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle)$, where $f(\vec{a}) = \vec{a}$ and g is the reflection across the x-axis. (Hint: apply linearity first!)
2. Let f and g both be the identity function on vectors of length 2, i.e. $f(\vec{a}) = \vec{a}$ and $g(\vec{a}) = \vec{a}$. Show that $f \otimes g$ is the identity function on vectors of length 4.

Since we proved that the tensor product of states is a state, we would like to prove that the tensor product of gates is a gate. Again, this proof requires linear algebra, and in fact it requires quite a bit, so just take it as a fact or a very challenging extra problem.

Last but not least, the long awaited physical interpretation, which is exactly as you expect. However, we must take it as an axiom, not a theorem, for reasons that you will explore in the following problem.

Axiom 2. Let f_1 and f_2 be quantum gates describing two physical processes. Then $f_1 \otimes f_2$ is a quantum gate that describes taking an isolated system $E = E_1E_2$ and applying the first physical process to E_1 and the second physical process to E_2.

Problem 12.

1. Prove the axiom (i.e. it's a theorem) when the subsystems E_1 and E_2 are isolated. (Note: if E_1 and E_2 are isolated, it's a physical fact that they remain isolated after applying processes that only involve the systems separately. Again, just verify the definition using Theorem 1.)
2. In general, E_1 and E_2 may not be isolated (i.e. Problem 10). Can you give some intuition for why we are forced to take the claim as an axiom?

4 Solution to the CHSH game

Finally, we have the tools we need to develop a solution for the CHSH game! Here's one quick preliminary that we'll need.

Problem 13. The function R_θ, known as the rotation function by angle θ, is defined by

$$R_\theta(a_1|0\rangle + a_2|1\rangle) = (a_1\cos(\theta) - a_2\sin(\theta))|0\rangle + (a_1\sin(\theta) + a_2\cos(\theta))|1\rangle.$$

1. Show that R_θ is a quantum gate on 1 qubit.
2. Explain geometrically why R_θ rotates a vector $(a_1, a_2) = a_1|0\rangle + a_2|1\rangle$ counter-clockwise around the origin by θ.

And now for the solution. Recall that Alice and Bob want to output the same value if either receives 0, and they want to output different values if they both receive 1.

Problem 14. Suppose Alice and Bob form the electrons of an EPR pair (i.e. corresponding to $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$), Alice takes the first electron, and Bob takes the second.

1. Suppose Alice and Bob just measure their own electron and output the spin they measured, without applying any physical processes. Explain why in the case Alice receives $x = 0$ and Bob receives $y = 0$, this strategy works. In which cases does this strategy not work well?

The idea is that when Alice or Bob receive 1, they rotate their own electron away from the original state, so that their measurements have a chance to differ. In particular, Alice applies $R_{\pi/8}$ if she gets $x = 1$ and Bob applies $R_{-\pi/8}$ if he gets $y = 1$. If someone gets 0, that person does nothing. They agree to wait a period of time before measuring, to make sure that both have time to finish their process.

2. Suppose $x = 1$ and $y = 0$ or vice versa. Using Axiom 2, how do you describe the resulting state of the electrons? Now compute the resulting state and its associated probability distribution upon measurement to show that Alice and Bob win with probability $\cos^2(\pi/8) \approx 85\%$.
3. Now suppose $x = y = 1$. With similar logic, show that they win with probability 50%. You will need the trigonometric identity $\cos^2(\theta) - \sin^2(\theta) = 2\sin(\theta)\cos(\theta)$. Why doesn't it matter who applied their rotation first?
4. Conclude that Alice and Bob win with probability about 80% overall.

Congratulations! You've reached the end of this worksheet. Extra Problem 4 asks you to improve this solution to get 85% accuracy and prove that 85% is best possible.

If you are interested to learn more about this quantum computing, a good modern resource is the Qiskit textbook. Qiskit is a Python library for simulating quantum algorithms, though the online textbook is a general introduction to quantum computing, not just their library. Here it is: https://qiskit.org/textbook/preface.html

5 Extra Problems

1. In this extra problem, we prove classical lower bounds on the CHSH game.

   (a) A classical deterministic strategy for Alice and Bob is a pair of functions $A, B : \{0,1\} \to \{0,1\}$, meaning that they each output 0 or 1 depending on whether they get 0 or 1 as input. Prove that 75% accuracy is optimal for such strategies.

   (b) A randomized strategy is a strategy where Alice and Bob may flip coins and make random decisions based on the coins and inputs they get. For example, when Alice receives $x = 0$, she could output 0 with probability 60% and 1 with probability 40%, and maybe use other probabilities when she receives $x = 1$. Prove that randomization does not help Alice and Bob, i.e. any randomized strategy also succeeds with probability at most 75%.

2. In this extra problem, we will investigate how to construct an EPR pair from scratch, assuming that certain fundamental quantum gates are constructible. The gates that we use will be the Hadamard gate and the CNOT gate. By the way, together with the phase gate and Toffoli gate (not shown), these form the four gates commonly used to perform all quantum computation.

   (a) Show that the Hadamard gate, defined by

   $$H(x_1|0\rangle + x_2|1\rangle) = \tfrac{1}{\sqrt{2}}((x_1 + x_2)|0\rangle + (x_1 - x_2)|1\rangle)$$

   is a valid 1-qubit gate.

   (b) Show that the CNOT (controlled-not) gate, defined by

   $$C(x_1|00\rangle + x_2|01\rangle + x_3|10\rangle + x_4|11\rangle) = x_1|00\rangle + x_2|01\rangle + x_4|10\rangle + x_3|11\rangle$$

   is a valid 2-qubit gate. Explain why it is called the controlled not gate.

   (c) Use the Hadamard gate and the CNOT gate to create a gate that sends $|00\rangle$ to $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Since $|00\rangle$ can be physically constructed by just looking at a bunch of electrons until we find two that are spin up, this gives a method to construct $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, supposing that the Hadamard and CNOT gates are actually constructible.

3. In this extra problem, we prove the existence and uniqueness of tensor product of linear functions, and that the tensor product of gates is a gate. Welcome to linear algebra! First, a matrix is a grid of numbers. For us, the grid will always be a square, but they can be rectangles in general. A matrix $[f]$ can be multiplied by a vector $\vec{a}$ to produce a vector $[f]\vec{a}$ as follows:

$$\begin{bmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,n} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n,1} & f_{n,2} & \cdots & f_{n,n} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} f_{1,1}a_1 + f_{1,2}a_2 + \cdots + f_{1,n}a_n \\ f_{2,1}a_1 + f_{2,2}a_2 + \cdots + f_{1,n}a_n \\ \vdots \\ f_{n,1}a_1 + f_{n,2}a_2 + \cdots + f_{n,n}a_n \end{bmatrix}$$

For notational convenience, let $\vec{e}_1, \ldots, \vec{e}_n$ denote the basis states $|0\ldots0\rangle, \ldots, |1\ldots1\rangle$ (binary strings of length $\log_2 n$).

(a) Let $[f]$ be a matrix. Show that the ith column of $[f]$ is exactly $[f]\vec{e}_i$.

(b) Let f be a linear function and define the matrix $[f]$ by taking the ith column to be $f(\vec{e}_i)$. Show that $[f]\vec{a} = f(\vec{a})$ for all vectors $\vec{a}$.

(c) Using the previous two parts, conclude that every linear function can be represented by a matrix, and that this representation is unique.

(d) Let f and g be linear functions. Recall we want to find a linear function $f \otimes g$ such that $(f \otimes g)(\vec{a} \otimes \vec{b}) = f(\vec{a}) \otimes g(\vec{b})$ for all $\vec{a}$ and $\vec{b}$. Using Extra Problem 3(c), translate this goal into a statement about matrices.

(e) Construct a matrix $[f \otimes g]$ in a way similar to Extra Problem 3(b) and show that it satisfies your goal. Explain why it is unique.

4. In this extra problem, we will improve the CHSH solution presented in the main handout, and show that this improved solution is essentially the best possible.

   (a) By trying slightly different rotations, improve the strategy for the CHSH game to one that gives a 85% probability of success.

   (b) Show that no matter how Alice and Bob rotate their electrons, 85% is the optimal probability of success.

   (It turns out that this is the optimal success probability for all quantum algorithms, not just rotations, but that is much harder to prove.)