REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 16, 2004	Final Progress Report 8/1/1998 - 3/31/2004

4. TITLE AND SUBTITLE
Quantum Computing Algorithms

5. FUNDING NUMBERS
Contract No. DAAG55-98-C-0040

6. AUTHOR(S)
Dr. Lov Grover

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Bell Laboratories, Lucent Technologies
600 Mountain Ave, Murray Hill, NJ 07974

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
38812.19-PH-QC

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This is the final progress report submission of Dr. Lov Grover's Quantum Computing Algorithms study.

14. SUBJECT TERMS

15. NUMBER OF PAGES
53

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev.2-89)
Prescribed by ANSI Std. 239-18
298-102

Quantum Searching & Related Algorithms

Lov K. Grover *
lkgrover@bell-labs.com
Bell Laboratories, Lucent Technologies,
600-700 Mountain Avenue, Murray Hill, NJ 07974

Contents

*Research was partly supported by NSA & ARO under contract DAAG55-98-C-0040.

1 Foreword

In 1994 when Peter Shor discovered his factorization algorithm, it was generally believed that now that there was a better understanding of quantum algorithms, more would be quickly discovered and the field would soon reach the kind of maturity that we associate with the field of (classical) randomized algorithms, for example. These hopes were bolstered when I discovered the search algorithm in 1996, especially when it was followed by the discovery of the amplitude amplification principle in 1998 which gave a general framework for the design of quantum algorithms. This was the background in which I wrote my original proposal in 1998.

The reality over the last few years has been sobering. Despite considerable research, it is still the belief that there are only two general quantum algorithms where quantum mechanics gives an advantage over classical - the factorization algorithm and the search algorithm. The factorization algorithm has continued to be a standalone algorithm (though a very important one), searching is a much simpler framework and through the amplitude amplification principle, it is easily adapted to different problems - it has resulted in numerous applications and variations.

There has been considerable research on extensions & modifications of quantum search. The amplitude amplification generalization of 1998 showed that in the quantum search algorithm, almost any unitary operation could replace the Walsh-Hadamard (W-H) transformation with only a constant slowdown. At first sight this seemed remarkable since the W-H transform was known to be singularly significant for other algorithms such as Simon's algorithm and Deutsch & Deutsch-Jozsa algorithms. This was explained by interpreting the algorithm as a simple rotation in two dimensional Hilbert space where these two dimensions are carefully defined vectors in the two-dimensional plane of rotation. With this definition, what the algorithm accomplishes is a gradual rotation from the vector corresponding to the initial state to the vector corresponding to the target state. This rotation is accomplished by two inversions about slightly non-orthogonal directions - it is an elementary theorem of Euclidean geometry that two inversions about non-orthogonal axes in a plane, lead to a well-defined rotation of any vector in the plane. This generalization and understanding considerably broadened the scope of application of the search algorithm. From a physical implementation point of view, it showed that there was a lot of leeway in choosing the driving transformation in quantum search, thus reducing the need for error-correction. From a computer science standpoint, it resulted in a lot of new algorithms since the main driving transformation could be chosen depending on the parameters of the problem.

There has been considerable research on these topics. A quick search of the quant-ph archives for relevant articles resulted in 241 hits. Some examples:

1. A framework for fast quantum mechanical algorithms, Lov K. Grover, quant-ph/9711043, STOC '98.

2. Quantum counting, Gilles Brassard, Peter Hoyer, Alain Tapp, quant-

ph/9805082.

3. The quantum query complexity of approximating the median and related statistics, Ashwin Nayak, Felix Wu, STOC, 1999, quant-ph/9804066.

4. Fast quantum algorithms for numerical integrals and stochastic processes, Daniel S. Abrams, Colin P. Williams, quant-ph/9908083.

5. Searching in Grover's Algorithm, Richard Jozsa, quant-ph/9901021.

6. Spectra of Quantized Walks and a $\sqrt{\delta\epsilon}$ rule, quant-ph/0401053, Mario Szegedy.

7. Grover's Quantum Search Algorithm for an Arbitrary Initial Mixed State, quant-ph/0306183, Eli Biham, Dan Kenigsberg.

8. Quantum Search of Spatial Regions, quant-ph/0303041, Scott Aaronson, Andris Ambainis.

9. Quantum Algorithms for Lowest Weight Paths and Spanning Trees in Complete Graphs, quant-ph/0303131, Mark Heiligman.

10. Tradeoffs in the Quantum Search Algorithm, quant-ph/0201152, Lov K. Grover.

11. Similarity between Grover's quantum search algorithm and classical two-body collisions, Jingfu Zhang, Zhiheng Lu, quant-ph/0110077.

12. Quantum walk algorithm for element distinctness, Andris Ambainis, quant-ph/0311001.

The list goes on and on.

One idea that was *not* motivated by the search algorithm was the one that appeared in the following paper: "Strengths and Weaknesses of Quantum Computing," SIAM Journal of Computing, 26[5]: 1510-1523, 1997, quant-ph/9701001. The authors were: Charles H. Bennett, Ethan Bernstein, Gilles Brassard & Umesh Vazirani [BBBV]. Even though this paper was published much later, the authors had realized as early as 1995 (a year before the search algorithm came out) that there was a fundamental limit to how far quantum parallelism could take us. In fact they proved that no algorithm could hope to search an unsorted database in fewer than $\Omega\left(\sqrt{N}\right)$ queries. They had given a lower bound that was precisely matched by my algorithm. [BBBV] was a truly remarkable result - a rare instance when a non-intuitive lower bound for a fundamental problem had come even before the algorithm. Most significantly it has convincingly held firm for the last ten years despite several efforts to find ways around it. Partly as a consequence of this result, no polynomial time algorithm has been discovered for any of the NP-complete problems. I say partly because as elaborated in the next paragraph, there is still some hope.

When quantum computing was first being invented, it was hoped that it would be able to solve NP-complete problems just through the *parallelism* of quantum mechanics. Such a scheme would do a brute force search and would not need to use any of the structure of these problems. These hopes were dashed in 1995 by the [BBBV] paper, this proved that the best improvement that such an unstructured search scheme could provide was a square-root speedup. Based on this result, it is often said that quantum computing algorithms could *not* possibly solve NP-complete problems. However, it should be emphasized that this is only true if we look at the NP-complete problem as an exhaustive search problem. NP-complete problems have considerable structure and there well might be other more advantageous ways of looking at them. The science of quantum computation is relatively new and there are several unexplored directions. As described in the interim reports and briefly in this report, we have spent some time exploring novel algorithms that make use of the power of quantum mechanics to take advantage of the structured nature of these problems.

This report describes the research that I and my collaborators have conducted at Bell Labs over the last five years. The report is organized as follows:

1. The next chapter describes research into quantum algorithms.
2. Chapter three describes research into quantum communication (some aspects of quantum communication are covered in the algorithms chapter, e.g. distributed computing).
3. Chapter four describes research into physical implementations.

2 Quantum Algorithms

There were two broad themes to our research in quantum algorithms:

1. Quantum searching and variants.
2. Algorithms for NP-complete problems.

The first theme built on the previous discovery of the quantum search algorithm [1]. This algorithm has proven to be remarkably versatile. Originally designed for unstructured searching, it has adapted surprisingly well to structured problems - the foreword mentions some applications [4],[6]. This chapter mentions some more extensions of quantum searching. The second theme was speculative, nevertheless, we undertook it as a worthwhile challenge. Research in both of these topics continues in the second (ongoing) phase of the program.

2.1 Quantum Searching and Variants

The search algorithm showed how to make use of the fact that a quantum system could simultaneously be in multiple states, to search an unsorted database of size N in only $O\left(\sqrt{N}\right)$ steps. The quantum search algorithm is perhaps the simplest possible quantum algorithm and because of its simplicity and power it attracted considerable interest from both physicists and computer scientists.

1. Physicists were interested because finally there was a simple scheme that would clearly demonstrate the power of quantum computing. So far there have been only two significant applications where quantum computing gives an advantage over classical computing - factorization and search. Unlike factorization, in searching there was minimal effort required to set up the system. As the NMR groups have shown, a demonstration can be done even on a two qubit system.
2. Computer scientists are intrigued by this algorithm because it had generally been assumed that in order to achieve any speedup one needed to make use of the structure of the problem - this is generally true in both deterministic and probabilistic algorithms, the quantum search algorithm showed that this clearly was not the case in quantum mechanical algorithms.
3. With the factorization algorithm, no one knows whether or not there exists a better classical or quantum algorithm. Last year there was a breakthrough in a related field when an Indian group discovered a deterministic algorithm for primality testing. In case there is another breakthrough by means of which it becomes possible to (classically) factorize numbers in logarithmic time, interest in the quantum algorithm would quickly vanish. That cannot happen with the search algorithm. It has been proved

that no algorithm, whether quantum or classical, can ever hope to beat quantum search for the application of exhaustive searching [3].

4. Finally there is the issue that searching is an application that existing computers actually spend a substantial portion of their CPU cycles in. Factorization, though a very important application from a fundamental standpoint, is probably not going to be of much significance if quantum computers ever become commonplace [5].

2.1.1 Classical Analog

We show that the quantum search algorithm can be described as a resonance phenomenon [8]. This opens the scope for implementing the algorithm using other possible architectures. We suggest one implementation based on coupled oscillators in a purely classical setting when there are N oscillators, one of which is of a different resonant frequency. We could identify which one this is by measuring the oscillation frequency of each oscillator, a procedure that would take about N cycles. We show, how by coupling the oscillators together in a very simple way, it is possible to identify the different one in only $\sqrt{N}$ cycles. Although there have been other classical analogs, they have just copied the original search algorithm, ours brings out the basic physics of the algorithm and suggests new applications and interpretations. For example, this yields a simple explanation for the $\sqrt{N}$ bound.

The quantum search algorithm has been rigorously proved to be the best possible algorithm for exhaustive search, i.e. no other algorithm can carry out an exhaustive search of N items in fewer than $O(\sqrt{N})$ steps [3]. The proof for this is complicated and based on subtle properties of unitary transformations. Fortunately, in the classical analog, there is a simple argument as to why it needs $O(\sqrt{N})$ cycles.

2.1.2 Scheduling Problem

The scheduling problem consists of finding a common 1 in two remotely located N bit strings (in case a 1 denoted an available slot for each party, a solution to this problem could be used for *scheduling* a meeting between the two - hence its name). The challenge is to solve this problem with the fewest possible bit-communication. It has been known for several decades that it is not possible to solve this classically with fewer than N bits of communication. In 1996, Buhrman, Cleve & Wigderson [19] were able to apply a version of the quantum search algorithm to solve this problem with only $O(\sqrt{N}\log_2 N)$ qubits of communication. We have discovered a new algorithm that works as well as or better than any known algorithm especially when one of the strings is sparse (i.e. it has only a few 1s).

Denote the number of 1s in the string with the fewer 1s by ϵN. Classically, it needs at least $O(\epsilon N \log_2 N)$ bits of communication to find the common 1. The best known quantum algorithm would require $O(\sqrt{N})$ qubits of communication [13], [11] - it is not obvious how to modify this to take advantage of the sparsity

of the strings. We designed a quantum algorithm to find the common 1 with only $O(\sqrt{\epsilon N}\log_2 N)$ qubits of communication using the amplitude amplification principle (an extension of quantum searching) [9].

2.1.3 Trade-offs in the Quantum Search Algorithm

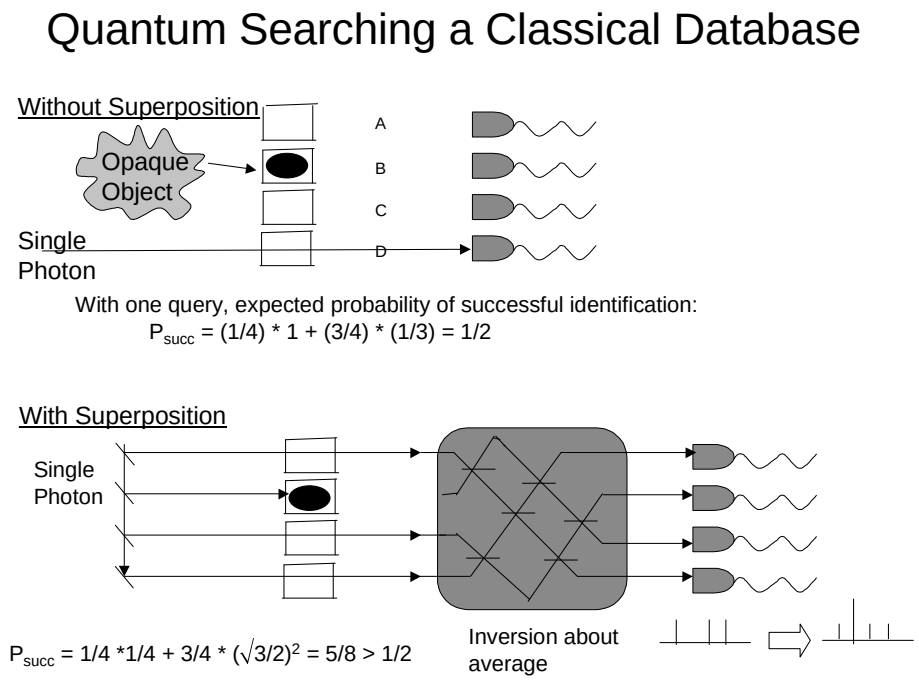
Quantum search is a quantum mechanical technique for searching N possibilities in only $\sqrt{N}$ steps. This has been proved to be the best possible algorithm for the exhaustive search problem in the sense the number of queries it requires cannot be reduced. However, as shown in [10] , the number of non-query operations, and thus the total number of operations, *can* indeed be reduced. The number of non-query unitary operations can be reduced by a factor of $\log N/\alpha \log(\log N)$ while increasing the number of queries by a factor of only $(1 + (\log N)^{-\alpha})$. Various choices of α yield different variants of the algorithm. For example, by choosing α to be $O(\log N/\log(\log N))$, the number of non-query unitary operations can be reduced by a third without a single increase in the number of queries.

2.1.4 Quantum searching for classical objects

It is inevitable that classical computers will have to deal with quantum effects; this is normally perceived as an obstacle. However we believe that some of the earliest uses of results from quantum information processing will be in small but useful applications of quantum effects within a classical computer.

The quantum search algorithm was originally phrased in terms of searching an unsorted database for a marked item. Clearly such a database would have to be a "specially constructed quantum" database, and could not be a "regular classical" database. As such the search algorithm is usually thought in terms of querying a (specially constructed) quantum oracle. We have recently shown how to perform a quantum search for a classical object, specifically for a classical object which performs no coherent evolution on the quantum computer being used for the search [20].

The simplest example of such a hybrid quantum/classical process can be understood by considering the case where an opaque object is used to mark one of N different objects, and we are limited to only a single query. Classically the probability of correctly identifying the marked item is $1/N$. However, using appropriate beamsplitters we can place a photon in a superposition of paths corresponding to all N items. In this way the photon queries all items simultaneously. Another array of beamsplitters can then be used to perform an inversion about average operation on the photon paths - it is not difficult to show that our probability of success is now boosted to about $4/N$ in the limit of large N. The following figure gives a detailed calculation of the success probability after a single query to a 4 item database, here too it gives a constant factor improvement over the best possible scheme. As mentioned earlier the loss of the photon due to probing the opaque object limits the success probability.



We have extended this simple one query example, by using interaction free measurement as a subroutine in the quantum search algorithm. This is necessary, because absorptive loss causes the naive one query procedure discussed above to become extremely inefficient after several iterations.

In addition to providing a simple example of how non-unitary processes which approximate unitary ones can be useful in a quantum algorithm, our procedure requires only one photon regardless of the size of the database, thereby establishing an upper bound on the amount of energy required to search an arbitrarily large database. Alternatively, our result can be interpreted as showing how to perform an interaction free measurement with a single photon on an arbitrarily large number of possible bomb positions simultaneously. The improvement we have obtained is only by a constant factor - despite much effort we have not been able to improve this to a square-root factor (the difference from the standard search algorithm is that there are losses at every step of the classical observation which reduces the amplitudes in all states that give any meaningful information).

2.1.5 Distributed computation

Classical communication and computation have been intricately linked since the time of Shannon. It is well known that appropriate coding can greatly facilitate the transmission of data. Similarly, distributing computation among

multiple computers can expedite the solution of certain problems for which the communication needs do not dominate. A similar situation prevails in the quantum world. Quantum teleportation and quantum cryptography all make use of the same concepts and framework as quantum computation. Indeed the quantum technique that gives the best known improvement in communication complexity as compared to classical, consists of an application of the quantum search algorithm in a distributed setting to solve the intersection problem.

Terry Rudolph and I worked intensely in this area of quantum communication complexity for several months. We have been trying to see what classical computations can be carried out in a distributed setting using entanglement. In particular our studies have focused on understanding the (entanglement assisted) communication complexity for arbitrary functions, rather than focussing on specific examples of functions as previous research has done.

Our investigations along these lines have led us into considering a generalization of a problem which has received much attention already, namely the minimal communication requirements (quantum or classical) under which a given entangled state can be transformed into another given state. The generalization we have been investigating, and hope to investigate further, arises when Alice and Bob hold one a set of entangled states (but they don't know which) and they wish to apply some transformation to a different set of entangled states.

To see how this question arises, assume that Alice and Bob initially share a resource of entangled states. They also each have some data, x_A or x_B and wish to compute $f(x_A, x_B)$. If they each perform some local operations which depend on their input data, we see that they now hold one of a set of possible entangled states - although they do not know which one. Their goal is to perform operations, with as little classical communication as possible, which result in a different entangled state. This final entangled state we generally envisage being such that one of the parties can tell, from local measurements, what the output $f(x_A, x_B)$ is.

We have begun our investigation into this general question, by looking at the case where Alice and Bob share either the entangled state $|\psi_0\rangle$ or $|\psi_1\rangle$. They wish to effect the transformation

$$\begin{aligned} |\psi_0\rangle &\rightarrow |\phi_0\rangle, \\ |\psi_1\rangle &\rightarrow |\phi_1\rangle, \end{aligned}$$

utilizing as little classical communication as possible. It is well known that if there were only a single state $|\psi\rangle$ which they wished to transform into $|\phi\rangle$, then they can do so with no communication if the two states have the same amount of entanglement. In our only slightly more complex generalization however, no such simple rules are evident. For example, there exists pairs of initial states $|\psi_0\rangle$, $|\psi_1\rangle$ which are orthogonal and have the same amount of entanglement, and corresponding pairs $|\phi_0\rangle$, $|\phi_1\rangle$ of final states which are also orthogonal and which have the same entanglement as the initial states, for which the desired transformation is not (deterministically) possible with no communication.

We have also made the following rather curious observation, which is a special

case of the above but for which we are yet to find a concrete application. Imagine that Alice and Bob have an unlimited resource of EPR pairs, and that they use the states $|0_L\rangle = |00\rangle + |11\rangle$ ($|1_L\rangle = |00\rangle - |11\rangle$) to encode a logical zero (one). Note that each of them can set the value of any qubit in the logical basis by a local operation, no communication is required. We have found that on a series of N such encoded logical qubits, Alice and Bob can perform an inversion about average operation (in the logical basis), without *any* communication. They do so by performing a phase inversion on the state with all 0's in the local basis (either party can perform this phase inversion. This result seems to indicate that some form of extended party quantum searching might be possible, we plan to work out the specific communication requirements for this.

2.1.6 How significant are the known collision and element distinctness quantum algorithms?

Quantum search is a technique for searching N possibilities for a desired target in $O(\sqrt{N})$ steps. It has been applied in the design of quantum algorithms for several structured problems through the amplitude amplification principle. Many of these algorithms require significant amount of quantum hardware. In this paper we propose the criterion that an algorithm which requires $O(P)$ hardware should be considered significant if it produces a speedup of better than $O\left(\sqrt{P}\right)$ over a simple quantum search algorithm (ignoring logarithmic factors)[7]. This is because a speedup of $O\left(\sqrt{P}\right)$ can be trivially obtained by dividing the search space into $O(P)$ separate parts and handing the problem to independent processors that do a quantum search. Our paper points out the surprising and previously unobserved fact that: all three known algorithms for collision and element distinctness [12], [14], [16] exactly saturate the criterion.

2.1.7 Using incoherent ancillas

We have recently noticed that a modified quantum search algorithm works almost the same as the original algorithm if the phase inversion step is replaced by a counting step in which a quantum device counts how many times the system has passed through the solution state. The advantage with such a structure is that it does not need to maintain phase matching with the rest of the structure. In fact, we have found using density matrix calculations that the algorithm still works even if the counter is not totally coherent.

We also find that this version of the search algorithm, while requiring an increase in the number of oracle queries (by only a constant factor) is much more stable with respect to overshooting/undershooting the optimal number of queries. We are still thinking of applications where this observation would give a decisive advantage over the standard search algorithm.

2.1.8 Quantum algorithm for detecting collisions in invertible functions

Resources required by quantum information systems are quite different from those required by classical systems. For example, entanglement is a major resource for quantum information processing; it is well known that for classical communication systems, no initialization made prior to transmission can augment the transmission capacity of a channel. In contrast, through superdense coding, it is possible to boost the transmission capacity of a quantum channel by a factor of two if the two parties share prior entanglement.

In this paper we give an instance in computation where a particular feature of a problem (partial invertibility of the given function) does not contribute any benefit if we were solving the problem on a classical computer, whereas on a quantum computer it gives an improvement over the best known algorithm. In fact, we are able to obtain provably the best possible collision detection quantum algorithm.

2.1.9 From Schrodinger's equation to the quantum search algorithm

The quantum search algorithm is a technique for searching a space of size N in only $O\left(\sqrt{N}\right)$ steps. Although the algorithm itself is widely known, not so well known is the series of steps that first led to it, which are quite different from any of the generally known forms of the algorithm (e.g. inversion about average, two dimensional rotation in Hilbert space). The quantum search algorithm was first invented as a discretized version of Schrodinger's equation [17]. I have found the insights that led to this algorithm very helpful in the design of other quantum algorithms, e.g. the algorithms described in: "A framework for fast quantum mechanical algorithms," Lov K. Grover, quant-ph/9711043, STOC '98.

I presented an outline of the original derivation to a small gathering of theoretical physicists in the Winter Institute on the Foundations of Quantum Theory, SN Bose Center, Calcutta, India in Jan. 2000. After seeing the interest it inspired, I decided to write a more complete version, not so much for historical reasons but with the view of providing a self-contained introduction to quantum computing algorithms from a different perspective. It has proved unexpectedly difficult to design fast quantum computing algorithms, a new perspective would help in this direction.

2.2 Quantum algorithms for NP-complete problems

We investigated how efficiently we could create superpositions that provide information about the solution of computer science problems more effectively than classical probabilistic algorithms. The quantum search algorithm has been shown to be applicable to the synthesis of general superpositions (and hence classical distributions), however it only gives a square-root advantage over classical methods. It remains to be seen what kinds of advantage it gives for structured superpositions. To give an indication of the breadth of possibilities, we mention

three approaches we have been investigating (several hundred such approaches have been tried):

Log-concave superpositions It is well known how to classically sample according to log-concave distributions (i.e. probability distributions whose logarithm is a concave function). Unfortunately, it is not known how to specify an NP-complete problem as that of sampling a log-concave distribution. Any obvious representation seems to require at least some log-convexity. We have been able to represent these problems as that of sampling slightly log-convex distributions, i.e. distributions that are slightly non-log-concave at certain well-defined points in certain well defined directions - everywhere else they are log-concave. This is accomplished by increasing the number of variables in the problem by a polynomial factor and having the log-convexity in each of the variables (I invented this technique independently, very recently I came to know that similar ideas are known in management science under the name "latent variables").
We have recently discovered ways of synthesizing quantum superpositions corresponding to log-concave distributions (quant-ph/0208112). Also, we have been able to prove that the magnitudes of the Fourier Transforms of superpositions that correspond to NP-complete problems are log-concave. All that remains is to estimate the phase of an arbitrarily specified state of this superposition. If we can somehow calculate this, we can rotate the phase of each state appropriately and then Fourier Transform back to get the original superposition.

Diffusion based algorithms The idea of generating a log-concave superposition, described in the previous paragraph, has led us to a related class of algorithms that make use of quantum mechanical principles, but can be implemented totally classically. The idea is that if we consider the overlap integral of two quantum mechanical states, it stays invariant under any unitary operation that is applied to both states. E.g. consider $\langle\phi|\psi\rangle$, assuming ϕ and ψ to be real, this is $\int \phi\psi$. We know that the overlap integral is invariant under a unitary transformation which transforms both ϕ as well as ψ in opposite directions, i.e. if U is an arbitrary unitary transformation, then $\int \left(U^{\dagger}\phi\right)\ (U\psi)$ is equal to $\int \phi\psi$. In particular if we let U be the $\left(1+i\epsilon\nabla^2\right)$ operation, which is unitary when ϵ is real and $\epsilon \to 0$, it follows that $\int \phi\psi = \int \left(\phi - \epsilon\nabla^2\phi\right)\left(\psi + \epsilon\nabla^2\psi\right)$. Therefore the integral of the product of two functions stays the same if one diffuses forward and the other backward in time. Note that this diffusion is completely classical. This simple result has led us to a whole class of possible algorithms described in the following subsections.
It is possible to represent a distribution whose integral yields the solution to NP-complete problems, say $f(\bar{x})$, as a product of two simple distributions $f_1(\bar{x},0)$ & $f_2(\bar{x},0)$, the integral is invariant when f_1 diffuses backward in time and f_2 diffuses forward in time by the argument of the previous paragraph. The shape of $f_1(\bar{x},0)$ is critical because it is diffusing backward

in time. Functions diffusing forward in time get smoothed out, functions when they diffuse backwards in time become more sharply peaked. The shape of $f_1(\bar{x}, t)$ can become very messy if we are not careful about the initial choice of the function (i.e. $f_1(\bar{x}, 0)$). To simplify f_1, we choose it in a way so that it is a bounded function of a small number of variables which is log-convex at some point in some direction. This is independent of the problem. The problem specific portion, $f_2(\bar{x}, 0)$, which is a joint function of several variables, can be chosen to be completely log-concave.

Multiplying through Convolution As pointed out in the previous paragraph, if we can sample a product of two distributions, we can obtain distributions that can give the solution of NP-complete problems. Consider the problem of multiplying two functions $f_1(x)$ & $f_2(x)$. If one can convolve the two and then take the Fourier transform of the product, one can get a function corresponding to the product of the two functions. Unfortunately, it is non-trivial to create a quantum superposition corresponding to to the convolution of two given quantum superpositions, this is unlike probability distributions where if we are given two probability distributions, one just has to shift one distribution by the other to obtain the distribution corresponding to the convolution. The reason for this difficulty lies in the fact that it is not easy to shift one superposition by another.

- In order to see the difficulty, consider two quantum superpositions ψ_1 & ψ_2 in the initial state: $\psi_1(x_1)|x_1\rangle \otimes \psi_2(x_2)|x_2\rangle$.
- Shift the second by the first $\psi_1(x_1)|x_1\rangle \otimes \psi_2(x_2)|x_2 - x_1\rangle$.
- Fourier transform in second register, this gives $\psi_1(x_1)|x_1\rangle \otimes \phi_2(k_2)|k_2\rangle \exp(ik_2x_1)$. Notice that if the first register did not have the $|x_1\rangle$ written, we would have a superposition corresponding to the product of the Fourier transforms in the second register. This is because the amplitude in the second would then be

$$\int_{x_1} \psi_1(x_1)\,\phi_2(k_2)\exp(ik_2x_1) = \phi_1(k_2)\phi_2(k_2)$$

  (probability will be the absolute square of this.)

- The $|x_1\rangle$ register completely changes things. For example, now the probability in the second register will be added up for each value of x_1 :

$$Probability(k_2) = \int_{x_1} \psi_1(x_1)\,\phi_2(k_2)\exp(ik_2x_1) \times (\psi_1(x_1)\,\phi_2(k_2)\exp(ik_2x_1))^* = \|\phi_2(k_2)\|^2$$

  The information about the x_1 register is completely lost.

2.2.1 Status

We have studied, and are currently studying, various ways of getting around these problems. Unitary transformations bring about an extremely powerful set of computational possibilities which we are only learning to harness. We continue to be optimistic about our progress on NP-complete problems and are continuing our research into these. We plan to further describe our progress in a future report.

References

[1] L. K. Grover, *Quantum Mechanics helps in searching for a needle in a haystack*, *Phys. Rev. Letters*, 78(2), 325, 1997, also at http://www.bell-labs.com/user/lkgrover/.

[2] C. H. Bennett, E. Bernstein, G. Brassard & U.Vazirani, *Strengths and weaknesses of quantum computing*, SIAM Journal on Computing, 26, no. 5, Oct. 1997, p. 1510-1524.

[3] C. Zalka, *Grover's quantum searching is optimal,* Phys. Rev. A 60, 2746 (1999).

[4] L. K. Grover, *Quantum computers can search rapidly by using almost any transformation*, Phys. Rev. Letters, 80(19), 1998, 4329-4332; *A framework for fast quantum mechanical algorithms*, Proc. 30th ACM Symposium on Theory of Computing (STOC), 1998, 53-63.

[5] Quantum Computing: Pro and Con, John Preskill (Caltech), quant-ph/9705032, Proc. Roy. Soc. Lond. A454 (1998) 469-486.

[6] G. Brassard, P. Hoeyer, M. Mosca and Alain Tapp, *Quantum amplitude amplification and estimation*, quant-ph/0005055; G. Brassard and P. Hoyer, quant-ph/9704027.

[7] L. K. Grover and Terry Rudolph, "How significant are known algorithms for collision finding & element distinctness?", quant-ph, Sep. 12, 2003, Vol. 4, No.3, May 30, 04, pp201-206, Quantum Information & Computation, QIC031008..

[8] L. K. Grover and Anirvan Sengupta, From coupled pendulums to quantum searching, Mathematics of Quantum Computation, pages 119-134, CRC Press, 2002; L. K. Grover and Anirvan Sengupta, A Classical Analog of Quantum Search, PRA.

[9] L. K. Grover, A new quantum scheduling algorithm, International Journal on Foundations of Computer Science, (IJFCS), special issue on quantum information, April 2003.

[10] L. K. Grover, "Trade-offs in the quantum search algorithm, Phys. Rev. A 66, 052314 (2002).

[11] S. Aaronson, *Quantum lower bound for the collision problem*, STOC '02, pp.635-642. Also quant-ph/0111102.

[12] H. Buhrman et al, *Quantum Algorithms for Element Distinctness*, quant-ph/0007016.

[13] S. Kutin, *Quantum lower bound for the collision problem,* quant-ph/0304162.

[14] A. Ambainis, *Quantum Lower Bounds for Collision and Element Distinctness with Small Range*, quant-ph/0305179.

[15] Y. Shih, *Quantum lower bounds for the collision and element distinctness problems*, quant-ph/0112086.

[16] G. Brassard, P. Hoyer & A. Tapp, *Quantum Algorithms for the collision problem*, SIGACT News, 28:14-19,1997. Also quant-ph/9705002

[17] From Schrödinger's Equation to the Quantum Search Algorithm, Lov K. Grover, American Journal of Physics, July 2001.

[18] Tight bounds on quantum searching, Michel Boyer, Gilles Brassard, Peter Hoyer, Alain Tapp, quant-ph/9605034, Fortsch. Phys. 46 (1998) 493-506.

[19] Quantum vs. Classical Communication and Computation, Harry Buhrman, Richard Cleve, Avi Wigderson, Proceedings of the 30th Annual ACM Symposium on Theory of Computing (ACM Press), 1998.

[20] *Quantum searching a classical database (or how we learned to stop worrying and love the bomb)* Terry Rudolph and Lov Grover, quant-ph/0206066.

3 Quantum Communication

3.1 Introduction & Overview

In the course of this grant we undertook a variety of studies related to issues in quantum communication. Some of these studies overlapped with our work on algorithms, and have been reported in the previous sections. The remainder of our work can be loosely categorized into research focussed on the role of reference frames in quantum communication, and research aimed at elucidating fundamental primitives of quantum communication such as state estimation and state targeting. Portions of the research described in this chapter were conducted independently by Terry Rudolph when he was at Bell Labs and being funded by this grant.

3.1.1 Reference Frames

It is generally presumed that when physical systems are being exchanged for the purposes of communication, the sender (Alice) and receiver (Bob) must share a reference frame – the precise nature of which depends on the particular physical systems involved. For example, when communicating via spin-1/2 systems, it is presumed Alice and Bob must share a spatial reference frame so that they may prepare and measure spin components relative to this frame. Because both the exchanged systems and the channels via which they are transmitted should ultimately be described quantum mechanically, it is natural to examine the extent to which the laws of quantum mechanics fundamentally *necessitate* this presumption.

The question of necessity or otherwise of a shared reference frame (SRF) is clearly of interest for pragmatic reasons. In general, establishing a perfect SRF requires infinite communication (i.e., transmitting a system with an infinite-dimensional Hilbert space [1]); as such, from a communication theory perspective, a perfect SRF is a resource that is often quantitatively comparable to the sharing of an infinite number of correlated classical bits. For example, if the SRF is secret (known only to Alice and Bob) it can be used by them to securely generate an arbitrarily long secret key suitable for cryptography [2]. In practise, perfect SRFs are an idealization, and any finite (i.e., approximate) SRF should be viewed as a quantitative physical resource.

In section **3.2** below, we report on our work aimed at providing a framework for tackling problems regarding the amount of communication required to establish spatial reference frames. In particular we show how to use a variant of the quantum search algorithm to facilitate establishment of a reference frame. Our scheme makes no use of entanglement in order to achieve efficiencies

[1] For example, establishing a shared direction or Cartesian frame in space can be accomplished to any desired accuracy by transmitting quantum systems [2, 3], with an associated communication cost.

[2] Specifically, in the case of a shared Cartesian frame, then Alice can generate a random classical key, determine a direction from it (i.e., angles θ, ϕ) and send a physical system aligned in this direction to Bob.

comparable to much less practical 1-way communication schemes which require large amounts of entanglement.

Along with requiring communication to establish, quantum mechanics dictates that finite SRFs necessarily drift [4] and thus are intrinsically depleted over time. Moreover, for the case of conserved quantities such as angular momentum, measurement of non-orthogonal states inevitably causes disturbances to the measuring apparatuses (by the Wigner-Araki-Yanase theorem [5]), again depleting the SRF. We also note that shared prior entanglement, a valuable resource in quantum information theory, can be consumed to establish SRFs [6].

In section **3.3** below we report on our work showing how the implicit assumption that SRF's are necessary for quantum communication is in fact quite wrong. By appropriate encoding of quantum information in the *relative* properties of the transmitted qubits, asymptotically perfect communication is possible even in the complete absence of SRF's.

Finally in section **3.4** we report on how the vacuum can be used as a resource for quantum communication, if two observers share a global position reference frame (by making use of the Unruh effect).

3.1.2 Primitives of quantum communication

A fundamental primitive of quantum communication is state estimation. This primitive encompasses a wide variety of tasks undertaken by the receiver of quantum systems under circumstances wherein she has only partial information about the state of the systems in question. In section **3.5** below we report on our work elucidating the problem of unambiguously discriminating mixed states, a task we were the first to realize was possible.

A second fundamental primitive of quantum communication is state targeting (sometimes known as state control). This primitive encompasses a wide variety of tasks undertaken by the sender of quantum system - many tasks have obvious duals to those of state estimation. We were the first to realize the existence of this important primitive. Section **3.6** below reports on our work on this primitive.

3.2 Direction Finding using Quantum Searching

The amplitude amplification transformation may be expressed in the form: $UI_tU^\dagger I_s$. Visualize U and U^{-1} as the transformation from Alice's to Bob's reference frame and vice-versa. Then the transformation $UI_tU^\dagger I_s$ is equivalent to taking a particle from Alice's frame to Bob's frame; inverting its phase in Bob's frame, going back to Alice's frame, inverting its phase in this frame and so on. As can be seen by a simple quantum search type analysis, this transformation has the effect of increasing the phase rotation angle of the particle that depends on how misaligned the axes of the two frames were. This provides a means for estimating the angles between the two reference frames.[20]

In a large quantum computer or in quantum communication, for states and operations to be well defined we presume the existence of perfectly aligned frames of reference. In reality such frames require resource overhead in order to establish. In a large quantum computer or in quantum communication, for states and operations to be well defined we presume the existence of perfectly aligned frames of reference. In reality such frames require resource overhead in order to establish. We undertook a rather novel analysis of the communication complexity of establishing a shared reference frame (SRF).

Quantum physics allows for powerful new communication tasks that are not possible classically. Such quantum communication tasks generically require one party to prepare systems in well defined quantum states, and send these systems to another party. Since the states used are generally defined only with respect to some sort of reference frame, a perfect shared reference frame (SRF) between both parties is normally presumed. In general, however, establishing a perfect SRF requires infinite communication (i.e. transmitting a system with an infinite-dimensional Hilbert space, or an infinite number of systems with finite-dimensional Hilbert spaces).

In quantum communication theory, the specific physical systems being exchanged determine the type of reference frame that the communicating parties must share; conversely, the ability to exchange physical systems generally allows for certain reference frames to be established. For example, in order for two parties to agree on the superposition $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ of a single spin-1/2 system, they must share aligned spatial axes; conversely, by exchanging spin-1/2 systems they can establish aligned spatial axes.

The problem of using spin-1/2 systems to establish either a single direction in space or an orthogonal trihedron (xyz-axes), has received considerable attention [3, 4, 5, 6, 3, 8]. In particular, the following *standard scenario* has been studied in depth: Alice sends Bob N spin-1/2 particles in a state which encodes some spatial direction $\vec{n}_A$. Bob performs a measurement on the N spins, which results, with probability $P(\vec{n}_e|\vec{n}_A)$, in an estimation $\vec{n}_e$ of the direction $\vec{n}_A$. The fidelity F of the estimation is defined as $\frac{1}{2}(1 + \vec{n}_e \cdot \vec{n}_A)$, and the goal is to optimize the expected fidelity, $\bar{F}$, with respect to initial states prepared by Alice and measurements performed by Bob, for uniformly chosen $\vec{n}_A$. (Note that a random guess of direction has an expected fidelity of 1/2; a fidelity of 0 corresponds to an estimate antiparallel to $\vec{n}_A$). In general it is found that if Alice sends Bob the systems in a tensor product of pure states, then $\bar{F}^{\max} = 1 - O(\frac{1}{N})$, while if Alice prepares entangled states then $\bar{F}^{\max} = 1 - O(\frac{1}{N^2})$. In both cases the measurements Bob must perform to achieve this are *joint* (i.e. entangled) measurements over the N particles, and in general they are positive operator valued measurements (POVM's) as opposed to standard Von-Neumann projection valued measurements (PVM's).

We have expanded the study of procedures for establishing SRFs, by demonstrating the wealth of nontrivial possibilities which remain to be explored. We show that by considering multi-round communication scenarios, it is possible to achieve a *worst case* fidelity of $F = 1 - O(\frac{\log^2 N}{N^2})$, which is within a logarith-

mic factor of the best *average case* fidelity obtainable in the standard scenario. Moreover, in contrast to the standard scenario procedure which achieves this best average case fidelity, the protocol that we propose makes no use of entanglement - either in the states that must be prepared or in the measurements that must be performed! We feel this is of great pragmatic importance, since if Alice and Bob had the ability to create and exchange the arbitrarily large entangled states, and perform the arbitrarily large joint measurements required within the standard scenario, then in most situations they would be far better off to use the ideas presented in the next section of this report [9] - wherein it is shown how they can perform quantum communication *perfectly* (i.e. without having noise due to the finiteness of the SRF) and with asymptotically no loss of resources.

In addition to the heavy use of entangled states and measurements, there are several other ways in which the standard scenario (and the extension of it in which Alice and Bob align an orthogonal trihedron as opposed to a single direction) is somewhat unsatisfactory. For a start, the particular choice of cost function (e.g. the fidelity) has a strong bearing on what the optimal states and measurements turn out to be [6]. Secondly, the optimizations are performed for the *average case* scenario, and not the *worst case* scenario, which is arguably more interesting (and which is the norm for evaluating communication costs). This yields the difficulty that if we wish to ask questions pertinent to future quantum communication using spatial axes aligned under such procedures, it is somewhat problematic to translate these results into standard properties of the quantum channel. This in turn makes it difficult to determine the extent to which such communication overhead can be amortized. The standard scenario also ignores the question as to whether allowing backwards communication (from Bob to Alice) can improve their ability to align their reference frames. Finally, in quantum communication scenarios it is natural to presume that Alice and Bob have access to *both* classical and quantum channels, and to examine the extent to which classical and quantum communication can in some sense be traded off against each other. Peres has raised some interesting questions about classical communication costs within the standard scenario [10], although within this scenario, from a communication theory perspective, one may generally assume that such costs are amortized into the definition of the protocol. Below we will give some simple examples of protocols for which such amortization is not possible.

With a view to rectifying some of the shortcomings of the standard scenario mentioned above, we consider strategies for aligning spatial reference frames that allow Bob, within a worst case scenario, to directly determine the Euler angles which relate his and Alice's axes. More precisely, if θ is an Euler angle relating Alice and Bobs' axes, and θ' is the estimation of θ inferred by Bob, then we will be interested in the amount (and type) of communication required for protocols that achieve $Pr[|\theta - \theta'| \geq \delta] \leq \epsilon$, for some fixed $\epsilon, \delta > 0$. By setting $\delta = 1/2^{k+1}$ we say that with probability $(1 - \epsilon)$ Bob has a k bit approximation to θ.

The simplest protocol we have been able to find for determining the Euler an-

gles $\{\phi, \theta, \psi\}$ in a worst-case scenario is as follows. Unless otherwise indicated by a superscript A, all states and operators are written in Bob's frame of reference. We define the Euler angles such that the rotation matrix describing the change from Alice to Bobs' frame of reference is given by $R \equiv e^{-i\psi\sigma_z/2}e^{-i\theta\sigma_y/2}e^{-i\phi\sigma_z/2}$. Explicitly,

$$R = e^{-i(\psi+\phi)/2}\begin{pmatrix} \cos\theta/2 & -e^{i\phi}\sin\theta/2 \\ -e^{i\psi}\sin\theta/2 & e^{i(\phi+\psi)}\cos\theta/2 \end{pmatrix}.$$

Let $\theta = \pi T$, where $0 \leq T \leq 1$ has a binary expansion $T = 0 \cdot t_1 t_2 \ldots$. The protocol we propose involves Alice and Bob following an iterative procedure which determines the bits t_1, t_2 up to t_k independently. We choose the probability of error for each bit of T to be ϵ/k, so that after finding the first k bits of T the total probability of error is $1 - (1 - \epsilon/k)^k \leq \epsilon$.

To find t_1, Alice sends a single spin polarized in her z direction, and Bob measures it in his $\pm z$ basis. The measurement by Bob yields the outcome 1 (spin down say) with probability: $P_1 = \cos^2\frac{\theta}{2} = \frac{1}{2}[1 + \cos 2\pi T] = \frac{1}{2}[1 + \cos(2\pi\ 0 \cdot t_1 t_2 \ldots)]$. Repeating this n times, Bob obtains an estimate P_1' as to the true value of P_1, and thus an estimate T' of the true value of T. If we choose n (details below) such that $|P_1 - P_1'| \leq 1/4$ with probability $(1 - \epsilon/k)$, then $|T - T'| \leq 1/4$ with the same probability, and this implies that T' agrees with T to at least the first bit t_1.

The procedure is readily generalized by more exchanges, in order to find θ to more bits of precision, the details can be found in the paper cited above. The total amount of qubit communication required to obtain bits t_1 through t_k by this procedure is

$$N = n \times \sum_{j=1}^{k} 2^{j-1} = n(2^k - 1) = O(2^k \ln(2k/\epsilon)).$$

Note that, since we determine the bits of T independently with this protocol, the number of *rounds* of communication can be reduced by running the procedure in parallel. In order to obtain the other Euler angles accurate to k bits, or, for that matter, to fix a direction in space with θ, ϕ angles fixed to k bits, we can extend this protocol by changing the transformations that Alice and Bob perform (and/or the initial state Bob prepares). This only increases the communication overhead by a constant factor.

It is useful to understand our protocol in quantum computational terms. In effect, Alice and Bob are performing a combination of a distributed quantum search algorithm [13] and a phase estimation algorithm [14]. In a quantum search algorithm, a generic transformation of the form $(I_t R^\dagger I_{\bar{0}} R)$, where R is an arbitrary unitary transformation and $I_t, I_{\bar{0}}$ are phase inversions about source and target states, is repeated some large number of times in order to coherently drive the state of the computer. Here we are performing a similar procedure, where the computer is now only a single bit, the phase inversions are Alice and Bobs' local σ_z rotations, and the unitary transformation R is passively provided

by their lack of a SRF. We may also interpret this procedure as one in which the eigenvalues of U are being 'quantum computed' - in fact there is much in common here with Kitaev's version of the quantum phase estimation procedure [15].

A more general distributed quantum computation would require Alice and Bob to create entangled states. Without a SRF, however, this is at first glance problematic - since pure entangled states in Alice's frame are generally mixed in Bob's frame. A possible resolution is for Alice and Bob to use the encodings of spin states presented in [9]. Such encodings allow for three entangled spin-1/2 particles to form logical qubit states, $\{|0_L\rangle, |1_L\rangle\}$ which are *not* reference frame dependent. As such, Alice and Bob could, for instance, run the more standard phase estimation algorithm [16], which involves using the discrete fourier transform to obtain the best k bit estimator of the eigenvalue(s) of a unitary transformation.

It is an open question whether the ability to exchange classical information ever helps in reducing the amount of qubit communication required. It does, as remarked upon in the introduction, facilitate certain types of protocols in which entanglement might be "traded in" for a reference frame. We leave the reader with the following related and important question: To what extent does sharing of one type of reference frame (e.g. synchronised clocks) facilitate in establishing a different type of reference frame (e.g. aligned spatial axes). Surprisingly, it seems that in some cases such facilitation is possible. Consider, for example, the case when Alice and Bob have synchronised clocks and thus can quantum communicate perfectly using two (possibly degenerate) energy eigenstates $\{|e_1\rangle, |e_2\rangle\}$ of some system. They can use a register of these qubits to take the place of the "logical qubits" discussed above in the phase estimation procedure. Since each logical qubit required three spin-1/2 particles, this results in at least a constant factor improvement in the total amount of qubit communication required.

3.3 Communication without shared reference frames

We have shown that both classical and quantum communication can be performed *without* first establishing a SRF by employing entangled states of multiple qubits. We prove that, without any prior SRF, the minimum number of qubits required to transmit a classical bit of information is two, and that four qubits can transmit an encoded "logical" qubit. Allowing increasingly more qubits to be entangled improves these ratios, and we prove that communication of one classical bit per transmitted qubit or one logical quantum bit per transmitted qubit can be achieved asymptotically. [21]

Our results provide the first link between decoherence free subspaces - an active area of study in quantum computation, and quantum communication theory. We now illustrate our results with the simplest examples:

3.3.1 Classical Communication

The following communication protocol illustrates the general idea for classical communication. Alice sends Bob the antisymmetric state $|\Psi^-\rangle$ to communicate $b = 0$ and *any* symmetric state for $b = 1$. Bob then performs a projective measurement onto the antisymmetric and symmetric subspaces and will recover b with certainty. Thus, using this protocol, Alice can communicate one classical bit to Bob for every two qubits sent, thereby obviating the need for a SRF.

The efficiency of the scheme can be increased by entangling more qubits. Consider the transmission of N qubits; the superoperator $\mathcal{E}_N$ that describes the lack of a SRF acting on a general density operator σ of N qubits is given by $\mathcal{E}_N(\sigma) = \int \mathrm{d}\Omega\, R_1(\Omega) \cdots R_N(\Omega) \sigma R_1^\dagger(\Omega) \cdots R_N^\dagger(\Omega)$. This "collective" tensor representation of $SU(2)$ on N $j = 1/2$ systems (i.e., $R(\Omega) \in SU(2)$ acting identically on all qubits) can again be decomposed into a direct sum of $SU(2)$ irreps, each with angular momentum quantum number j ranging from 0 or $1/2$ to $N/2$.

We have, in fact, been able to prove:

Claim: The maximum number of classical messages that can be perfectly transmitted without a SRF is equal to the number of $SU(2)$ irreps in the direct sum decomposition (denoted $C^{(N)}$). Using standard group theory, the number of classical bits that can be transmitted per qubit using the above scheme is $N^{-1} \log_2 C^{(N)}$, which tends asymptotically to $1 - \frac{\log_2 N}{2N}$. Thus, in the large N limit, one classical bit can be transmitted for every qubit sent. Remarkably, this rate is equivalent to what can be accomplished if they *do* employ a SRF.

In general, the states to be transmitted in the optimal scheme for N qubits are highly entangled. (They include, for example, singlet states of N qubits.) Such multipartite entangled states are difficult to prepare in practice. However, it is clear that for the case $N = 2$ the required entanglement is easily achieved in quantum optics, in particular in the polarization degree of freedom.

3.3.2 Quantum Communication

At first glance, the requirements on any SRF are more stringent for quantum communication utilizing non-orthogonal states and operations than for analogous classical communication. For instance, communicating a classical bit using a single spin-1/2 system requires Alice and Bob to agree only on a z-direction: Alice prepares a qubit in an eigenstate of $\hat{L}_z$ encoding this classical bit, and Bob then measures $\hat{L}_z$ obtaining the desired bit. For quantum communication, superpositions of such states would require a shared Cartesian frame in order that the relative phases in the superposition be well defined. In fact, it was argued in [9] that such SRFs are a necessary, hidden cost of quantum teleportation; our results show this claim is erroneous.

Despite the decohering effect of the superoperator $\mathcal{E}_N$ describing the absence of a SRF logical qubits can be encoded into the transmitted qubits in such a way that the encoded quantum states are preserved even without an SRF. It is useful to treat $\mathcal{E}_N$ as a decohering channel that describes a collective decoherence

mechanism acting identically on all qubits, and so we appeal to the techniques of decoherence free subspaces (DFS's) [10, 11]. For N (even) transmitted qubits, we observe that the superoperator $\mathcal{E}_N$ leaves all $j = 0$ states in the direct sum decomposition invariant. Thus, the $j = 0$ states span a DFS, denoted $\mathbb{H}_{\rm DFS}$. The number of $j = 0$ states is given by the multiplicity

$$\dim \mathbb{H}_{\rm DFS} = c_0^{(N)} = \binom{N}{N/2} \frac{1}{N/2+1} \,. \tag{1}$$

For $N = 2$, there is only one $j = 0$ state: the Bell state $|\Psi^-\rangle$. For $N = 4$, there are two distinct $j = 0$ states, and thus four physical qubits can encode a single logical qubits as follows:

$$|0_L\rangle = \tfrac{1}{2}(|01\rangle_{12} - |10\rangle_{12})(|01\rangle_{34} - |10\rangle_{34})$$
$$|1_L\rangle = \tfrac{1}{\sqrt{3}}(|0011\rangle_{1234} + |1100\rangle_{1234}) - \tfrac{1}{2\sqrt{3}}(|01\rangle_{12} + |10\rangle_{12})(|01\rangle_{34} + |10\rangle_{34}) \,,$$

where $\{|0\rangle, |1\rangle\}$ is *any* orthogonal basis for the single qubit Hilbert space. The superoperator $\mathcal{E}_N$ preserves the two-dimensional subspace spanned by these states, i.e., this subspace is a DFS. Single-qubit operations on this logical qubit are an encoded representation of $SU(2)$ that commutes with the tensor representation generating the superoperator $\mathcal{E}_N$. The encoded generators are given by Hermitian exchange operations (i.e., two-qubit permutations), which clearly do not require a SRF; for details of the encoded $SU(2)$ group as well as two-logical-qubit coupling operations, see [10, 11].

Thus, a logical qubit can be encoded into four physical qubits [3]. Asymptotically, the number $N^{-1} \log_2 c_0^{(N)}$ of logical qubits encoded per physical qubit in N physical qubits using DFSs behaves as $1 - \frac{3 \log_2 N}{2N}$, which approaches unity for large N. This remarkable result proves that quantum communication without a SRF is asymptotically as efficient as quantum communication *with* a SRF, and is the communication analog of the "asymptotic universality" proven in [11].

Many interesting questions remain. For instance, we have considered only situations where *local* SRFs are generally presumed necessary. However, for scenarios involving position-momentum entanglement it appears that *global* shared coordinate systems are required. We have also limited our discussion to non-relativistic quantum mechanics; given the ubiquitous nature of reference frames in relativity, it may be advantageous to examine similar questions in a relativistic context.

3.4 The vacuum as a communication resource

Entanglement is in the eyes of the beholder. Unitary transformations that affect the definition of one's systems change, in general, the amount of entanglement in a given state. For instance, the Lorentz transformation of the spin degrees of freedom of a particle depends on its momentum. Thus the entanglement between

[3] Using decoherence free *subsystems*, it is possible to encode one logical qubit into three physical qubits [11].

the spin and momentum of a particle is not a Lorentz-invariant concept [1]. One observer may see a product state, while another believes there is entanglement. For another example, take a state containing a single circularly polarized photon. When written in terms of linear polarization, this state becomes $|0\rangle|1\rangle + |1\rangle|0\rangle$, which seems to be maximally entangled (for more such examples see [2]). In both these examples, however, the apparent entanglement is always *local*. As such, it cannot be used for any nontrivial quantum communication protocols.

Here we discuss a well-known phenomenon that does produce *nonlocal* entanglement, the Unruh effect. It involves just the vacuum, and the unitary transformations arise when one describes accelerating observers. We investigate which, if any, quantum communication protocols could be implemented using this resource.

3.4.1 The Unruh effect

Suppose Alice is accelerating at a uniform acceleration a. As is well known [3], she will perceive the Minkowski vacuum state (of, say, the electromagnetic field) as a mixed thermal state with equivalent temperature $k_B T = \hbar a/(2\pi c)$. Since the transformation from an inertial to an accelerating frame is unitary, however, the vacuum should be transformed into a pure state, not a mixed state. Indeed, the state of the modes inside Alice's event horizon only appears mixed because it is entangled with modes that lie outside that horizon. More precisely, each mode is entangled with one "mirror" mode, a mode propagating along a trajectory that is the mirror image relative to the appropriate event horizon. For each pair of mirror modes of frequency ω' (as measured by the accelerating observers), the entangled state is in fact a two-mode squeezed state of the form

$$|\Psi\rangle = \sqrt{1-\mu^2} \sum_n \mu^n |n\rangle|n\rangle, \tag{2}$$

where $\mu = \exp(-\pi\omega' c/a)$. Mirror modes are the appropriate modes for an observer Bob accelerating uniformly at the same acceleration a but in the opposite direction along a trajectory that is, again, a mirror image relative to the same event horizon.

The Unruh effect can be understood by considering the transformation between creation and annihilation operators from Alice's frame of reference to that of a Minkowski observer, Mork. The transformation is of the form

$$\begin{aligned} a' &= (a - \mu\tilde{a}^\dagger)/\sqrt{1-\mu^2} \\ \tilde{a}' &= (\tilde{a} - \mu a^\dagger)/\sqrt{1-\mu^2}. \end{aligned} \tag{3}$$

where we absorb irrelevant phase factors in the definitions of the mode operators. Here we use notational conventions that primed operators and variables correspond to accelerating observers, and that operators with a tilde correspond to mirror modes. The modes here are assumed to be localized wave packet modes, as constructed in [4]. The fact that a creation operator appears in the transformation of an annihilation operator, distinguishes (3) from standard unitary transformations of modes [2].

3.4.2 Quantum communication protocols

The questions we consider now are *(i)* what useful quantum information tasks might Alice and Bob perform with the entangled state (2)? *(ii)* how does the Minkowski observer Mork describe their actions and makes sense of it? After all, according to Mork, Alice and Bob share nothing but the vacuum and are causally disconnected, and so it may seem they should not be able to perform any interesting protocols. We will consider several quantum information processing protocols that are known to rely on entanglement and discuss to what extent they can be implemented by Alice and Bob.

Concerning question *(i)*, there is an important distinction between two types of quantum communication protocols: those that terminate with at least one party holding a quantum state, and those that terminate with all parties holding purely classical information. In the former case the desired quantum states typically exist only in the eyes of Alice and Bob, and thus, in the scenarios considered here, only as long as they keep accelerating. Clearly this does not allow Alice and Bob to ever communicate, not even classically. This does restrict at least the usefulness of the protocol and sometimes it prevents the protocol from being executed at all. In the latter type of protocols, however, Alice and Bob are *both* free to decelerate after having performed the required quantum operations (since we presume, hopefully correctly, that classical information, unlike quantum information, is not affected by deceleration), and thus may thus communicate afterwards. This then leads, apart from practical considerations, to useful implementations of certain quantum protocols. Our primary goal here is to discuss in detail an example of each type, to demonstrate both the potential and the limitations of vacuum entanglement for quantum communication protocols. We also briefly mention various other protocols.

Concerning question *(ii)* we note that Alice's and Bob's local operations appear nonlocal to Mork, and *vice versa*. The parameter μ, which measures the strength of the Unruh effect and the amount of nonlocality, written in Mork's coordinates is equal to (using Ref. [4]) $\mu = \exp(-\pi^2 D/\lambda)$, where D is the distance between the mirror trajectories and λ the wavelength. In order to have any appreciable effect, at the moment Alice and Bob wish to use their entanglement, they must be within a distance $D \sim \lambda/\pi^2$ of each other, that is, within the coherence length of the vacuum fluctuations[9]. This is how Mork can make some physical sense out of the nonlocal character of Alice's and Bob's actions and of the fact that, counter to Mork's expectations, some of their protocols seem to work!

We examined teleportation as viewed by both Unruh and Minkowski observers. Another interesting protocol we examined was a two-party protocol known to be impossible within the standard paradigm, namely (strong) coin flipping:

3.4.3 Secure coin flipping

Two-party cryptographic protocols involve two antagonistic parties, Alice and Bob, who wish to complete some information processing task. In classical information theory it has been proven that no two-party protocols exist which have "information theoretic" security. In quantum cryptography protocols *do* exist with various degrees of quantum information theoretic security, and thus examining these protocols provides a readily quantifiable way of distinguishing classical from quantum information theory.

It is standard to assume in two-party quantum cryptography that the initial state of systems held by Alice and Bob is separable, i.e. of the form $|0\rangle_A |0\rangle_B$. However it is interesting to note that if Alice and Bob share prior trusted entangled states then some (otherwise impossible) arbitrarily secure quantum cryptographic protocols become possible, while others remain impossible. For example, if they share a maximally entangled state of two qubits, then an arbitrarily secure coin flip is trivially possible - the coin flip outcome is simply the result each party obtains by measuring their half of the entangled pair in an orthogonal basis. By contrast, as can be deduced from [11], the sharing of a prior trusted entangled state does *not* give Alice and Bob the ability to perform an arbitrarily secure bit commitment. Thus there is an intricate hierarchy of the security obtainable in these protocols with respect to any initially trusted entanglement resources.

What we are proposing here is that the (Minkowski) vacuum state $|0\rangle_A |0\rangle_B$ can also be considered a "prior trusted" state. Since, as discussed above, this is in fact also a (Rindler) entangled state, we surmise that it can, in fact, be used to implement a secure coin flip. It has been shown by Kitaev, that within the standard quantum communication paradigm wherein Alice and Bob start with a state of the form $|0\rangle_A |0\rangle_B$ and build up an entangled state via rounds of communication, all coin flipping protocols satisfy $(1/2 + \epsilon_A^b)(1/2 + \epsilon_B^b) \geq 1/2$, $b = 0, 1$ where $\epsilon_{A,B}^b$ are the biases achievable by Alice and Bob.. Thus, arbitrarily secure quantum coin flipping within this paradigm is impossible. (The best known protocols do not even saturate Kitaev's lower bound).

We should emphasize that in two-party cryptographic protocols there is a basic presumption that each party feels secure about their own laboratory. In fact, it is desirable that this need be the *only* thing they feel secure about - i.e. we presume that the parties should not have to feel secure about things outside their own lab.

The protocol we proposed is as follows:

> *Unruh based coin flipping:*
>
> An instance of the protocol is specified by a point in space-time (X, T), chosen to be located in Alice's lab, and at time $t = 0$ Alice, who is uniformly accelerating with acceleration a, is instantaneously at rest. At time $t = 0$ and position $x = X - cT$ Alice turns on and then off a detector (D_1), and verifies the initial state is Minkowski vacuum (see Figure). At (X, T) Alice turns on a detector D_2, if she

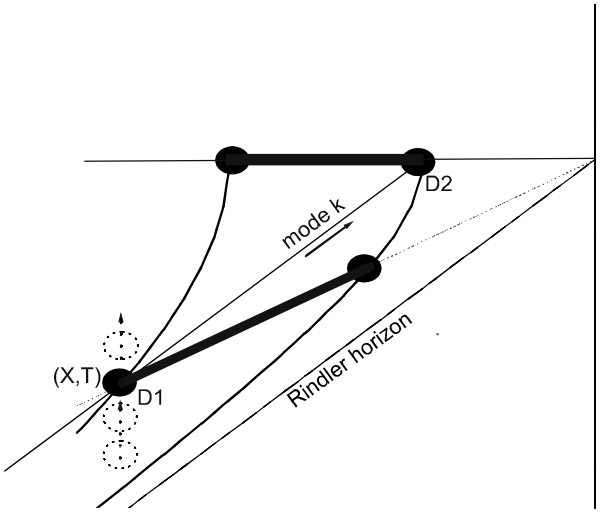


Figure 1: Relativistic quantum communication is achieved by means of the Unruh effect.

records a photon then the outcome of the coin flip is 1, otherwise it is 0. Bob follows the "mirror trajectory" and employs a "mirrored procedure" to Alice, such that he is detecting the other half of the Unruh entangled state.

The above protocol is, to say the least, slightly unconventional. However, intuitively speaking, it is simply relying on the fact that what Minkowski observers consider to be a separable vacuum state $|0\rangle_A |0\rangle_B$, transforms to the entangled state (2) for accelerating observers. The purpose of the first detector measurement at time $t = 0$ is to ensure that the mode k (see Fig. 1) which will determine the coin flip outcome is in the correct Minkowski initial state. (A cheating Bob could have his friend try and populate this mode prior to it entering Alice's laboratory, for example).

Several other technical issues arise. Clearly a must be chosen to ensure that the probability of detector D_2 registering 0 photons is the same as that of registering one or more photons – i.e. such that $\mu^2 = 1/2$. We also wish this detector to be sensitive to a localized, travelling Unruh wavepacket. A formal quantization of Rindler space in terms of such modes can be found in [4], and from these results one can infer the appropriate detector mode function responses required.

We conclude with a few observations. Firstly we must assume that Alice's laboratory is large enough to contain both detectors at the appropriate space-time points. (Alice does not, however, require other guarantees about the whereabouts of Bob). Also, the further Alice and Bob are apart, the larger the

acceleration has to be. Thus there are nontrivial trade-offs between the various physical requirements of such a protocol.

Certain two-party quantum communication protocols that require entanglement can be performed with just the vacuum. Typically, protocols whose goal it is to produce a quantum state will not work in any useful way, but two-party protocols aimed at establishing purely classical information may work. In particular, unconditionally secure coin flipping is possible, so is unconditionally secure key distribution. On the other hand, teleportation is only possible in a weaker version.

3.5 Unambiguous discrimination of mixed states

Although the optimal procedures for discriminating between sets of pure states have been much studied, it is not generally appreciated that mixed states may also be unambiguously discriminated. In fact one sometimes encounters claims to the contrary in the literature. However this is only true *if the two mixed states have the same support.[22]*

There have, in fact, been some rather complicated extensions of the pure state discrimination problem, such as "state comparison" [17], and the problem of distinguishing one pure state given three possible initial states [18]. In fact these problems are just different versions of the more general problem of unambiguously discriminating two mixed states ρ_0, ρ_1.

More precisely, we seek the optimal three outcome POVM, $\{E_0, E_1, E_?\}$ which satisfies

$$\mathrm{Tr}(\rho_0 E_1) = 0 = \mathrm{Tr}(\rho_1 E_0) \tag{4}$$

and which maximizes the probability P of successful unambiguous discrimination:

$$P = w_0 \mathrm{Tr}(\rho_0 E_0) + w_1 \mathrm{Tr}(\rho_1 E_1), \tag{5}$$

where w_0, w_1 are the prior probabilities. Clearly unambiguous discrimination is not possible if the supports of the two density operators are identical. We assume therefore that $\mathrm{supp}(\rho_0) \neq \mathrm{supp}(\rho_1)$. In particular, we denote the kernel of ρ_b by $\mathcal{K}_b$ (b=0,1). It is also clear that any intersection of $\mathcal{K}_0$ and $\mathcal{K}_1$ is not useful for the purposes of discriminating ρ_0 and ρ_1 - we need be interested only in the part of $\mathcal{K}_0$ which lies in the support of ρ_1 for example. As such we presume that $\mathcal{K}_0$ and $\mathcal{K}_1$ are defined in $\mathrm{supp}(\rho_0) \cup \mathrm{supp}(\rho_1)$; they have null intersection. A necessary and sufficient constraint for satisfying Eq. (4) is that the POVM element E_b have support only in the subspace $\mathcal{K}_{\bar{b}}$., $b = 0, 1$ The remaining constraint to be satisfied while optimizing (5) is that the operator $E_?$be positive, that is

$$I - E_0 - E_1 \geq 0. \tag{6}$$

Although we do not have a general solution to this problem, we have been able to obtain upper and lower bounds which numerical studies indicate are quite stringent.

Lower bound for unambiguous discrimination between any two mixed states We consider a strategy that achieves UD of an arbitrary pair of mixed states and which is strongly dependent on the geometrical relationship between the two subspaces $\mathcal{K}_0$ and $\mathcal{K}_1$. We have been able to prove:

Theorem *Consider two arbitrary mixed states ρ_0 and ρ_1. Denote the dimensionality of their kernels, $\mathcal{K}_0$ and $\mathcal{K}_1$ by r_0 and r_1, and assume that $r_0 \geq r_1$. There exist orthonormal bases $\{|k_b^j\rangle\}_{j=1}^{r_b}$ for $\mathcal{K}_b (b = 0, 1)$ such that for $1 \leq j \leq r_0$, $1 \leq i \leq r_1$,*

$$\langle k_0^j | k_1^i \rangle = \delta_{ij} \cos(\theta_j),$$

where the θ_j are the canonical angles between $\mathcal{K}_0$ and $\mathcal{K}_1$ [19]. In this case, the expression

$$P_L = \sum_{j=1}^{r_1} P_{1D}^{\max}(|k_0^j\rangle, |k_1^j\rangle) + \sum_{j=r_1+1}^{r_0} \langle k_0^j | \rho_1 | k_0^j \rangle \tag{7}$$

forms a lower bound on the maximum probability of discriminating unambiguously between ρ_0 and ρ_1.

The eigenbases for the POVM achieving this lower bound are simply the vectors $|k_b^i\rangle$. In order to understand the geometry of the eigenbases for the POVM elements in this lower bound, it is helpful to realize that the canonical angles θ_i form the unique geometrical invariants describing the relationship between two subspaces. They can be defined iteratively: θ_1 is the smallest angle between any pair of vectors drawn from $\mathcal{K}_0$ and $\mathcal{K}_1$, and $|k_0^1\rangle, |k_1^1\rangle$ are the corresponding pair of vectors. θ_2 is the smallest such angle after these two vectors are removed, and so on. In this way, one obtains a simple geometrical picture of the measurement achieving the lower bound.

An upper bound for unambiguous discrimination between any two mixed states The upper bound is

$$P^{\max} \leq \begin{cases} 1 - 2\sqrt{w_0 w_1} F(\rho_0, \rho_1) & \text{if } F(\rho_0, \rho_1)^2 < \sqrt{\frac{w_{\min}}{w_{\max}}} \\ w_{\max}(1 - F(\rho_0, \rho_1)^2) & \text{otherwise} \end{cases}$$

where $F(\rho_0, \rho_1) = Tr \left| \sqrt{\rho_0} \sqrt{\rho_1} \right|$ is the fidelity. In the case of equal prior probabilities, the upper bound has the simple form $P^{\max} \leq 1 - F(\rho_0, \rho_1)$. Numerical studies of rank 2 mixed states in a 4 dimensional Hilbert space indicate that even for randomly chosen ρ_0 and ρ_1, our upper and lower bounds are generally very close.

We have also shown that our lower bound reproduces *exactly* both the Chefles-Barnett result and the Sun-Bergou-Hillery result mentioned previously, by a much simpler analysis. We have no counterexample showing that our lower bound is not, in fact the optimal procedure for unambiguously discriminating two mixed states.

3.6 Optimal estimation of relative quantum information [23]

Observers within QM are generally presumed to measure physical quantities by means of classical apparatuses. Such devices are fixed with respect to a particular frame of reference, about which the observer has complete knowledge.

From a general perspective there are compelling reasons to go beyond this standard paradigm into one in which we treat all systems, including the measurement apparatuses, within the framework of QM. The first is internal consistency: Reference frames (which often form part of the measurement apparatus) and measurement devices are themselves constructed with physical objects, and thus should be describable with the framework of the theory itself. The second is more philosophical: If one accepts the generic validity of a principle underlying General Relativity, namely that the primitives of physical theories should be phrased in purely relational terms, then quantum states should be examined and understood within the context of their relationship to the physical apparatuses with respect to which they were prepared.

We have argued in the introduction that from the more specialized perspective of quantum information theory, the finite nature of reference frames is a subject of great interest, for both pragmatic and conceptual reasons. Such reference frames form a resource; they are a type of physical correlate with close analogies to entanglement. For instance they are consumed with use, and they cannot be established by local operations and classical communication.

A fundamental primitive of quantum information theory is *state estimation*. All previous studies of state estimation have worked within a restricted paradigm wherein the states are both prepared and measured with respect to perfect external classical reference frames. In this work we begin the process of examining a more general problem - state estimation of relative parameters of two uncorrelated (i.e., unentangled) physical systems, the states of which have small variance in the relevant degree of freedom. Estimation tasks for such an example include estimating the distance between two minimum uncertainty wavepackets of a massive particle, or the phase between a pair of coherent states of the electromagnetic field, or estimating the angle between the directions defined by a pair of SU(2) spin coherent states. It is this last example which shall be the focus of this section, although our results apply to a larger class of states, and our approach can be applied to other variables.

One scheme for measuring relative quantities is to measure each system independently with respect to an external RF, e.g., to perform an optimal estimation of each spin direction and to then calculate the angle between these estimates. We prove that such (local) schemes are not optimal. In fact, we find that possessing an external RF provides no advantage. On the other hand, the ability to perform *non-local* measurements *is* necessary to achieve the optimum. However, it is clear that measuring a single spin against a classical reference frame does not involve a non-local measurement. We resolve the apparent conflict, by showing that in the limit of one spin becoming classical, our optimal relative measurement gives the same information gain as does the optimal measurement

for estimating a single spin's direction relative to a classical RF, and that the need for non-local measurements disappears. These results contribute to our understanding of how the macroscopic systems that act as RFs can be treated within quantum theory, and more specifically how global degrees of freedom, which are defined relative to a classical RF, can be treated as a relative ones between quantized systems. Such an understanding is likely to be critical for quantum gravity and cosmology, wherein all degrees of freedom are expected to be relative.

3.6.1 Two spin-1/2 systems

The simplest example of relative parameter estimation arises in the context of a pair of spin-1/2 systems. Alice prepares the product state $|\mathbf{n}_1\rangle \otimes |\mathbf{n}_2\rangle$, where $|\mathbf{n}\rangle$ is the eigenstate of $\mathbf{J}\cdot\mathbf{n}$ with positive eigenvalue (note that every state of a spin 1/2 system is an SU(2) coherent state). Bob's task is to estimate the relative angle $\alpha = \cos^{-1}(\mathbf{n}_1 \cdot \mathbf{n}_2)$ given no knowledge of the global orientation of the state. Because the joint Hilbert space decomposes into a $J = 0$ and a $J = 1$ irrep, the optimal POVM has the form $\{\Pi_A, \Pi_S\}$, where $\Pi_A = |\Psi^-\rangle\langle\Psi^-|$ is the projector onto the antisymmetric ($J = 0$) subspace and $\Pi_S = \mathbb{I} - \Pi_A$ is the projector onto the symmetric ($J = 1$) subspace. The conditional probability of outcomes A and S given α are simply $p(A|\alpha) = \mathrm{Tr}(\Pi_A \rho_\alpha) = \frac{1}{2}\sin^2(\alpha/2)$ and $p(S|\alpha) = 1 - p(A|\alpha)$. The average information gain and the optimal guess for the value of α depend on Bob's prior over α.

If we consider a uniform prior for each system's spin direction, the prior over α is $p(\alpha) = \frac{1}{2}\sin\alpha$. This implies posteriors $p(\alpha|A) = \sin^2(\alpha/2)\sin\alpha$ and $p(\alpha|S) = \frac{1}{3}(2 - \sin^2(\alpha/2))\sin\alpha$ which are peaked at $2\pi/3$ and 0.4094π respectively. It follows that these are the best guesses for the angle α given each possible outcome. Using the posteriors, we find $I_A \simeq 0.2786$, $I_S \simeq 0.02702$, which yields $I_{\mathrm{av}} \simeq 0.08993$. Less information is acquired than in the parallel-antiparallel estimation problem, because angles near $\pi/2$ are more difficult to distinguish.

3.6.2 One spin-1/2, one spin-j system

We now consider the estimation of the angle between a spin-1/2 system and a spin-j system for some arbitrary j, where the latter is in an SU(2) coherent state $|j\mathbf{n}\rangle$ (the eigenstate of $\mathbf{J}\cdot\mathbf{n}$ associated with the maximum eigenvalue) [**?**]. Alice prepares $|\mathbf{n}_1\rangle \otimes |j\mathbf{n}_2\rangle$ and Bob seeks to estimate $\alpha = \cos^{-1}(\mathbf{n}_1 \cdot \mathbf{n}_2)$. The joint Hilbert space decomposes into a sum of a $J = j + 1/2$ irrep and a $J = j - 1/2$ irrep. The optimal measurement is the two outcome POVM $\{\Pi_+, \Pi_-\}$, where $\Pi_\pm$ is the projector onto the $j \pm 1/2$ irrep [4]. Using Clebsch-Gordon coefficients, the probabilities for each of the outcomes are found to be $p(-|\alpha) = \mathrm{Tr}(\Pi_- \rho_\alpha) = \frac{2j}{2j+1}\sin^2(\alpha/2)$ and $p(+|\alpha) = 1 - p(-|\alpha)$. We again consider two possible priors over α.

[4] This measurement is identical to the one for optimal programmable measurements, developed using similar techniques.

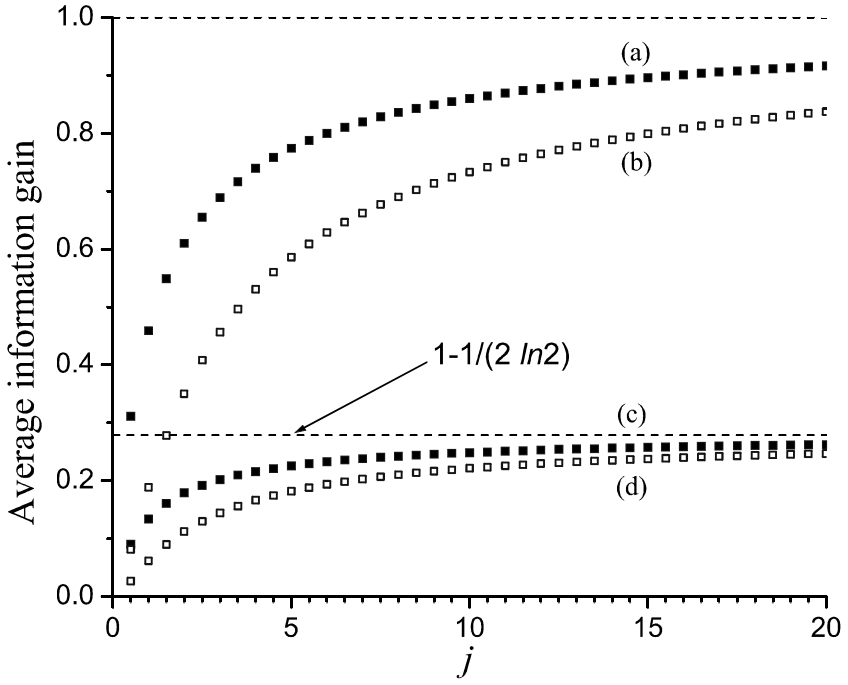


Figure 2: Average information gain for measurements on a spin-1/2 system and a spin-j system. The curves (a),(b) correspond to the optimal measurement and the optimal local measurement for the case when the spins are prepared parallel or antiparallel with equal probability. The curves (c),(d) correspond to the optimal measurement and the optimal local measurements for the case when the initial direction of each spin is chosen uniformly from the sphere.

Following the same steps as before, for a uniform prior, the average information gain can be derived as a function of j; the result is curve (c) of Fig. 2. In the limit $j \to \infty$, we find $I_{\rm av} = 1 - (2\ln 2)^{-1} \simeq 0.2787$ bits, which is precisely the information gain for the optimal measurement of the angle of a spin-1/2 system relative to a classical direction given a uniform prior over spin directions [10].

3.6.3 Optimal local measurements

Consider again the simplest case of a pair of spin-1/2 systems. The optimal measurement in this case was found to be the POVM $\{\Pi_A, \Pi_S\}$. This measurement cannot be implemented by local operations on the individual systems because Π_A is a projector onto an entangled state. In general we want to show that the measurements discussed above are not implementable locally, but that in the limit of one spin becoming classical the optimal local (separable) measurements are as good as the optimal joint measurements. This intuition is, in fact, borne out by the detailed calculations - which can be found in the paper. The average information gain achieved by the best local measurement, as a function of j, is plotted as curves (b) and (d) of Fig. 2. Note that the optimum *can* be achieved by LOCC measurements in the limit $j \to \infty$.

3.6.4 Discussion

We now briefly discuss some other relative parameter estimation tasks for which our result provides the solution. The case we have yet to address is the estimation of the angle between a spin-j_1 and a spin-j_2 system, both in SU(2) coherent states, for arbitrary j_1, j_2. Assuming $j_2 \geq j_1$, the optimal measurement is the $(2j_1 + 1)$-element projective measurement which projects onto the subspaces of fixed total angular momentum J. The posterior distributions over α and the average information gain can be calculated in the same manner as before, although in this case they are substantially more complicated. However, in the limit $j_2 \to \infty$, the Clebsch-Gordon coefficients simplify, and one can show that the probability of a measurement outcome J approaches the probabilities obtained using the Born rule for a projective measurement along the classical direction defined by the spin-j_2 system. As a result, the posterior distribution for any measurement result will agree with what would be obtained classically, regardless of the prior over α. If, in addition, we take $j_1 \to \infty$, the information gain for α becomes infinite (for any prior distribution) and thus α can be inferred with certainty from the measurement result, as expected for a measurement of the angle between two classical directions. Our results also indicate that, in the classical limit, a measurement of the magnitude of total angular momentum should be sufficient to estimate the relative angle, which is indeed the case if the magnitude of each spin is known.

It should be noted that estimating the relative angle between a pair of SU(2) coherent states is of particular importance because estimating the eccentricity of an elliptic Rydberg state of a Hydrogen atom is an instance of the same problem [**?**]. Rydberg states are significant as they can be prepared experimentally.

Our results imply that an optimal estimation of eccentricity is in fact straightforward to achieve experimentally because it involves only a measurement of the magnitude of the total angular momentum of the atom.

Our results are also applicable to systems other than spin. For example, for *any* realization of a pair of 2-level systems (qubits), the degree of nonorthogonality between their states (measured by, say, the overlap $|\langle\psi_1|\psi_2\rangle|$) is invariant under global transformations and is thus a relative parameter. Our measurement is thus optimal for estimating this nonorthogonality.

In addition to solving various estimation problems, we have shown that a macroscopic spin in the appropriate limit is equivalent to a classical external RF as far as relative parameter estimation is concerned. This result suggest that it may be possible to express all measurements (and possibly all operations) in a covariant, relative framework that respects the underlying symmetries of the theory. Such a framework is necessary if one wishes to abide by the principle, which has been so fruitful in the study of space and time but has yet to be embraced in the quantum context, that all degrees of freedom must be defined in terms of relations.

There remain many important questions for future investigation. While we have focussed on estimating relative parameters of product states, one can also consider relative parameters of entangled states, and here the landscape becomes much richer. For instance, for a pair of spin-1/2 systems, while the set of product states supports a single relative parameter, the set of all two-qubit states supports three: the angle between the spins in a term of the Schmidt decomposition [10], the phase between the two terms of this decomposition, and the degree of entanglement between the spins. Our measurement scheme is optimal for estimating these relative parameters as well. Given the significance of entanglement for quantum information theory, there is likely much to be learned from investigations of other sorts of relative quantum information.

3.7 State Targeting

We have undertaken an exhaustive study of state targeting. Like state estimation it is a primitive of quantum communication. State targeting is important for analyzing the options available to the *sender* of quantum systems - it is dual to the primitive of state estimation which is important for the receivers of quantum systems. To introduce them, consider the following: The communication starts with Alice submitting a quantum system to Bob. Eventually, Bob either tests the system for being in state $|\psi_0\rangle$ or else tests the system for being in state $|\psi_1\rangle$ (where these are not necessarily orthogonal). It is assumed that Alice at some point learns which state she would prefer to convince Bob that she submitted. We refer to this preferred state as the *target state*. The problem (from Alice's perspective) is that she must submit the system to Bob prior to knowing the identity of the target state. It is assumed that Alice has the freedom of telling Bob which state he is to test for, but that she may sometimes prefer to pass a test for the non-target state rather than failing the test for the target state. As such, she does not always ask Bob to test for the target state.

More precisely, consider for the moment the following two scenarios:
Scenario 1
(i) Alice submits a system to Bob.
(ii) Alice learns the identity of the target state.
(iii) Alice announces a state to Bob (not necessarily the target state).
(iv) Bob performs a Pass/Fail test for the announced state on the system Alice submitted.
Scenario 2

This is the same as Scenario 1, except that Alice has the option of declining from announcing a state to Bob, in which case no test is performed. more precisely, the difference from Scenario 1 is that step (iii) must be replaced by:
(iii′) Alice has the option of either (a) announcing a state to Bob (not necessarily the target state), or (b) declining to announce a state to Bob.

Scenarios 1 and 2 are quite generic to analyses of quantum communication between antagonistic parties. The option (b) to "decline" at step (iii′) of Scenario 2 is analogous to the "inconclusive" result in unambiguous state discrimination.

Heuristically then, Alice's *control* (the quantity similar to *information gain* in state estimation) quantifies the extent to which she can convince Bob that a system is in a particular state (by passing the test at step (iv)), given that she must submit the system to him (step (i)) prior to her learning (at step (ii)) which state it is most advantageous for her to convince Bob she submitted. We quantify the control by the average probability that Alice succeeds. Her *maximum control* is simply the maximum value of this average probability in a variation over all strategies available to Alice. Alice's *unambiguous control* quantifies the largest probability of success she can achieve, subject to the constraint that she runs exactly zero risk of failing Bob's test. In general, one would like to determine the most control that Alice can achieve for a given probability of failing Bob's test. When considered as a function of the probability of failing Bob's test, this yields a monotonic function; thus it also specifies the minimum probability of failing Bob's test for a given control.

It is most common to consider versions of Scenarios 1 and 2 where the tests which Bob performs are for *pure* states. A more subtle, and much more powerful, version of these scenarios can involve Bob's tests being for mixed states. In particular, we envision in these more general scenarios that Alice initially prepares an entangled state over two systems, such that the initial system she sends Bob is in a certain mixed state. At step (iii) she may then be required to also submit the other half of the entangled state, and Bob's test is performed on the composite system. We have analyzed this mixed state scenario in detail. What we know about control between two mixed states ρ_0, ρ_1 and the

equivalent state estimation quantities can be summarized:

$$\begin{aligned}
\text{Maximum Control} &: (1 + F(\rho_{0,}\rho_1))/2 \\
\text{Maximum Info. Gain} &: (1 + D(\rho_{0,}\rho_1))/2 \\
\text{Unambiguous Control} &: \frac{1}{1+\sqrt{1-F(\rho_{0,}\rho_1)\hat{}2}} \leq ?? \leq 1 - \frac{1}{2}D(\rho_{0,}\rho_1) \\
\text{Unambiguous Discrimination} &: \text{In progress (see below)}
\end{aligned}$$

Here D denotes the trace distance, while F denotes (Uhlmann's) fidelity.

It is interesting to note that the maximum information gain possible for distinguishing two mixed states is given by $\frac{1}{2}D(\sigma_0, \sigma_1)$. The above equation implies that the maximum control is given by $\frac{1}{2}F(\sigma_0, \sigma_1)$. Although the trace distance and fidelity are known to be closely related mathematical measures of distinguishability for mixed states, the former is generally presumed to be much better operationally motivated because of its connection to state estimation. This result on maximum control can be interpreted as providing a simple and physically well motivated quantification of the fidelity and its relationship to the trace distance.

References for comm. complexity of establishing SRF:

References

[1] E. Wigner, Rev. Mod. Phys. **29**, 255 (1957); Y. Aharanov and T. Kaufherr, Phys. Rev. D. **30**, 368 (1984).

[2] T. Rudolph, quant-ph/9902010;

[3] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[4] R. Derka *et al*, Phys. Rev. Lett. **80**, 1571 (1998); J. I. Latorre *et al*, Phys. Rev. Lett. **81**, 1351 (1998).

[5] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).

[6] S. Massar, Phys. Rev. A. **62**, R040101 (2000).

[7] E. Bagan *et al*, Phys. Rev. Lett. **85**, 5230 (2000); A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001); E. Bagan *et al*, Phys. Rev. Lett. **63**, 052309 (2001); A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901(2001); E. Bagan *et al*, Phys. Rev. Lett. **87**, 257903 (2001).

[8] E. Bagan, quant-ph/0106155.

[9] S. Bartlett, T. Rudolph and R. Spekkens, Phys. Rev. Lett. **89**, 227901 (2001).

[10] Asher Peres, private communication.

[11] E. Schrödinger. *Proc. Camb. Phil. Soc.*, 31:555, 1935; *Proc. Camb. Phil. Soc.*, 32:446, 1936.

[12] A. Acin, E. Jane and G. Vidal, quant-ph/0012015.

[13] L. Grover, Phys. Rev. Lett. **78**, 325 (1997).

[14] R. Cleve *et al*, Proc. R. Soc. London A. **454**, 339 (1998).

[15] A. Kitaev, quant-ph/9511026.

[16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information,* (Cambridge University Press, Cambridge, 2000).

Unruh References:

References

[1] A. Peres, P.F. Scudo, and D.R. Terno, Phys. Rev. Lett. **88**, 230402 (2002).

[2] S.J. van Enk, `quant-ph/0206135`.

[3] W.G. Unruh, Phys. Rev. D **14**, 870 (1976); W.G. Unruh and R.M. Wald, Phys. Rev. D **29**, 1047 (1984).

[4] J. Audretsch and R. Müller, Phys. Rev. D **49**, 4056 (1994).

[5] B. Reznik, `quant-ph/0008006`.

[6] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett., **70**, 1895 (1993).

[7] A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science **282**, 706 (1998).

[8] S.L. Braunstein and H.J. Kimble, Phys. rev. Lett. **80**, 869 (1998).

[9] D.N. Klyshko, Phys. Lett. A **154**, 433 (1991).

[10] S.J. van Enk, J. Mod. Optics **48**, 2049 (2001).

[11] R.W. Spekkens and Terry Rudolph, Phys. Rev. A. **65**, 012310 (2002).

[12] S.J. Summers and R. Werner, J. Math. Phys. **28**, 2440 (1987); *ibidem* **28**, 2448 (1987).

References for Communication without SRF's

References

[1] R. Jozsa and N. Linden, quant-ph/0201143.

[2] A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001); E. Bagan *et al*, Phys. Rev. A. **63**, 052309 (2001).

[3] A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901 (2001); E. Bagan *et al*, Phys. Rev. Lett. **87**, 257903 (2001).

[4] E. Wigner, Rev. Mod. Phys. **29**, 255 (1957).

[5] E. P. Wigner, Z. Physik **131**, 101 (1952); H. Araki and M. M. Yanase, Phys. Rev. **129**, 622 (1960).

[6] T. Rudolph, quant-ph/9902010; A. Acin *et al*, Phys. Rev. A. **64** 050302(R) (2001).

[7] M. Dickson, quant-ph/0102053.

[8] Y. Aharonov and L. Susskind, Phys. Rev. **155**, 1428 (1967).

[9] S. van Enk, J. Mod. Opt. **48**, 2049 (2001).

[10] D. Bacon *et al*, Phys. Rev. Lett. **85**, 1758 (2000).

[11] J. Kempe *et al*, Phys. Rev. A. **63**, 042307 (2001).

[12] A. Einstein, B. Podolsky, and N. Rosen. Phys. Rev., **47**, 777–780, 1935.

[13] E. Schrödinger. Proc. Camb. Phil. Soc., 31:555, 1935; Proc. Camb. Phil. Soc., 32:446, 1936.

[14] L.P. Hughston, R. Jozsa and W. K. Wootters, Phys. Lett. A. **183**, 14 (1993).

[15] G. Vidal, J. Mod. Opt. **47**(2/3):355–376, 2000.

[16] M.A. Nielsen. Phys. Rev. Lett., **83**:436–439, 1999.

[17] S. M. Barnett, A. Chefles, and I. Jex, Phys. Lett. A **307**, 189 (2003).

[18] Y. Sun, J. Bergou, and M. Hillery, Phys. Rev. A 66, 032315 (2002).

[19] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).

Others

[20] Terry Rudolph and Lov Grover, Communication Complexity of establishing a shared reference frame, Phys. Rev. Lett. **91**, 217905 (2003).

[21] Phys. Rev. Lett. **91**, 027901 (2003)

[22] Phys. Rev. A 68, 010301(R) (2003) .

[23] quant-ph/0310009, Quantum state targeting Terry Rudolph and Robert W. Spekkens quant-ph/0310060 (accepted to Phys. Rev. A.)

4 Quantum Gates and Implementations

In this section we outline several directions in which we are trying to push the boundaries of our understanding about what is necessary versus what is sufficient to obtain the extra power of quantum computation [1]. In particular we are interested in whether we need the full power of the standard model of non-relativistic quantum mechanics to simulate any quantum computation and the extent to which coherent quantum processes can be replaced by incoherent ones while retaining the full strength of standard quantum computation. We have also examined alternative schemes for linear optics quantum computation, designed to drastically reduce the number of optical components and mode-matched interactions required.

4.1 A rebit gate for quantum computing

It is interesting, and presumably of practical importance, that the requirements of universal quantum computing are in some sense weaker than the requirements of non-relativistic quantum mechanics. This was originally shown within the quantum Turing machine model [2]. In effect it was shown that a quantum Turing machine can operate in a *real* Hilbert space.

In general quantum computation is approached more commonly through the circuit model (the quantum Turing machine model is not intuitive for constructing useful quantum devices or algorithms.) When evaluating a new proposal for implementing quantum computation, the standard procedure is to check whether one can perform (i) a controlled-NOT gate between two qubits, and (ii) arbitrary single qubit unitary transformations. If so, then universal quantum computing is certainly possible, since we can perform arbitrary unitary operations by combinations of these gates. In accordance with the result on quantum Turing machines however, one should expect that the set of requirements (i) and (ii) is too stringent.

We have recently constructed a simple scheme for mapping generic quantum algorithms (such as Shor's) which use complex amplitudes, to algorithms requiring only real amplitudes. Our investigations have shown that there exists a two-qubit gate which is universal for quantum computing *even though it cannot be used to build up arbitrary unitary transforms.* This implies that the practical requirements for implementing a universal quantum computer can be simplified from those currently considered essential.

Our scheme revolves around showing how any quantum computation can be simply translated into a quantum circuit in which all quantum states and gates are real. In particular showed that the following two qubit gate (written in the computational basis) is universal for quantum computing:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & -\sin\phi \\ 0 & 0 & \sin\phi & \cos\phi \end{pmatrix}, \tag{8}$$

where ϕ is some irrational multiple of π. Note that this gate does *not* allow arbitrary unitary operations to be performed, as can be easily deduced from the fact that the matrix entries are real - and thus it can only produce superpositions of states with real amplitudes. In other words, such a gate cannot in fact evolve us through much, in fact most, of an n qubit Hilbert space, but is still universal for quantum computing.

A key idea to show the universality of G, is to show how any quantum computation which uses complex amplitudes, can be replaced by one which is as efficient (in the complexity theoretic sense), but which makes use of only real amplitudes. To do this, imagine the standard quantum algorithm involves the creation at some point of the state:

$$|\psi\rangle = \sum_j r_j e^{i\theta_j} |j\rangle . \tag{9}$$

If we introduce an ancilla 2-level qubit, the orthonormal states of which we label $|R\rangle$ and $|I\rangle$, then an equivalent state for the purposes of quantum computing is

$$|\psi_E\rangle = \sum_j r_j \cos\theta_j |j\rangle |R\rangle + r_j \sin\theta_j |j\rangle |I\rangle . \tag{10}$$

The purpose of the two-level "R-I" ancilla bit is to keep track of Real and Imaginary parts of the amplitudes which appear in (9). We will use the terminology that the state (10) is the *encoded form* of (9). Note that the probability of obtaining the state $|j\rangle$, upon a measurement in the computational basis, is r_j^2 for both $|\psi\rangle$ and $|\psi_E\rangle$, and of course the amplitudes of $|\psi_E\rangle$ are real.

We showed that if an efficient algorithm is implemented such that our standard quantum computer now undergoes an evolution

$$|\psi\rangle \to |\psi'\rangle = \sum_j r'_j e^{i\theta'_j} |j\rangle ,$$

then an efficient set of gates built from G can be found such that

$$|\psi_E\rangle \to |\psi'_E\rangle = \sum_j r'_j \cos\theta'_j |j\rangle |R\rangle + r'_j \sin\theta'_j |j\rangle |I\rangle .$$

Such considerations may be useful for practical implementations, as well as for probing the more interesting questions about precisely where quantum computers gain their power and to what extent the standard complex Hilbert space formulation of quantum mechanics can actually be argued as necessary as opposed to merely sufficient.

4.2 Quantum computing with the Zeno effect

Performing universal quantum computation is generically equated with the ability to build up arbitrary unitary transformations on a large number of qubits out of a set of unitary transformations that act on a small number of qubits

at a time. As such, the primary challenge of building a quantum computer is most often considered to be finding quantum systems with appropriately controllable Hamiltonians, such that the desired unitary evolution is obtained to within some small error.

While this standard paradigm certainly enables universal quantum computing, recent results have shown that it is not necessary that the computation be built up in such a way. In particular it has been shown that we can often replace the 'hard' parts of a quantum computation (generally the 2 qubit interaction) by using measurements and appropriately prepared ancilla states. In particular, Gottesman and Chuang [3] showed that teleportation is such a universal computational primitive. Recently some beautiful ideas for implementing quantum computation by performing measurements on appropriately prepared ancilla states have been presented [4], these latter schemes are remarkable in that they require no coherent (unitary) evolution during the computation at all.

By coupling an idea of Paul Kwiat's with an idea of ours (which originated in the work on quantum searching a classical database, Section 2.1.4 of this report), we have shown that a two outcome projective measurement

$$P_1 = |0\rangle\langle 0| + |1\rangle\langle 1|, P_2 = I - |0\rangle\langle 0| + |1\rangle\langle 1| = \sum_{n=2}^{\infty} |n\rangle\langle n|$$

on a single harmonic oscillator mode can act as quantum computational primitive, which, along with easily implemented single qubit unitary transformations, enables us to perform universal quantum computation. In contrast with the aforementioned schemes, we need make no use of prepared ancilla states. Instead we use the quantum Zeno effect in such a way that a series of measurements approximate a useful unitary evolution.

As an abstract mathematical result this is perhaps not particularly interesting. However our scheme allows for the P_2 outcome to be destructive - that is, it absorbs the quanta involved. This is somewhat surprising, since one normally expects that such processes will result in loss of the quantum systems which are being used in the computation.

Fig.3. is a schematic showing how to use an interaction free measurement to turn the incoherent projective measurement P_1, P_2 into a coherent gate. The black box labelled A consists of a balanced Mach-Zender interferometer, with a measurement of P_1, P_2 in both of its arms. (If two photons are incident on a beamsplitter then the output state is $|2,0\rangle + |0,2\rangle$. Thus a measurement of P_1, P_2 in both outputs will certainly give the absorptive outcome P_2 in one output. If one photon, or the vacuum, is initially present then the non-destructive outcome P_1 will occur in each arm. In effect the box A absorbs the target photon if and only if the control photon is present.) The target photon enters at the switchable mirror M1. It passes through a weakly reflecting beam splitter, of reflectivity $\sin^2\theta = \pi/N$. If the control photon is present, then it collapses onto the path which doesn't contain A; if the control photon is not present then the target proceeds through the interferometer coherently. The photons are cycled

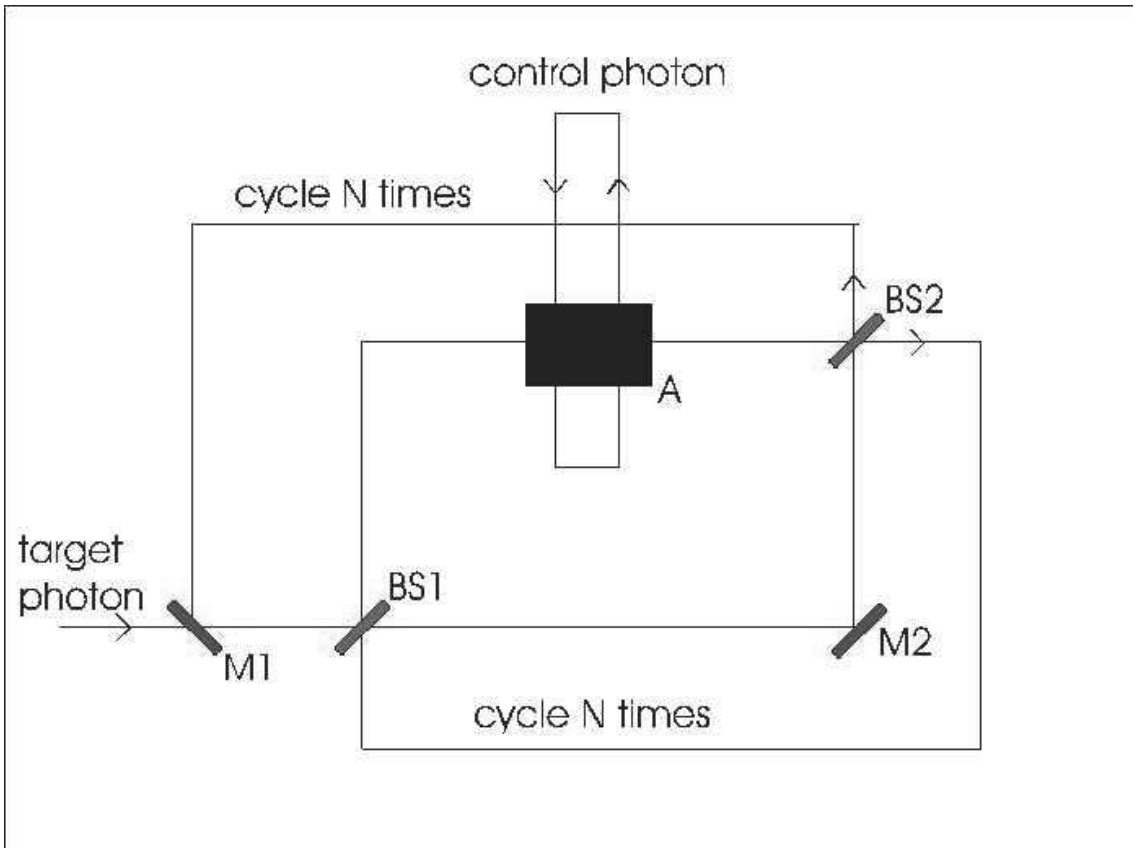


Figure 3: By using interaction-free measurements, it is possible to use an absorbing process to achieve quantum computation

N times; by choosing N large enough we can make the probability of failure as small as we wish. It can be shown that this process implements the following two qubit gate:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

This gate coupled with single qubit transformations suffices for quantum computing.

Thus our results show that *absorptive* nonlinear processes can be used to perform useful quantum computation.. As a simple example of why this can be of practical significance, let us think for the moment in terms of photonic qubits. The interaction strength between two photons is very weak (of order $\frac{1}{137^8}$), unless we make use of some nonlinear media. Even with such a medium however, if we limit our considerations to non-resonant (dispersive) interactions then they are still not particularly strong. The primary reason we would limit ourselves to non-resonant interactions however, is simply that resonant ones (which are orders of magnitude stronger) are going to cause absorptive loss of the photons with which we are trying to compute. However using our scheme, although the interaction is incoherent, they are not lost to the computation.

Although phrased in terms of photons, our ideas apply quite generally. As such, we are currently working with our experimentalist colleagues at Bell Labs to think of systems in which strong nonlinear effects are observed at the single quantum level. Almost any system with a strong nonlinearity will suffice. (A preprint is available.)

4.3 Linear optical quantum computation the easy way

Knill, Laflamme and Milburn made the exciting discovery that quantum computation is possible using linear optics, single photon sources and photodetectors. The particular constructions they gave were quite inefficient in terms of resources required, their construction also required particular ancillas and gates that, due to the large number of mode combinations required, would present an experimentalist with a scary set of mode-matching problems to solve.

Following an idea of Michael Nielsen's, we have looked at alternative methods for LOQC, in particular schemes for building up optical versions of Raussendorf and Briegel's cluster states. Our analysis has shown that *almost any* two photon gate is universal for quantum computing.

We imagine that some non-deterministic gate implements a nontrivial (i.e. non-factorizable) unitary transformation U on the state of two photons with probability p. For simplicity, but without loss of generality, we will phrase our discussion in terms of the polarization degree of freedom. We will not be concerned with how such a transformation U is constructed - in general it may use several ancillary photons and interferometers of varying degrees of complexity. All that is important is that the implementation of U is performed

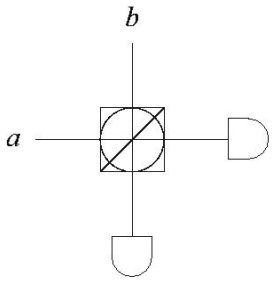


Figure 4: Parity Gate.

in a *classically feed-forwardable* manner. By this we mean that the information as to whether the gate succeeded or not is available, and thus can be used to condition future operations within the quantum computer. Such a gate was recently demonstrated by the group of Anton Zeilnger.

As is well known, a controlled-NOT operation can be built (with sufficient precision) by the implementation of some fixed number of U operations, combined with single qubit transformations. The latter are easily performed deterministically with linear optics. Thus, any non-trivial gate U can be used to build a controlled-NOT gate that succeeds with probability p^k for some fixed k.

Give such a controlled-NOT operation, we can use it twice to create GHZ states of three photons in different spatial modes:

$$|GHZ\rangle = \tfrac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right).$$

It is these states which will be our critical resource from which we can very simply construct cluster states. The crucial operation we will use to exploit this resource is the nondeterministic *parity measurement* on two photons. The parity measurement is extremely simple - it consists of a polarizing beamsplitter oriented at 45°. It can be understood by observing how each of the four basis states evolves through such a beamsplitter:

$$\begin{aligned}
|HH\rangle &\Rightarrow \tfrac{1}{2}|HH\rangle + \tfrac{1}{2}|VV\rangle + |\chi_{-+-+}\rangle \\
|HV\rangle &\Rightarrow -\tfrac{1}{2}|HV\rangle - \tfrac{1}{2}|VH\rangle + |\chi_{-++-}\rangle \\
|VH\rangle &\Rightarrow -\tfrac{1}{2}|HV\rangle - \tfrac{1}{2}|VH\rangle + |\chi_{+--+}\rangle \\
|VV\rangle &\Rightarrow \tfrac{1}{2}|HH\rangle + \tfrac{1}{2}|VV\rangle + |\chi_{+-+-}\rangle .
\end{aligned}$$

The subscripts on the states $|\chi\rangle$ refer to the phases in a superposition of four states, a characteristic example being:

$$\left|\chi_{-+-+}\right\rangle \equiv \tfrac{\sqrt{2}}{4}\left(-\left|2_H,0\right\rangle+\left|2_V,0\right\rangle-\left|0,2_H\right\rangle+\left|0,2_V\right\rangle\right).$$

In this expression the state $|2_H,0\rangle$ denotes the Fock state with two horizontally polarized photons in spatial mode 1 and no photons in spatial mode 2.

We see, therefore, that if a (polarization sensitive) measurement is made on the output modes from the beamsplitter, and one photon is found per mode, then the gate succeeds (this occurs with probability 1/2) - realizing a degenerate parity measurement on the input photons. If, however, two photons are detected in one output spatial mode, then the gate has failed, and the computational states pick up the positive or negative phases easily determined from examining the states $|\chi\rangle$. Such a measurement has the advantage that it does not need detectors with the ability to explicitly count photons (presuming good single photon sources are available) in order to determine the form of the failure outcome. This could have significant practical significance.

It is simple to see that, given a resource of three photon GHZ states, we can efficiently stitch them together with parity measurements into larger GHZ states of the form $|GHZ_m\rangle = \frac{1}{\sqrt{2}}(|H^m\rangle + |V^m\rangle))$, where we use the notation that a tensor product of m horizontally polarized photons in different modes is written H^m.

To produce the cluster states discussed above, we will use multiple photons to encode each abstract qubit within the cluster state:

$$|0\rangle \Leftrightarrow |H^m\rangle, \quad |1 \Leftrightarrow |V^m\rangle.$$

Let us illustrate the basic idea by imagining that we have a cluster, and wish to add a single qubit to it. The initial state of the cluster may be written

$$|X_0\rangle|H^m\rangle + |X_1\rangle|V^m\rangle,$$

where we have singled out on the right the m photons encoding the qubit of the cluster to which the bond will be made (the "source" qubit). The n photons corresponding to the isolated qubit which will be added to the cluster (the "target qubit") begin in the state $|GHZ_n$ - this is the encoded version of the state $|+$ mentioned in the introduction. To make the desired bond, we wish to achieve an evolution of the form (ignoring normalization)

$$\begin{aligned}&(|X_0\rangle|H^m\rangle + |X_1\rangle|V^m\rangle)(|H^n\rangle + |V^n\rangle)\\ &\Rightarrow |X_0\rangle|H^{m'}\rangle|H^{n'}\rangle + |X_0\rangle|H^{m'}\rangle|V^{n'}\rangle + |X_1\rangle|V^{m'}\rangle|H^{n'}\rangle\\ &- |X_1\rangle|V^{m'}\rangle|V^{n'}\rangle,\end{aligned}$$

where the primes on the m,n indicate that some photons will be destroyed in the process of making the bond.

To achieve this evolution, consider implementing the following steps:

(i) Apply a Hadamard rotation (quarter wave plate) to one photon of the n photons encoding the target qubit.

(ii) Perform a parity measurement between this photon, and one photon of those encoding the source qubit.

(iii) If the parity measurement succeeds, then the bond is formed. If the measurement fails, then repeat the process with a new set of photons $|GHZ_n\rangle$.

The crucial aspect of a failure outcome in the above procedure, is that it leaves the photons in the state

$$(|X_0\rangle|H^{m-1}\rangle \pm |X_1\rangle|V^{m-1}\rangle)|V^{n-1}\rangle$$

Thus, the initial cluster is left essentially unaffected - it has lost only a single photon from one encoded qubit, and has possibly received an (easily correctable) phase error. In the event of a Π_O outcome to the parity measurement, the bond is successful, although a phase error is also obtained. In fact, such phase errors need not be actively corrected for in the photonic cluster state - similar errors form an integral part of a cluster state computation anyway, and such errors can be corrected for by changing some of the single qubit measurements during the actual computation with the cluster state.

It is quite simple to see that if the bond is successful, then another bond can be made between the target qubit and some other state of the cluster using exactly the same procedure of a Hadamard rotation followed by a parity measurement. In all such cases, a failure of the parity measurements leaves the main cluster intact and removes the target qubit.

Such a construction of a cluster state clearly requires only polynomial space and time resources. It should be noted that at the end of the construction the abstract qubits of the original cluster may well be encoded by more than one photon. However the extra photons may be removed by measurements in the $|H\rangle \pm |V\rangle$basis, with only easily correctable phase errors. Several other features of our scheme make it interesting. The primary one is that *melding* of cluster qubits becomes possible, also by a single parity measurement. The melding procedure operates so as to create a nontrivial topology in a small number of steps. It also has the distinct advantage that if a meld fails, then it does not destroy either of the photonic qubits involved in the attempt (unless we have run out of photons in the redundant encoding for these qubits). Thus a failed meld can simply be re-attempted.

References

[1] A 2 rebit gate universal for quantum computing,Terry Rudolph, Lov Grover, quant-ph-0210187.

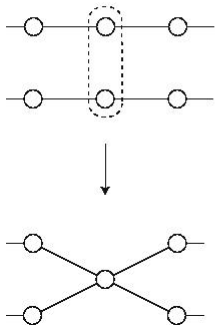


Figure 5: Cluster gates can simulate unitary evolution merely through appropriately chosen projective measurements.

[2] Quantum Computability, SIAM Journal on Computing, Volume 26 , Issue 5 (October 1997), pp 1524 - 1540,1997, Leonard M. Adleman , Jonathan DeMarrais , Ming-Deh A. Huang

[3] Quantum Teleportation is a Universal Computational Primitive, Daniel Gottesman, Isaac L. Chuang, quant-ph/9908010.

[4] Robert Raussendorf and Hans J. Briegel Physical Review Letters – May 28, 2001 – Volume 86, Issue 22, pp. 5188-5191, A One-Way Quantum Computer.

5 Papers that appeared during this period

- L. K. Grover, "Quantum computers can search rapidly by using almost any transformation", Phys. Rev. Letters, 80(19), 1998, 4329-4332; Proc. 30th ACM Symposium on Theory of Computing (STOC), 1998, 53-63, quant-ph/9712011.
- How fast can a quantum computer search?, Lov K. Grover, http//xxx.lanl.gov/quant-ph/9809029.
- L. K. Grover, "Quantum computing: The advantages of superposition", Science 280, 5361, 228 (1998).
- L. K. Grover, "Quantum computing: Beyond factorization and search", Science 281, 5378, 792-794 (1998).
- L. K. Grover, "Quantum search on structured problems", in C. P. Williams (ed.), 1st NASA Int. Conf. on Quantum Computing and Quantum Communications (Palm Springs, California, 1998), Lecture Notes in Computer Science 1509, Springer-Verlag, New York, 1999; quant-ph/9802035.
- Quantum Computation - finding important applications and physical systems to realize these, Lov K. Grover, IEEE Potentials, April, 1999.
- Quantum search on structured problems, Lov K. Grover, Chaos, Solitons and Fractals, special issue on quantum computing. Vol. 10, No. 10, 1695-1705, June 1999.
- L. K. Grover, "Synthesis of quantum superpositions by quantum computation", Phys. Rev. Lett. 85, 6, 1334-1337 (2000).
- L. K. Grover, "Rapid sampling through quantum computing", in Proc. of the 32nd Annual ACM Symp. on Theory of Computation (2000); quant-ph/9912001.
- L. K. Grover, "Searching with quantum computers", quant-ph/0011118, introductory article, published in Dr. Dobb's Journal.
- L. K. Grover, "From Schrödinger's equation to the quantum search algorithm", Am. J. Phys. 69, 7, 769-777 (2001); quant-ph/0109116.
- L. K. Grover and Anirvan Sengupta, From coupled pendulums to quantum searching, Mathematics of Quantum Computation, pages 119-134, CRC Press, 2002quant-ph/0109123..
- L. K. Grover and Anirvan Sengupta, A Classical Analog of Quantum Search, Phys Rev A 65 032319 (2002)
- L. K. Grover, "Trade-offs in the quantum search algorithm, Phys. Rev. A 66, 052314 (2002)..

- L. K. Grover, "Quantum computation and quantum information, Am. J. Phys. 70, 5, 558-559 (2002). Review of [Nielsen-Chuang 00].
- L.K. Grover and T. Rudolph, "Creating superpositions that correspond to efficiently integrable probability distributions", quant-ph/0208112.
- T. Rudolph and L. K. Grover, "Quantum searching a classical database (or how we learned to stop worrying and love the bomb)", quant-ph/0206066.
- Lov Grover and Terry Rudolph, A 2 rebit gate universal for quantum computing, quant-ph/0210187.
- Terry Rudolph and Lov Grover, Communication Complexity of establishing a shared reference frame, Phys. Rev. Lett. **91**, 217905 (2003).
- L. K. Grover and Terry Rudolph, "How significant are known algorithms for collision finding & element distinctness?", quant-ph, Sep. 12, 2003, Vol. 4, No.3, May 30, 04, pp201-206, Quantum Information & Computation, QIC031008.
- L. K. Grover, A new quantum scheduling algorithm, Bell Labs TM, International Journal on Foundations of Computer Science, Vol. 14, no. 5, October 2003, quant-ph/0202033.

Terry Rudolph's publications

- *Creating superpositions that correspond to efficiently integrable probability distributions*, Lov Grover and Terry Rudolph, quant-ph/0208112.
- *Constructing physically intuitive graph invariants* Terry Rudolph, quant-ph/0206068.
- *Complete eigenstates of N identical qubits arranged in regular polygons,* Terry Rudolph, Itay Yavin and Helen Freedhoff, quant-ph/0206067.
- *Quantum searching a classical database (or how we learned to stop worrying and love the bomb)* Terry Rudolph and Lov Grover, quant-ph/0206066.
- *The laws of physics and cryptographic security* Terry Rudolph, quant-ph/0202143.
- *A quantum protocol for cheat-sensitive weak coin flipping*, Rob Spekkens and Terry Rudolph, quant-ph/0202118. (To be published in Phys. Rev. Lett.)
- *Degrees of Concealment and Bindingness in Quantum Bit Commitment Protocols*, Rob Spekkens and Terry Rudolph, quant-ph/0106019, Phys. Rev. A. **65**, 012310 (2002).
- *Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol*, Rob Spekkens and Terry Rudolph, quant-ph/0107142, Journal Quantum Information & Computation , **2**, 66 (2002).

- *A simple gate for linear optics quantum computing*, T. Rudolph and J.-W. Pan, quant-ph/0108056.
- *Requirement of Coherence for Continuous Variable Teleportation*, Terry Rudolph and Barry Sanders, Phys. Rev. Lett. **87**, 077903 (2001).
- *Quantum information processing in localized modes of light within a photonic band-gap material*, Nipun Vats and Terry Rudolph, J. Mod. Opt. **48** 1495-1502 (2001).
- *Better schemes for Quantum Interrogation in lossy experiments*, T. Rudolph, Phys. Rev. Lett. **85**, 2925-2928 (2000).
- "Classical and quantum communication without shared reference frames," Terry Rudolph and RW Spekkens,(2003)Phys. Rev. Lett. **91**, 027901 (2003)·
- Unambiguous discrimination of mixed states, Terry Rudolph, Robert W. Spekkens, and Peter S. Turner, Phys. Rev. A 68, 010301(R) (2003) (4 pages)

6 Personnel Supported

Visitors are essential for maintaining a lively exchange of ideas for which it is very helpful to have the NSA/ARO grant. Please see the interim reports for a year by year list of the short-term and long-term vistors.

6.1 Lov K. Grover

He is the main researcher in this program. As mentioned in the text of this report, he has pioneered some of the ground-breaking recent concepts in quantum computation. In recognition of his achievements, in 2002 Bell Labs promoted him to a Distinguished Member of Technical Staff. He has been at Bell Labs, Murray Hill since 1994. Prior to that he was a faculty member in the School of Electrical Engineering at Cornell University. He got his Ph.D. in Electrical Engineering and an M.S. in Physics from Stanford University in 1984 and an M.S. in Electrical Engineering from Caltech in 1982. He got his B. Tech. in Electrical Engineering from IIT (Indian Institute of Technology, New Delhi, India) in 1981.

6.2 Terry Rudolph

Dr. Rudolph was a post-doctoral fellow at Bell Labs. He is a theoretician most recently from the Institute for Experimental Physics at the University of Vienna. Prior to that he was a faculty member at the University of Toronto. Dr. Rudolph completed his PhD in 1998 (at age 24), in the field of theoretical quantum optics. He still collaborates intensively with members of the experimental quantum optics community on problems associated to practical implementations of quantum computing. Within the field of quantum information, Dr. Rudolph has authored over ten papers, and is particularly known for his fundamental work on two-party quantum cryptographic protocols. In his keynote address at the Workshop on Quantum Computing in Huangshan, China in Sep. 2001, Charlie Bennett prominently referred to him as *the world's leading expert on direction finding.* He spent the period from Nov. 2001 through Sep. 2003 at Bell Labs. He has recently moved to Imperial College, London, as a faculty member. He continues to interact with researchers at Bell Labs and visits several times a year.

6.3 Hein Roehrig

Hein was a Ph.D. candidate in computer science at CWI, Netherlands and is a regular visitor to Bell Labs. He is originally from Germany and was sponsored by the German foundation Studienstiftung des Deutschen Volkes. He was at Bell Labs for a period of 11 months April, 1999 - March, 2000, for a 2 month period during the summer of 2000 (May - August) and again in 2003 and 2004. He successsfully completed his Ph.D. in December 2003 and is presently a post-doctoral fellow in the Universsity of Calgary, Canada.