Quantum Communication Complexity with Coherent States and Linear Optics

Juan Miguel Arrazola[1] and Norbert Lütkenhaus[1,2]

1 **Institute for Quantum Computing, University of Waterloo**
200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada
2 **Department of Physics and Astronomy, University of Waterloo**
200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada

Abstract

We introduce a general mapping for encoding quantum communication protocols involving pure states of multiple qubits, unitary transformations, and projective measurements into another set of protocols that employ coherent states of light in a superposition of optical modes, linear optics transformations and measurements with single-photon threshold detectors. This provides a general framework for transforming a wide class of protocols in quantum communication into a form in which they can be implemented with current technology. In particular, we apply the mapping to quantum communication complexity, providing general conditions under which quantum protocols can be implemented with coherent states and linear optics while retaining exponential separations in communication complexity compared to the classical case. Finally, we make use of our results to construct a protocol for the Hidden Matching problem that retains the known exponential gap between quantum and classical one-way communication complexity.

1998 ACM Subject Classification J.2 Physics, E.4 Formal Models of Communication

Keywords and phrases Quantum Communication Complexity, Quantum Optics

Digital Object Identifier 10.4230/LIPIcs.TQC.2014.36

1 Introduction

What information-processing tasks are unachievable in a classical world but become possible when exploiting the intrinsic quantum mechanical properties of physical systems? This question has been a driving force of numerous research endeavours over the last two decades and remarkable progress has been made in our understanding of the advantages that quantum mechanics can provide, as well is in developing the experimental platforms that will allow them to be realized in practice [18, 7, 13, 22]. An example pertains to the field of quantum communication [14], where quantum systems can be used, for instance, to distribute secret keys [4, 5] or reduce the amount of communication required for joint computations [8, 9, 19, 2].

In terms of experimental implementations, only quantum key distribution (QKD) has been routinely demonstrated and deployed over increasingly complex networks and large distances [24, 21]. This is possible largely due to the fact that, fundamentally, QKD can be carried out with sequences of independent signals and measurements [22]. QKD and other cryptographic applications are easier to implement, as imperfections in implementations only need to be overcome to the point of being able to achieve their qualitative goal.

Other tasks, such as those in quantum communication complexity, face the additional challenge of demonstrating, in practice, their quantitative improvements over classical alternatives. Moreover, many of these tasks require sophisticated quantum states to be transmitted and measured. As such, there is a large set of quantum communication protocols


9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC'14).
Editors: Steven T. Flammia and Aram W. Harrow; pp. 36–47

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

whose potential advantages currently escape the grasp of available technology. Thus, only a few proof-of-principle implementations have been reported [28, 26, 16].

Confronted with these challenges we face two alternatives: We can either strive to improve current technology or we can flip the issue around and ask: Can protocols in quantum communication be adapted to a form that makes them ready to be deployed with available techniques? To adopt the latter strategy is to push for a theoretical reformulation that converts previously intractable protocols into a form that, while conserving their relevant features, eliminates the obstacles affecting their implementation. This is precisely the road that has already been successfully followed for QKD.

In this work, we describe in detail an abstract mapping that converts quantum communication protocols that use pure states of multiple qubits, unitary operations, and projective measurements into another class of protocols that use only a sequence of coherent states, linear optics operations, and measurements with single-photon threshold detectors. The new class of protocols requires a number of optical modes equal to the dimension of the original states, but the number of photons can be chosen freely and is typically very small. This results in the signal states occupying a small Hilbert space, so that they can only be used to transmit the equivalent of a number of qubits that is only logarithmic in the number of modes used. We proceed by examining how the mapping may be generally applied in the context of quantum communication complexity and conclude by illustrating a coherent-state protocol for the Hidden Matching problem.

2 Coherent-state Protocols

We consider a wide class of quantum communication protocols that require only three basic operations: the preparation of pure states of a fixed dimension, unitary transformations on these states, and projective measurements on a canonical basis. This set of protocols is not completely general since we are not accounting for the possibility of shared entanglement or non-unitary evolution, although these extensions could potentially be considered. The simplest form of a protocol in this class is one in which Alice prepares a state $|\psi\rangle$ and sends it to Bob, who then applies a unitary transformation U_B to that state, followed by a projective measurement on the canonical basis. More complex protocols can be constructed by increasing the number of these basic operations as well as the number of parties. Even though these protocols generally involve states of some arbitrary dimension d, we can always think of them as corresponding to a system of $\mathcal{O}(\log_2 d)$ qubits. Hence, we refer to them as *qubit protocols*.

An exact implementation of such protocols can be achieved without the use of actual physical qubits by instead considering a single photon in a superposition of optical modes. Any pure state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$, with $\sum_{k=1}^{d} |\lambda_k|^2 = 1$, can be equally thought of as the state of a single photon in a superposition of d modes

$$a_\psi^\dagger |0\rangle = \sum_{k=1}^{d} \lambda_k |1\rangle_k \,, \tag{1}$$

where $a_\psi^\dagger = \sum_{k=1}^{d} \lambda_k b_k^\dagger$ for a collection of creation operators $\{b_1, b_2, \ldots, b_d\}$ corresponding to d optical modes, and where $|1\rangle_k$ is the state of a single photon in the k-th mode.

In this picture, unitary operations correspond exactly to linear optics transformations, and measurements in the canonical basis are equivalent to a photon counting measurement in each of the modes. From a practical perspective, the issue with implementing qubit protocols in terms of a single photon in a superposition of modes is that the experimental preparation

of these states also presents daunting challenges. Instead, we are interested in an adaptation of this formulation of qubit protocols into another that is more readily implementable in practice.

With this purpose in mind, we outline a method for converting qubit protocols into another class of protocols that, although seemingly disparate, actually retain the essential properties of the original ones. We call these *coherent-state protocols* since they can be implemented by using only coherent states of light and linear optics operations. The recipe for constructing coherent-state protocols is specified by the following rules:

Coherent-state Mapping

1. The original Hilbert space $\mathcal{H}$ of dimension d with canonical basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ is mapped to a set of d orthogonal optical modes with corresponding annihilation operators $\{b_1, b_2, \ldots, b_d\}$:

$$|k\rangle \longrightarrow b_k. \tag{2}$$

2. A state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ is mapped to a coherent state with parameter α in the mode $a_\psi = \sum_{k=1}^{d} \lambda_k b_k$:

$$\begin{aligned} |\psi\rangle \longrightarrow |\alpha, \psi\rangle &:= D_{a_\psi}(\alpha)\,|0\rangle \\ &= \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k\,, \end{aligned} \tag{3}$$

   where $|\alpha\,\lambda_k\rangle_k$ is a coherent state with parameter $\alpha\,\lambda_k$ in the k-th mode. The value of α can be chosen freely but remains fixed.

3. A unitary operation U acting on a state in $\mathcal{H}$ is mapped into linear optics transformation corresponding to the same unitary operator U acting on the modes $\{b_1, b_2, \ldots, b_d\}$. Thus, the transformation of a state is linked to a transformation of the modes as:

$$|\psi'\rangle = U\,|\psi\rangle \longrightarrow \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{pmatrix} = U \begin{pmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_d \end{pmatrix}. \tag{4}$$

4. A projective measurement in the canonical basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ is mapped into a two-outcome measurement in each of the modes:

$$\{|k\rangle\langle k|\} \longrightarrow \{F^k_{\text{no-click}}, F^k_{\text{click}}\}, \tag{5}$$

   where $F^k_{\text{no-click}} = |0\rangle\langle 0|$ is a projection onto the vacuum, $F^k_{\text{no-click}} = \sum_{n=1}^{\infty} |n\rangle_k\langle n|_k$ and $|n\rangle_k$ is a state with n photons in the k-th mode. As such, an outcome in a coherent-state protocol corresponds to a pattern of clicks in the modes. For coherent-state protocols, the observation of N clicks correspond to a particular pattern of N outcomes of a qubit protocol. Thus, an immediate interpretation of the outcomes is not provided by the mapping, but instead must be chosen according to the particular context.

Since any qubit protocol can be constructed from the basic operations of state preparation, unitary transformations, and projective measurements, the above instructions are sufficient to construct the coherent-state version of any qubit protocol up to an interpretation of the

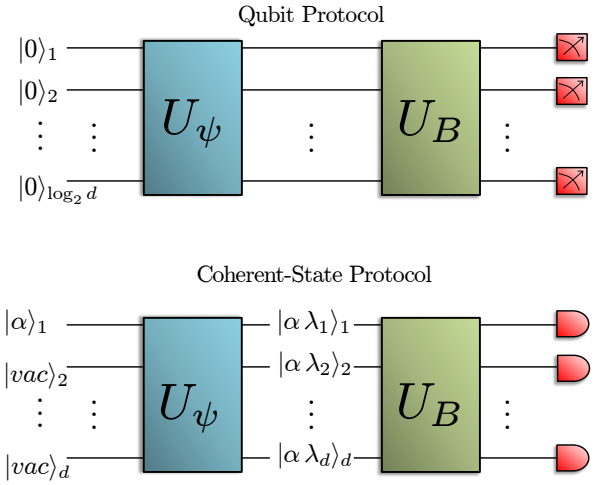

Figure 1 (Color online) In a simple qubit protocol, Alice prepares a state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ of $\log_2 d$ qubits by applying a unitary transformation U_ψ on an inital state $|\bar{0}\rangle := |0\rangle^{\otimes \log_2 d}$. She sends the state to Bob, who applies a unitary transformation U_B and measures the resulting state in the computational basis. In the equivalent coherent-state protocol, the initial state corresponds to a coherent state in a single mode and the vacuum on the others. The state $|\alpha, \psi\rangle = \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k$ is prepared by applying the transformation U_ψ to the optical modes. This state is sent to Bob, who applies the transformation U_B and consequently measures each mode for the presence of photons with threshold single-photon detectors.

measurement outcomes. As an illustration, a simple qubit protocol and its coherent-state counterpart are depicted in Fig. 1.

An immediate appealing property of coherent-state protocols is that their implementation faces much lesser obstacles than their qubit counterparts. Indeed, the fundamental challenge of a quantum-optical implementation of qubit protocols lies in the difficulty of generating entangled states of many qubits and performing global unitary transformations on them. On the other hand, coherent-state protocols face significantly less daunting obstacles. The experimental generation of coherent states is a commonplace task and the construction of linear-optical circuits can, in principle, be realized with simple devices such as beam splitters and phase-shifters [20], though experimental challenges may remain depending on the required unitary operation. Moreover, the platforms for linear optics experiments continue to improve at a fast rate, most notably with the development of integrated optics [25] and time-bin encodings [17, 10].

As we have mentioned already, an advantage of coherent-state protocols is that they employ a coherent state in a superposition of modes, which is equivalent to a tensor product of individual coherent states across the various modes. However, qubit protocols usually require high amounts of entanglement. This seems to indicate that the 'quantumness' of the original qubit protocol has been lost through the mapping. Nevertheless, it is important to realize that this is not the case, as coherent-state protocols showcase a truly quantum property: non-orthogonality. Given two states $|\alpha, \psi\rangle = \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k$ and $|\alpha, \varphi\rangle = \bigotimes_{k=1}^{d} |\alpha\,\nu_k\rangle_k$, with $d \gg \alpha$, the individual coherent states in each mode will typically be highly non-orthogonal, i.e. $\langle \alpha\,\nu_k | \alpha\,\lambda_k \rangle \approx 1$. Moreover, the presence of single-photon detectors also permit truly quantum phenomena, such as unambiguous state discrimination of non-orthogonal states. In fact, it can be useful to intuitively think of the coherent-state mapping as an exchange

between entanglement and non-orthogonality, since an implementation of qubit protocols with actual physical qubits usually requires entanglement amongst the qubits.

In coherent-state protocols, the average photon number, $|\alpha|^2$, is a parameter that can be chosen independently of the dimension of the states of the original qubit protocol. This is to be put in contrast with any quantum-optical realization of a qubit protocol, which inevitably requires a number of photons that scales with the dimension of the states. Hence, coherent-state protocols offer an intrinsic saving in the number of photons required for their implementation. The drawback, of course, is that the number of optical modes is exponentially larger than the number of qubits in the original protocol. This means that the mapping is only suitable for its application to protocols that originally require only a small number of qubits. From a theoretical perspective, the relationship between these two types of protocols may provide an insight into the trade-offs between different resources in quantum communication, as well as into the interplay between entanglement and non-orthogonality in quantum mechanics.

Now that we have outlined the coherent-state mapping, we continue by describing how these techniques can be applied in the construction of protocols in quantum communication complexity.

3 Quantum Communication Complexity

Communication complexity is the study of the amount of communication that is required to perform distributed information-processing tasks. This corresponds to the scenario in which two parties, Alice and Bob, respectively receive inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and their goal is to collaboratively compute the value of a Boolean function $f(x,y)$ with as little communication as possible [27]. Although they can always do this by communicating their entire input, the pertaining question in communication complexity is: What is the minimum amount of communication that is really needed? Likewise, quantum communication complexity studies the case where the parties are allowed to employ quantum resources such as quantum channels and shared entanglement [6, 7].

Remarkably, it has been proven that there exist various problems for which the use of quantum resources offer exponential savings in communication compared to their classical counterparts [9, 19, 2, 12, 8]. As discussed previously, coherent-state protocols require a number of modes that is exponentially larger than the number of qubits of the original protocol. Thus, from a practical perspective, the exponential savings that are possible for certain tasks in quantum communication complexity conveniently balance the exponential increase in the number of modes, making them a natural candidate for the application of the coherent-state mapping.

We are first interested in quantifying the amount of communication that takes place in a quantum communication complexity protocol. Informally, this is done by counting the number of qubits that are employed. But what happens if a protocol uses physical systems that are manifestly *not* qubits? In that case, we quantify the amount of communication in terms of the smallest number of qubits that would be required, in principle, to replicate the performance of the protocol. More precisely, if a quantum communication protocol uses states in a Hilbert space of dimension d, this space can be associated to a system of $\mathcal{O}(\log_2 d)$ qubits. Therefore, the amount of communication C in a quantum protocol is generally given by

$$C = \log_2[\dim(\mathcal{H})] \tag{6}$$

where $\mathcal{H}$ is the smallest Hilbert space containing all states of the protocol. Moreover, Holevo's theorem [15] guarantees that no more than $\log_2 d$ classical bits of information could be transmitted, on average, by a quantum protocol that uses state in a Hilbert space of dimension d.

Quantifying communication in qubit protocols is straightforward. For coherent-state protocols, even though the *actual* Hilbert space associated to all possible signal states is large (distinct coherent states are linearly independent), they effectively occupy a small Hilbert space, as is expressed in the following theorem:

▶ **Theorem 1.** *[1] For any state $|\psi\rangle$ in a Hilbert space of dimension d, let $|\alpha,\psi\rangle$ be the state associated to it through the coherent-state mapping. Then, for any $\epsilon > 0$, there exists a Hilbert space $\mathcal{H}_\alpha$ of dimension d_α such that*

$$\log_2 d_\alpha = \mathcal{O}(\log_2 d),$$
$$\langle\alpha,\psi|P_{\mathcal{H}_\alpha}|\alpha,\psi\rangle \geq 1-\epsilon,$$

and where $P_{\mathcal{H}_\alpha}$ is the projector onto $\mathcal{H}_\alpha$.

Proof. For a given $\Delta > 0$, let $\mathcal{H}_\alpha$ be the subspace spanned by the set of Fock states $\{|n_1\rangle \otimes |n_2\rangle \otimes \ldots \otimes |n_d\rangle\}$ over d modes whose total photon number $n = \sum_{k=1}^{d} n_k$ satisfies $|n - |\alpha|^2| \leq \Delta$. The dimension of $\mathcal{H}_\alpha$ is equal to the the number of distinct ways in which n photons can be distributed into the d different modes. Since the photons are indistinguishable, this quantity is given by the binomial factor $\binom{n+d-1}{d-1}$ [23]. In the case of $\mathcal{H}_\alpha$, there are 2Δ different possible values of n, the largest being $n = |\alpha|^2 + \Delta$. Thus, the dimension d_α of this subspace satisfies

$$\begin{aligned}\log_2 d_\alpha &\leq \log_2 \left[2\Delta \binom{|\alpha|^2+\Delta+d-1}{d-1}\right] \\ &\leq (|\alpha|^2+\Delta)\log_2\left[(|\alpha|^2+\Delta+d-1)\right] + \log_2(2\Delta), \end{aligned} \tag{7}$$

which is $\mathcal{O}(\log_2 d)$ for any fixed α and Δ.

Now notice that the number $\langle\alpha,\psi|P_{\mathcal{H}_\alpha}|\alpha,\psi\rangle$ is equal to the probability of performing a photon number measurement on $|\alpha,\psi\rangle$ and obtaining a value satisfying $|n - |\alpha|^2| \leq \Delta$. Since any coherent state $|\alpha,\psi\rangle$ has a Poissonian photon number distribution with mean $|\alpha|^2$, we can use the properties of this distribution to calculate the probability that the measured number of photons lies within the desired range. This probability satisfies [11]

$$P(|n-|\alpha|^2| \geq \Delta) \leq 2e^{-|\alpha|^2}\left(\frac{e|\alpha|^2}{|\alpha|^2+\Delta}\right)^{|\alpha|^2+\Delta} \tag{8}$$

which can be made equal to any $\epsilon > 0$ by choosing Δ accordingly while keeping α fixed. ◀

Therefore, the fact that the mean photon number $|\alpha|^2$ is fixed in coherent-state protocols leads to the states involved effectively occupying a Hilbert space of dimension that is comparable to that of the original one. This implies that the asymptotic behaviour of the amount of communication is the same for both classes of protocols. Moreover, the effectively unused sections of the entire Hilbert space can still be used, in principle, for other purposes such as the transmission of additional information.

We now focus on the bounded-error model in which Alice and Bob have randomness at their disposal and need only determine the value of the function $f(x,y)$ with probability greater or equal to $1-\epsilon$ for all possible values of x and y. They can send quantum states to

each other, apply unitary transformations on these states, and make measurements in the same way as the quantum communication protocols discussed before. Since they are only interested in learning the value of the function, their final measurement can always be thought of as a projective measurement onto two orthogonal subspaces H_0 and H_1, corresponding to $f(x,y)=0$ and $f(x,y)=1$ respectively.

In a coherent-state version of this model, the crucial difference lies in the measurement stage, where the subspaces H_0 and H_1 are mapped onto sets of modes S_0 and S_1. Unlike the qubit protocol, there can be clicks happening in both sets of modes and as a consequence, checking for the presence of clicks does not suffice to determine the value of the function. Instead, in order to decide between both possible values of $f(x,y)$, we opt for the strategy of counting the number of clicks that occur in each set of modes and selecting the one with the largest number of clicks.

Let C_b be the random variable corresponding to the number of clicks observed in the set of modes S_b, with $b=0,1$. The distribution of C_b is known as a Poisson-binomial distribution and its expectation value is given by

$$\mathbb{E}(C_b)=\sum_{k\in S_b} p_{\alpha,k} := \mu_b, \tag{9}$$

where $p_{\alpha,k}=1-\exp(-|\alpha\,\lambda_k|^2)$ is the probability of obtaining a click in the k-th mode.

This distribution can be difficult to work with in its exact form, so it is usual to approximate it by a Poisson distribution with the same mean. This approximation can be made precise through the following result:

▶ **Theorem 2.** *[3] Let C_b be a Poisson-binomial random variable with mean μ_b. Similarly, let L_b be a Poisson random variable with the same mean μ_b. Then, for any set A, it holds that*

$$|\Pr(C_b\in A)-\Pr(L_b\in A)|\leq \min(1,\mu_b^{-1})\tau_b, \tag{10}$$

where $\tau_b := \sum_{k\in S_b}(p_{\alpha,k})^2$ and $p_{\alpha,k}$ is the probability of obtaining a click on the k-th mode.

We can use this fact to show that, under certain conditions, a coherent-state version of a bounded-error qubit protocol also gives the correct value of the function with bounded error.

▶ **Theorem 3.** *Let a qubit protocol for communication complexity have a probability of success $P\geq 1-\epsilon$. Then the corresponding coherent-state protocol has a probability of success $P_\alpha > 1-\epsilon$ if there exists a $\mu=|\alpha|^2$ such that*

$$2e^{-P\mu}(2eP\mu)^{\mu/2}+\max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau\leq\epsilon \tag{11}$$

where μ_b is the expected number of clicks in the set of modes S_b and $\tau=\sum_k(p_{\alpha,k})^2$.

Proof. Without loss of generality, we take $f(x,y)=0$ to correspond to the correct value of the function. We can bound the success probability as

$$\begin{aligned}P_\alpha &= \Pr(C_0>C_1)\\ &\geq \Pr(C_0>\tfrac{\mu}{2})\Pr(C_1<\tfrac{\mu}{2})\\ &= (1-\Pr(C_0<\tfrac{\mu}{2}))(1-\Pr(C_1>\tfrac{\mu}{2})).\end{aligned}$$

From Theorem 2 we can also write

$$\begin{aligned}\Pr(C_0<\tfrac{\mu}{2}) &\leq \Pr(L_0<\tfrac{\mu}{2})+\min(1,\mu_0^{-1})\tau_0\\ &\leq e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2}+\min(1,\mu_0^{-1})\tau_0,\end{aligned}$$

where we have bounded the Poisson distribution as in Eq. (8). Similarly we have

$$\Pr(C_1 > \tfrac{\mu}{2}) \leq e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} + \min(1,\mu_1^{-1})\tau_1.$$

Putting these together we get

$$\begin{aligned} P_\alpha \geq & \left(1 - e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} - \min(1,\mu_0^{-1})\tau_0\right)\left(1 - e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} - \min(1,\mu_1^{-1})\tau_1\right) \\ > & 1 - e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} - e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} - \min(1,\mu_0^{-1})\tau_0 - \min(1,\mu_1^{-1})\tau_1 \\ \geq & 1 - e^{-P\mu}(2eP\mu)^{\mu/2} - e^{-(1-P)\mu}(2e(1-P)\mu)^{\mu/2} - \max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau, \end{aligned}$$

where $\tau = \tau_0 + \tau_1 = \sum_k (p_{\alpha,k})^2$ and we have used the fact that

$$P\mu = \sum_{k\in S_0} |\alpha|^2 p_k > \sum_{k\in S_0}(1 - e^{-|\alpha|^2 p_k}) = \mu_0 \tag{12}$$

and similarly $(1-P)\mu > \mu_1$. Whenever $P > 1/2$, it holds that $e^{-P\mu}(2eP\mu) > e^{-(1-P)\mu}(2e(1-P)\mu)$ so we can finally write

$$P_\alpha > 1 - 2e^{-P\mu}(2eP\mu)^{\mu/2} - \max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau. \tag{13}$$

From this expression it is clear that whenever condition (11) holds, $P_\alpha > 1-\epsilon$ as desired. ◀

Notice that the quantity $2e^{-P\mu}(2eP\mu)^{\mu/2}$ can be made arbitrarily small for any $P > 1-\epsilon$ by choosing a large enough value of $\mu = |\alpha|^2$. However, large values of μ result in higher values of the individual click probabilities $\{p_{k,\alpha}\}$ and consequently larger values of $\tau = \sum_k (p_{\alpha,k})^2$, making it harder for the quantity $\max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau$ to be small. Therefore, condition (11) may only be satisfied when the original probabilities $\{p_i\}$ are very small, as this results in a small τ even when μ is large. Of course, whenever the communicated states lie in a Hilbert space of large dimension, we expect the outcome probabilities to be small and, consequently, the coherent-state protocol to function adequately.

We would like to apply the coherent-state mapping to known protocols in quantum communication complexity. In fact, this has already been demonstrated in [1], where, essentially, a coherent-state mapping was used to construct a protocol for quantum fingerprinting. We now discuss how the mapping can be used to construct a protocol for the Hidden Matching Problem.

The Hidden Matching Problem. In this communication complexity problem, Alice receives an n-bit string $x \in \{0,1\}^n$ as input, with n an even number. Additionally, Bob receives a perfect matching $M = \{(i_1,j_1),(i_2,j_2),\ldots,(i_{n/2},j_{n/2})\}$ on the set of numbers $\{1,2,\ldots,n\}$, i.e. a partition into $n/2$ disjoint pairs. A perfect matching can be visualized as a graph with n vertices and $n/2$ edges, where each vertex is connected to only one other vertex. Only one-way communication from Alice to Bob is permitted and their goal is to output an element of the matching (i,j) and a bit value b such that $b = x_i \oplus x_j$, where x_i is the i-th bit of the string x.

It has been shown that any classical protocol requires $\Omega(\sqrt{n})$ bits of communication, even in the presence of errors [2]. On the other hand, there exists an efficient quantum

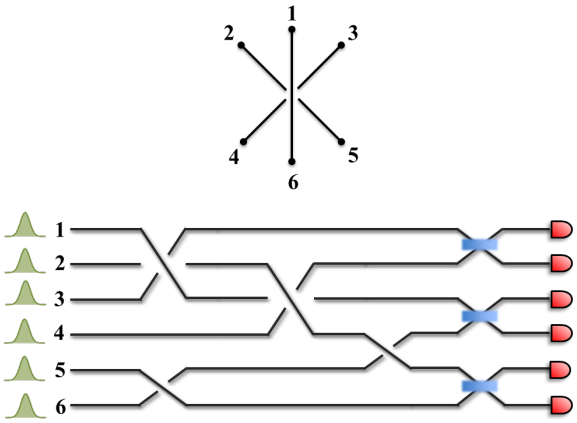

Figure 2 (Color online) An example of an implementation of a coherent-state protocol for the Hidden Matching problem. Alice receives a string of six bits and Bob receives the matching $(1,6),(2,5),(3,4)$, as represented in the graph. Alice encodes her input values in the phases of six coherent states in different modes and sends them to Bob. His measurement consists of a circuit in which the modes are permutated in accordance with the matching and then interefere pairwise in three balanced beamsplitters. Bob can output a correct solution to the problem based on the detectors that click.

protocol that uses only $\mathcal{O}(\log_2 n)$ qubits of communication and outputs the correct answer with certainty. In this protocol, Alice prepares the state

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \tag{14}$$

and sends it to Bob, who measures it in the basis

$$\{\tfrac{1}{\sqrt{2}}(|i\rangle \pm |j\rangle)\}, \tag{15}$$

with $(i,j) \in M$. The outcome $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ only occurs if $x_i \oplus x_j = 0$ and similarly, $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$ only occurs if $x_i \oplus x_j = 1$. This allows Bob to give a correct output after performing his measurement. Note that Bob's measurement basis is constructed from the canonical basis by applying a Hadamard transformation to the subspaces $\{|i\rangle, |j\rangle\}$, with $(i,j) \in M$.

To construct a coherent-state protocol for the Hidden Matching problem, we just have to apply the rules of the mapping. In this case, Alice prepares the state

$$|\alpha, x\rangle = \bigotimes_{i=1}^{n} \left| (-1)^{x_i} \tfrac{\alpha}{\sqrt{n}} \right\rangle \tag{16}$$

and sends it to Bob. The linear-optical equivalent of a Hadamard gate is a balanced beamsplitter, so Bob's measurement consists of interfering each of the pairs of modes $\{b_i, b_j\}$ (with $(i,j) \in M$) in a balanced beam-splitter and detecting photons in the outputs as illustrated in Fig. 2. If the incoming states to the input ports of the beam splitter are

$$\left| (-1)^{x_i} \tfrac{\alpha}{\sqrt{n}} \right\rangle \otimes \left| (-1)^{x_j} \tfrac{\alpha}{\sqrt{n}} \right\rangle, \tag{17}$$

the output states will be

$$\left| \left(1 + (-1)^{x_i \oplus x_j}\right) \tfrac{\alpha}{\sqrt{n}} \right\rangle \otimes \left| \left(1 - (-1)^{x_i \oplus x_j}\right) \tfrac{\alpha}{\sqrt{n}} \right\rangle. \tag{18}$$

Notice that for each possible value of $x_i \oplus x_j$, one of the output states will be a vacuum while the other is a coherent-state with non-zero amplitude. Therefore, we can associate a value of $x_i \oplus x_j$ to each of the output detectors so that whenever a click occurs, the correct value can be inferred with certainty. Even if there are many clicks, they will always correspond to a correct value. Thus, the only issue that can arise is that no-clicks occur and the probability that this happens is given by

$$P_{\text{no-click}} = e^{-|\alpha|^2}, \tag{19}$$

which can be made arbitrarily small by choosing α appropriately. Moreover, Theorem 1 guarantees that the amount of communication in the coherent-state protocol is $\mathcal{O}(\log_2 n)$ and an exponential separation in communication complexity is maintained.

4 Conclusions

We have outlined a general framework for encoding quantum communication protocols involving pure states, unitary transformations, and projective measurements, into another set of protocols that employs coherent states of light in a superposition of modes, linear optics transformations, and measurements with single-photon threshold detectors. Although seemingly disparate at first glance, qubit and coherent-state protocols share in fact many properties, including the amount of communication required and the outcome statistics. Moreover, since the mapping depends on a parameter α that can be freely chosen, coherent-state protocols offer increased tunability compared to qubit protocols.

This work thus provides a general method for mapping protocols in quantum communication into a form in which they can be implemented with current technology. It is of great interest to explore what other protocols in quantum communication, besides the ones we have outlined in this work, could be implemented by applying the coherent-state mapping to their qubit versions.

Fundamentally, coherent-state protocols require a fixed and small number of photons at the price of an exponentially large number of optical modes. For practical purposes, this implies that their application to protocols that originally require a large number of qubits will be difficult. Nevertheless, the fact that very few photons are needed not only implies an inherent savings in the energy cost of communication, but may also provide other practical advantages. For example, since optical multiplexing is limited by nonlinear effects arising from large amplitudes of the electromagnetic field, the fact that coherent-state protocols employ signals with very few photons implies that they can be easily assimilated into multiplexing schemes, or even provide a new way of multiplexing quantum messages, for example by utilizing the unused sections of the entire Hilbert space. Additionally, the low photon number may result in increased clock rates: Since only a few clicks are expected to occur even in cases when many modes are transmitted, the detector dead times and jitter times do not pose a barrier to the achievable rates.

From a theoretical perspective, the coherent-state mapping can be thought of as a tool for understanding fundamental aspects about quantum communication and information. In particular, the mapping provides us with a connection between two intrinsically quantum properties: entanglement and non-orthogonality. It may also serve as a theoretical test bed for proving results regarding qubit protocols, in the same way as many other dualities have been useful in both physics and mathematics.

Acknowledgements. J. M. Arrazola would like to thank A. Ignjatovic for her help in preparing this manuscript and designing the figures, and he is grateful for the support of the

Mike and Ophelia Lazaridis Fellowship. We acknowledge support from Industry Canada, the NSERC Strategic Project Grant (SPG) FREQUENCY and the NSERC Discovery Program.

References

1 Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A*, 89:062305, Jun 2014.

2 Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *STOC*, pages 128–137, 2004.

3 Andrew D Barbour, Lars Holst, and Svante Janson. *Poisson approximation*. Clarendon press Oxford, 1992.

4 C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, may 1992.

5 C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, dec 1984. IEEE.

6 Gilles Brassard. Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003.

7 Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, Mar 2010.

8 Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.

9 Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *STOC*, pages 63–68, 1998.

10 John M. Donohue, Megan Agnew, Jonathan Lavoie, and Kevin J. Resch. Coherent ultrafast measurement of time-bin encoded photons. *Phys. Rev. Lett.*, 111:153602, Oct 2013.

11 Massimo Franceschetti, Olivier Dousse, David Tse, and Patrick Thiran. Closing the gap in the capacity of wireless networks via percolation theory. *Information Theory, IEEE Transactions on*, 53(3):1009–1018, 2007.

12 Dmitry Gavinsky. Classical interaction cannot replace a quantum message. In *STOC*, pages 95–102, 2008.

13 Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.

14 Nicolas Gisin and Rob Thew. Quantum communication. *Nature Photonics*, 1(3):165–171, 2007.

15 Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

16 Rolf T. Horn, S. A. Babichev, Karl-Peter Marzlin, A. I. Lvovsky, and Barry C. Sanders. Single-qubit optical quantum fingerprinting. *Phys. Rev. Lett.*, 95:150502, Oct 2005.

17 Peter C. Humphreys, Benjamin J. Metcalf, Justin B. Spring, Merritt Moore, Xian-Min Jin, Marco Barbieri, W. Steven Kolthammer, and Ian A. Walmsley. Linear optical quantum computing in a single spatial mode. *Phys. Rev. Lett.*, 111:150501, Oct 2013.

18 Thaddeus D Ladd, Fedor Jelezko, Raymond Laflamme, Yasunobu Nakamura, Christopher Monroe, and Jeremy L O'Brien. Quantum computers. *Nature*, 464(7285):45–53, 2010.

19 Ran Raz. Exponential separation of quantum and classical communication complexity. In *STOC*, pages 358–367, 1999.

20 M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, 1994.

21 M Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

22 Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

23 R. Sheldon. *A First Course In Probability, 6/E*. Pearson Education, 2002.

24 Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S Gray, CR Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003, 2009.

25 Sébastien Tanzilli, Anthony Martin, Florian Kaiser, Marc P De Micheli, Olivier Alibart, and Daniel B Ostrowsky. On the genesis and evolution of integrated quantum optics. *Laser & Photonics Reviews*, 6(1):115–143, 2012.

26 Pavel Trojek, Christian Schmid, Mohamed Bourennane, Časlav Brukner, Marek Żukowski, and Harald Weinfurter. Experimental quantum communication complexity. *Phys. Rev. A*, 72:050305, Nov 2005.

27 Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *STOC*, pages 209–213, 1979.

28 Jun Zhang, Xiao-Hui Bao, Teng-Yun Chen, Tao Yang, Adán Cabello, and Jian-Wei Pan. Experimental quantum "guess my number" protocol using multiphoton entanglement. *Phys. Rev. A*, 75:022302, Feb 2007.