Capacity Approaching Coding for Low Noise Interactive Quantum Communication

Debbie Leung
C&O and IQC
University of Waterloo
Waterloo, Ontario, Canada
wcleung@uwaterloo.ca

Ashwin Nayak
C&O and IQC
University of Waterloo
Waterloo, Ontario, Canada
anayak@uwaterloo.ca

Ala Shayeghi
C&O and IQC
University of Waterloo
Waterloo, Ontario, Canada
ashayeghi@uwaterloo.ca

Dave Touchette
C&O and IQC
University of Waterloo, and
Perimeter Institute
Waterloo, Ontario, Canada
touchette.dave@gmail.com

Penghui Yao
State Key Laboratory for Novel
Software Technology
Nanjing University
Nanjing, Jiangsu, P.R.China
phyao1985@gmail.com

Nengkun Yu
CQSI, FEIT
University of Technology Sydney
Ultimo, NSW, Australia
nengkunyu@gmail.com

ABSTRACT

We consider the problem of implementing two-party interactive quantum communication over noisy channels, a necessary endeavor if we wish to fully reap quantum advantages for communication. For an arbitrary protocol with n messages, designed for *noiseless* qudit channels (where d is arbitrary), our main result is a simulation method that fails with probability less than $2^{-\Theta(n\epsilon)}$ and uses a qudit channel $n\left(1+\Theta\left(\sqrt{\epsilon}\right)\right)$ times, of which an ϵ fraction can be corrupted adversarially. The simulation is thus capacity achieving to leading order, and we conjecture that it is optimal up to a constant factor in the $\sqrt{\epsilon}$ term. Furthermore, the simulation is in a model that does not require pre-shared resources such as randomness or entanglement between the communicating parties. Perhaps surprisingly, this outperforms the best known overhead of $1+O\left(\sqrt{\epsilon\log\log\frac{1}{\epsilon}}\right)$ in the corresponding *classical* model, which is also conjectured to be optimal [Haeupler, FOCS'14]. Our work also improves over the best previously known quantum result where the overhead is a non-explicit large constant [Brassard *et al.*, FOCS'14] for low ϵ.

CCS CONCEPTS

• **Mathematics of computing → Coding theory**; • **Theory of computation → Quantum communication complexity**; **Interactive computation**;

KEYWORDS

Quantum Communication Complexity, Quantum Information Theory, Coding Theory, Interactive Coding, Capacity

STOC'18, June 25–29, 2018, Los Angeles, CA, USA

ACM ISBN 978-1-4503-5559-9/18/06…$15.00
https://doi.org/10.1145/3188745.3188908

ACM Reference Format:
Debbie Leung, Ashwin Nayak, Ala Shayeghi, Dave Touchette, Penghui Yao, and Nengkun Yu. 2018. Capacity Approaching Coding for Low Noise Interactive Quantum Communication. In *Proceedings of 50th Annual ACM SIGACT Symposium on the Theory of Computing (STOC'18).* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3188745.3188908

1 INTRODUCTION

1.1 Motivation

1.1.1 The Main Questions. Quantum communication offers the possibility of distributed computation with extraordinary *provable* savings in communication as compared with classical communication (see, e.g., [51] and the references therein). Most often, if not always, the savings are achieved by protocols that assume access to *noiseless* communication channels. In practice, though, imperfection in channels is inevitable. Is it possible to make the protocols robust to noise while maintaining the advantages offered by quantum communication? If so, what is the cost of making the protocols robust, and how much noise can be tolerated? In this article, we address these questions in the context of quantum communication protocols involving two parties, in the low noise regime. Following convention, we call the two parties Alice and Bob.

1.1.2 Channel Coding Theory as a Special Case. In the special case when the communication is one-way (say, from Alice to Bob), techniques for making the message noise-tolerant, via error correcting codes, have been studied for a long time. Coding allows us to simulate a noiseless communication protocol using a noisy channel, under certain assumptions about the noise process (such as having a memoryless channel). Typically, such simulation is possible when the *error rate* (the fraction of the messages corrupted) is lower than a certain threshold. A desirable goal is to also maximize the *communication rate* (also called the *information rate*), which is the length of the original message, as a fraction of the length of its encoding. In the classical setting, Shannon established the capacity (i.e., the optimal communication rate) of *arbitrarily accurate* transmission, in the limit of *asymptotically large* number of channel uses, through the Noisy Coding Theorem [56]. Since then, researchers have discovered many explicit codes with desirable

properties such as good rate, and efficient encoding and decoding procedures (see, for example, [2, 60]). Analogous results have been developed over the past two decades in the quantum setting. In particular, capacity expressions for a quantum channel transmitting classical data [40, 55] or quantum data [25, 49, 58] have been derived. Even though it is not known how we may evaluate these capacity expressions for a general quantum channel, useful error correcting codes have been developed for many channels of interest (see, for example, [7, 10, 21, 22]). Remarkably, quantum effects give rise to surprising phenomena without classical counterparts, including *superadditivity* [27, 39], and *superactivation* [59]. All of these highlight the non-trivial nature of coding for noisy quantum channels.

1.1.3 Communication Complexity as a Special Case. In general two-party protocols, data are transmitted in each direction alternately, potentially over a number of rounds. In a computation problem, the number of rounds may grow as a function of the input size. Such protocols are at the core of several important areas including distributed computation, cryptography, interactive proof systems, and communication complexity. For example, in the case of the Disjointness function, a canonical task in the two-party communication model, an n-bit input is given to each party, who jointly compute the function with as little communication as possible. The optimal quantum protocol for this task consists of $\Theta\left(\sqrt{n}\right)$ rounds of communication, each with a constant length message [1, 20, 41], and such a high level of interaction has been shown to be necessary [17, 42, 43]. Furthermore, quantum communication leads to provable advantages over the classical setting, without any complexity-theoretic assumptions. For example, some specially crafted problems (see, for example, [50, 51]) exhibit exponential quantum advantages, and others display the power of quantum interaction by showing that just one additional round can sometimes lead to exponential savings [43].

1.1.4 The Problem, and Motivation for the Investigation. In this paper, we consider two-party interactive communication protocols using *noisy* communication. The goal is to effectively implement an interactive communication protocol to arbitrary accuracy despite noise in the available channels. We want to minimize the number of uses of the noisy channel, and the complexity of the coding operations. The motivation is two-fold and applies to both the classical and the quantum setting. First, this problem is a natural generalization of channel coding from the 1-way to the 2-way setting, with the "capacity" being the best ratio of the number of channel uses in the original protocol divided by that needed in the noisy implementation. Here, we consider the combined number of channel uses in both directions. Note that this scenario is different from "assisted capacities" where some auxiliary noiseless resources such as a classical side channel for quantum transmission are given to the parties for free. Second, we would like to generalize interactive protocols to the noisy communication regime. If an interactive protocol can be implemented using noisy channels while preserving the complexity, then the corresponding communication complexity results become robust against channel noise. In particular, an important motivation is to investigate whether the quantum advantage in interactive communication protocols is robust against quantum noise. Due to the ubiquitous nature of quantum noise and fragility of quantum data, noise-resilience is of fundamental importance for the realization of quantum communication networks. The coding problem for interactive quantum communication was first studied in [15]. In Section 1.3, we elaborate on this work and the questions that arise from it.

1.2 Fundamental Difficulties in Coding for Quantum Interactive Communication

For some natural problems the optimal interactive protocols require a lot of interaction. For example, distributed quantum search over n items [1, 20, 41] requires $\Theta\left(\sqrt{n}\right)$ rounds of constant-sized messages [17, 42, 43]. How can we implement such highly interactive protocols over noisy channels? What are the major obstacles?

1.2.1 Standard Error Correcting Codes Are Inapplicable. In both the classical and quantum settings, standard error correcting codes are inapplicable. To see this, first suppose we encode each message separately. Then the corruption of even a single encoded message can already derail the rest of the protocol. Thus, for the entire protocol to be simulated with high fidelity, we need to reduce the decoding error for each message to be inversely proportional to the length of the protocol, say n. For constant size messages, the overhead of coding then grows with the problem size n, increasing the complexity and suppressing the rate of simulation to 0 as n increases. The situation is even worse with adversarial errors: the adversary can invest the entire error budget to corrupt the shortest critical message, and it is impossible to tolerate an error rate above $\approx 1/\text{number of rounds}$, no matter what the rate of communication is. To circumvent this barrier, one must employ a coding strategy acting collectively over many messages. However, most of these are generated dynamically during the protocol and are unknown to the sender earlier. Furthermore, error correction or detection may require communication between the parties, which is also corruptible. The problem is thus reminiscent of fault-tolerant computation in that the steps needed to implement error correction are themselves subject to errors.

1.2.2 The No-Cloning Quantum Problem. A fundamental property of quantum mechanics is that learning about an unknown quantum state from a given specimen disturbs the state [5]. In particular, an unknown quantum state cannot be cloned [26, 61]. This affects our problem in two fundamental ways. First, any logical quantum data leaked into the environment due to the noisy channel cannot be recovered by the communicating parties. Second, the parties hold a joint quantum state that evolves with the protocol, but they cannot make copies of the joint state without corrupting it.

1.3 Prior Classical and Quantum Work

Despite the difficulties in coding for interactive communication, many interesting results have been discovered over the last 25 years, with a notable extension in the quantum setting.

1.3.1 Classical Results Showing Positive Rates. Schulman first raised the question of simulating noiseless interactive communication protocols using noisy channels in the classical setting [52–54]. He developed *tree codes* to work with messages that are determined one at a time, and generated dynamically during the course of the

interaction. These codes have constant overhead, and the capacity is thus a positive constant. Furthermore, these codes protect data against adversarial noise that corrupts up to a $\frac{1}{240}$ fraction of the channel uses. This tolerable noise rate was improved by subsequent work, culminating to the results by Braverman and Rao [19]. They showed that $< \frac{1}{4}$ adversarial errors can be tolerated provided one can use large constant alphabet sizes and that this bound on noise rate is optimal.

1.3.2 Classical Results with Efficient Encoding and Decoding. The aforementioned coding schemes are not known to be computationally efficient, as they are built on tree codes; the computational complexity of encoding and decoding tree codes is unknown. Other computationally efficient encoding schemes have been developed [12–14, 31, 32, 34]. The communication rates under various scenarios have also been studied [16, 28, 29, 35]. However, the rates do not approach the capacity expected of the noise rate.

1.3.3 Classical Results with Optimal Rates. Kol and Raz [44] first established coding with rate approaching 1 as the noise parameter goes to 0, for the binary symmetric channel. Haeupler [36] extended the above result to adversarial binary channels corrupting at most an ϵ fraction of the symbols, with communication rate $1 - O\left(\sqrt{\epsilon \log\log\left(\frac{1}{\epsilon}\right)}\right)$, which is conjectured to be optimal. For oblivious adversaries, this increases to $1 - O(\sqrt{\epsilon})$. Further studies of capacity have been conducted, for example, in [3, 38]. For further details about recent results on interactive coding, see the extensive survey by Gelles [30].

1.3.4 Quantum Results Showing Positive Rates. All coding for classical interactive protocols relies on "backtracking": if an error is detected, the parties go back to an earlier stage of the protocol and resume from there. Backtracking is impossible in the quantum setting due to the no cloning principle described in the previous subsection. There is no generic way to make copies of the quantum state at earlier stages without restarting the protocol. Brassard, Nayak, Tapp, Touchette, and Unger [15] provided the first coding scheme with constant overhead by using two ideas. The first idea is to teleport each quantum message. This splits the quantum data into a protected quantum share and an unprotected classical share that is transmitted through the noisy channels using tree codes. Second, backtracking is replaced by *reversing* of steps to *return* to a desirable earlier stage; i.e., the joint quantum state is evolved back to that of an earlier stage, which circumvents the no-cloning theorem. This is possible since local operations can be made unitary, and communication can be reversed (up to more noise). Together, a positive simulation rate (or constant overhead) can be achieved. In the noisy analogue to the Cleve-Buhrman communication model where entanglement is free, error rate $< \frac{1}{2}$ can be tolerated. In the noisy analogue to the Yao (plain) model, a noisy quantum channel with one-way quantum capacity $Q > 0$ can be used to simulate an n-message protocol given $O\left(\frac{1}{Q}n\right)$ uses. However, the rate can be suboptimal and the coding complexity is unknown due to the use of tree codes. The rate is further reduced by a large constant in order to match the quantum and classical data in teleportation, and in coordinating the action of the parties (advancing or reversing the protocol).

1.4 Results in This Paper, Overview of Techniques, and Our Contributions

Inspired by the recent results on rate optimal coding for the classical setting [36, 44] and the rate suboptimal coding in the quantum setting [15], a fundamental question is: can we likewise avoid the loss of communication rate for interactive *quantum* protocols? In particular, is it possible to protect quantum data without pre-shared free entanglement, and if we have to generate it at a cost, can we still achieve rate approaching 1 as the error rate vanishes? Further, can erroneous steps be reversed with noisy resources, and with negligible overhead as the error rate vanishes? What is the complexity of rate optimal protocols, if one exists? Are there other new obstacles?

Our main result addresses all these questions. We focus on alternating protocols, in which Alice and Bob exchange qudits back and forth in alternation.

Theorem 1. *Consider an interactive two-party communication protocol Π with n messages of size one qubit each. We provide a simulation protocol Π' using $n\left(1 + \Theta\left(\sqrt{\epsilon}\right)\right)$ messages over a fully adversarial binary quantum channel corrupting at most an ϵ fraction of these messages. (In other words, the simulation achieves a communication rate of $1 - \Theta\left(\sqrt{\epsilon}\right)$.) The probability of a successful simulation is at least $1 - 2^{-\Theta(n\epsilon)}$ and the computational complexity of the coding operations is $O\left(n^2\right)$. Similar results hold for other alphabet sizes.*

1.4.1 Remarks on Our Main Result. Besides resolving the question concerning rate optimal coding for quantum interactive communication in the low-noise regime, our work achieves a few additional goals. First, the above result is achieved in the plain quantum model, where the two parties have no pre-shared resource (such as secret key or entanglement). Remarkably, our rate outperforms the conjectured optimal bound in the corresponding plain classical model! Intuitively, this is possible in the quantum setting because a secret key can be obtained from low noise quantum communication (or from entanglement) and then more efficient hashing can be performed. Second, our work provides the first computationally efficient interactive coding scheme in the quantum setting. Third, our result is the first of its kind for establishing the capacity for a noisy quantum channel used in both directions to leading order.

1.4.2 Outline of the Ideas and Our Contributions. Our rate optimal protocol requires a careful combination of ideas to overcome various obstacles. Some of these ideas are well-established, some are not so well known, some require significant modifications, and some are new. A priori, it is not clear whether these ideas would be useful in the context of the problem. For the clarity of presentation, we start with two simplifications, namely free entanglement and large alphabet size $d = \text{poly}(n)$. We introduce several key ideas while developing a basic solution to approach the optimal rate in this scenario. Then, we extend these ideas to the plain model with large alphabet size. Finally, we adapt our protocols to the binary alphabet in both settings. In the process, we solve the coding problem in all 4 scenarios.

A priori, there is little reason to expect that the simulation framework and the tools developed for each successive case extend to the next. However, the extensions are surprisingly seamless and without serious obstacles, culminating in the final result. This testifies to the power of the framework and choice of tools we deploy.

In this extended abstract, we focus on the simplest model we study, teleportation-based protocols via noisy classical channels with large alphabet. This is the focus of Section 2. We then briefly discuss in Section 3 the ideas required to extend this to the noisy quantum communication setting without pre-shared entanglement. Section 4 then briefly discusses how to extend to the small alphabet setting. All of these are discussed in greater details in the full version of this work [47]. We conclude by discussing the implication of our work as well as related open questions.

1.5 Preliminaries

1.5.1 Teleportation [4]. Suppose two parties Alice and Bob share entanglement in the form of a maximally entangled state (MES) over two d-dimensional systems, and Alice has a d-dimensional quantum message. She can perform a simple joint measurement on the message and her half of the MES, and upon getting one of d^2 possible outcomes k, Bob's half of the MES will be in the quantum state which is the original quantum message rotated by a *Pauli* unitary operation labeled by k. If Alice transmits k to Bob, he can reverse the unitary operation to obtain the message. (Similarly Bob can teleport a d-dimensional message to Alice. They have to agree beforehand who is teleporting to whom.)

1.5.2 The Cleve-Burhman Model and the Yao Model. In the Cleve-Buhrman communication complexity model [24], the parties have access to free entanglement and a two-way noiseless classical channel. The parties may simulate quantum communication through teleportation. In the Yao model [62], the parties have access to noiseless quantum channels, but no pre-shared entanglement.

1.5.3 Adversarial Noise Model. In the noisy analogue to the Cleve-Burhman model, adversarial noise with noise parameter δ corrupts up to a fraction δ of the classical messages. The location of the errors can be chosen by the adversary, even adaptively depending on the earlier messages. In the noisy analogue to the Yao model (plain model), a strongly adversarial noise model with noise parameter δ includes malicious adaptative channel attacks, as long as the overall noisy evolution has Kraus operators acting nontrivially on at most a fraction δ of all messages.

1.5.4 The Large Alphabet Assumption. Following Haeupler [36], we first consider the "large alphabet case" which allows the message size to grow with n (the number of messages in the interactive protocol Π we wish to implement). In particular, the message has a poly (n)-sized alphabet (which is equivalent to a message block of $O(\log n)$ qubits). This simplifies the problem in several ways. First, adversarial noise is reduced to corruption of blocks of $O(\log n)$ qubits. Second, the given communication protocol Π is in effect less interactive. Third, simpler synchronisation (detailed below) between Alice and Bob is possible, since a constant number of symbols are sufficient to exchange position information (how far each party has simulated Π in his/her view). Similarly a constant number of messages allows for the exchange of sufficient key to perform hashing and to compare hashes.

2 TELEPORTATION-BASED PROTOCOLS VIA CLASSICAL CHANNEL WITH LARGE ALPHABET

2.1 Main Ideas

We adapt from [15] the ideas to teleport each quantum message and to reverse the protocol instead of backtracking.

We also adapt Haeupler's template [36] to make a conversation robust to noise: Both parties conduct their original conversation as if there were no noise, except for the following:

- At regular intervals they exchange concise summaries (a $\Theta(1)$ or $\Theta(\log\log n)$-bit hash value) of the conversation up to the point of the exchange.
- If the summary is consistent, they continue the conversation.
- If the summary is inconsistent, an error is detected. The parties backtrack to an earlier stage of the conversation and resume from there.

This template can be interpreted as an error correcting code over many messages, with trivial (and most importantly *message-wise*) encoding. The 2-way summaries measure the error syndromes over a large number of messages, thereby preserving the rate. It works (in the classical setting) by limiting the maximum amount of communication wasted by a single error to $O_\epsilon(1)$. The worst case error disrupts the consistency checks, but Alice and Bob agree to backtrack a constant amount when an inconsistency is detected. As the error fraction vanishes, the communication rate goes to 1. In addition, these consistency tests are efficient, consisting of evaluation of hash functions.

2.1.1 Insufficiency of Simply Combining [15] and [36]. Suppose we have to simulate an interactive protocol Π that uses noiseless classical channels in the teleportation-based model. When implementing Π with noisy classical channels, it is *not sufficient* to apply Haeupler's template to the classical messages used in teleportation, and reverse as in [15] when an error is detected. The reason is that, in [15], each message is expanded to convey different types of actions in one step (simulating the protocol forward or reversing it). This also maintains the matching between classical data with the corresponding MES, and the matching between systems containing MESs. However, this method incurs a large constant factor overhead which we cannot afford to incur.

2.1.2 New Difficulties in Rate-Optimal Simulations. Due to errors in communication, the parties need to actively rewind the simulation to correct errors on their joint quantum state. This itself can lead to a situation where the parties may not agree on how they proceed with the simulation (to rewind simulation or to proceed forward). In order to move on, both parties first need to know what the other party has done so far in the simulation. This allows them to obtain a global view of the current joint state and decide on their next action. In Ref. [15], this reconciliation step was facilitated by the extra information sent by each party and the use of tree codes. This mechanism is not available to us.

2.1.3 Framework. Our first new idea is to introduce sufficient yet concise data structures so that the parties can detect inconsistencies in (1) the stage in which they are in the protocol, (2) what type of action they should be taking, (3) histories leading to the above, (4) histories of measurement outcomes generated by one party versus the potentially different (corrupted) received instruction for teleportation decoding, (5) which system contains the next MES to be used, (6) a classical description of the joint quantum state, which is only partially known to each party. Each of Alice and Bob maintain her/his data (we collectively call these D_A, D_B respectively, here), and also an estimate of the other party's data ($\widetilde{D_B}, \widetilde{D_A}$ respectively). Without channel noise, these data are equal to their estimates.

2.1.4 A Major New Obstacle: Out-of-Sync Teleportation. Now, at every step in the simulation protocol Π', Alice and Bob may engage in one of three actions: a forward step in Π, step in reverse, or the exchange of classical summaries. However, the summaries can also be corrupted. This leads to a new difficulty: errors in the summaries can trigger Alice and Bob to engage in different actions. In particular, it is possible that one party tries to teleport while the other expects classical communication, with only one party consuming his/her half of an MES. They then become out-of-sync over which MESs to use. This kind of problem, to the best of our knowledge, has not been encountered before, and it is not clear if quantum data can be protected from such error. (For example, Alice may try to teleport a message into an MES that Bob already "used" earlier.) One of our main technical contributions is to show that the quantum data can always be located and recovered when Alice and Bob resolve the inconsistencies in their data $(D_A, \widetilde{D_B})$ and $(\widetilde{D_A}, D_B)$ in the low noise regime. This is particularly surprising since quantum data can potentially leak irreversibly to the environment (or the adversary): Alice and Bob potentially operate in an open system due to channel noise, and out-of-sync teleportation a priori does not protect the messages so sent.

2.1.5 Tight Rope Between Robustness and Rate. The simulation maintains sufficient data structures to store information about each party's view so that Alice and Bob can overcome all the obstacles described above. The simulation makes progress so long as Alice's and Bob's views are consistent. The robustness of the simulation requires that the consistency checks be frequent and sensitive enough so that errors are caught quickly. On the other hand, to optimize interactive channel capacity, the checks have to remain communication efficient and not too frequent neither. This calls for delicate analysis in which we balance the two. We also put in some redundancy in the data structures to simplify the analysis.

2.2 Results

In this section, we focus on the teleportation-based quantum communication model. In more detail, Alice and Bob share an unlimited number of EPR pairs (MESs) before the protocol begins. The parties effectively send each other a qubit (or a qudit) using an EPR-pair (or an MES) and two classical bits (or dits) of communication. The complexity of the protocol is the number of classical bits (or dits) exchanged, while the the number of EPR-pairs (or MESs) used are available for free. We call this model noiseless if the classical channel is noiseless.

Our main result about this model is the simulation of an n-message noiseless communication protocol over an adversarial channel that corrupts any ϵ fraction of the transmitted symbols. First, we state the result for large alphabets.

Theorem 2. *Consider teleportation-based noiseless communication protocols of length n defined over a channel with a $\Theta(\log n)$-bit alphabet, and the problem of simulating them with a noisy version of the channel over the same alphabet.*

There is a protocol that with probability at least $1 - 2^{-\Omega(\epsilon n)}$, simulates any n-symbol teleportation-based noiseless communication protocol using $n(1 + \Theta(\sqrt{\epsilon}))$ symbols over any fully adversarial error channel with error rate at most ϵ. In other words, the simulation achieves information rate $1 - \Theta(\sqrt{\epsilon})$.

The simulation of channels over constant-size alphabets is more challenging. Nonetheless, we show that a similar simulation is possible in this case as well.

Theorem 3. *Consider teleportation-based noiseless communication protocols of length n defined over a channel with a constant-size alphabet, and the problem of simulating them with a noisy version of the channel over the same alphabet.*

There is a protocol that with probability at least $1 - 2^{-\Omega(\epsilon n)}$, simulates any n-symbol teleportation-based noiseless communication protocol using $n(1 + \Theta(\sqrt{\epsilon}))$ symbols over any fully adversarial error channel with error rate at most ϵ. In other words, the simulation achieves information rate $1 - \Theta(\sqrt{\epsilon})$.

2.3 Description of Simulation

In the teleportation-based quantum communication model, Alice and Bob implement a protocol Π_0 with prior shared entanglement and quantum communication by substituting teleportation for quantum communication. For simplicity, we assume that Π_0 is alternating, and begins with Alice. It acts on input state $|\psi_{\text{init}}\rangle^{ABCER}$, with the A register held by Alice, the B register held by Bob, the C register a qudit communication register exchanged back-and-forth between Alice and Bob, and held by Alice at both the beginning and the end of the protocol, the E register held by Eve, a potential adversary, and the $ABCE$ registers are purified by a reference register R, untouched throughout. In the implementation Π of Π_0, the message register C from Π_0 has two counterparts, C_A and C_B, held by Alice and Bob, respectively. The unitary operations on AC in Π_0 are applied by Alice on AC_A in Π. When Alice sends the qudit in C to Bob in Π_0, she applies the teleportation measurement to C_A and her share of the next available MES, and sends the measurement outcome to Bob in Π. Then Bob applies a decoding operation on his share of the MES, based on the message received, and swaps the MES register with C_B. Bob and Alice's actions in Π when Bob wishes do a local operation and send a qudit to Alice in Π_0 are analogously defined. For ease of comparison with the joint state in Π_0, we describe the joint state of the registers in Π (or its simulation over a noisy channel) in terms of registers ABC. There, C stands for C_A if Alice is to send the next message or all messages have been sent, and for C_B if Bob is to send the next message.

Starting with such a protocol Π in the teleportation-based model, we design a simulation protocol Π' which uses a noisy classical channel. The simulation works with *blocks* of even number of messages. By a *block* of size r (for even r) of Π, we mean a sequence of r local operations and messages alternately sent in Π by Alice and Bob, starting with Alice.

Roughly speaking, Alice and Bob run the steps of the original protocol Π as is, in blocks of size $r := \Theta(\frac{1}{\sqrt{\epsilon}})$, with r even. They exchange summary information between these blocks, in order to check whether they agree on the operations that have been applied to the quantum registers ABC in the simulation. The MESs used for teleportations are correspondingly divided into blocks of r MESs, implicitly numbered from 1 to r: the odd numbered ones are used to simulate quantum communication from Alice to Bob, and the even numbered ones from Bob to Alice. If either party detects an error in transmission, they may run a block of Π in reverse, or simply communicate classically to help recover from the error. The classical communication is also conducted in sequences equal in length to the ones involving a block of Π. A block of Π' refers to any of these types of sequences.

2.3.1 Meta Data. In more detail, Alice uses an iteration in Π' for one out of four different types of operations: evolving the simulation by running a block of Π in the forward direction (denoted a "+1" block); reversing the simulation by applying inverses of unitary operations of Π (denoted a "−1" block); synchronizing with Bob on the number of MESs used so far by applying identity operators between rounds of teleportation (denoted a "0" block, with 0 standing for the application of unitary operations U_i^0 which are I^{AC}"); catching up on the description of the protocol so far by exchanging classical data with Bob (denoted a "C" block, with C standing for "classical"). Alice records the sequence of types of blocks as her "metadata" in the string FullMA $\in \{\pm 1, 0, \mathrm{C}\}^*$. FullMA gets extended by one symbol for each new block of the simulation protocol Π'. The number of blocks of r MESs Alice has used is denoted q_{MA} which corresponds to the number of non-C symbols in FullMA. Similarly, Bob maintains data FullMB and q_{MB}.

FullMA and FullMB may not agree due to the transmission errors. To counter this, the two players exchange information about their metadata at the end of each block. Hence, Alice also holds $\widetilde{\mathrm{MB}}$ and $q_{\widetilde{\mathrm{MB}}}$ as her best estimation of Bob's metadata and the number of MESs he has used, respectively. Similarly, Bob holds $\widetilde{\mathrm{MA}}$ and $q_{\widetilde{\mathrm{MA}}}$. We use these data to control the simulation; before taking any action in Π', Alice checks if her guess $\widetilde{\mathrm{MB}}$ equals FullMB. Bob does the analogous check for his data.

2.3.2 Number of MESs Used. Once the two parties reconcile their view of the other's metadata with the actual metadata, they might detect a discrepancy in the number of MESs they have used. The three drawings in Figure 1 represent the $\lceil \frac{n}{r}(1 + O(r\epsilon)) \rceil$ blocks of $r = O(\sqrt{1/\epsilon})$ MESs at different points in the protocol: first, before the protocol begins; second, when Alice and Bob have used the same number of MESs; and third, when they are not synchronized, say, Alice has used more blocks of MESs than Bob. A difference in q_{MA} and q_{MB} indicates that the joint state of the protocol Π can no longer be recovered from registers $AC_{\mathrm{A}}C_{\mathrm{B}}B$ alone. Since one party did not correctly complete the teleportation operation, the (possibly erroneous) joint state may be thought of as having "leaked" into the partially measured MESs which were used by only one party.

2.3.3 Pauli Data. The last piece of information required to complete the description of what has happened so far on the quantum registers ABC is about the Pauli operators corresponding to teleportation, which we call the "Pauli data". These Pauli data contain information about the teleportation measurement outcomes as well as about the teleportation decoding operations. Since incorrect teleportation decoding may arise due to the transmission errors, we must allow the parties to apply Pauli corrections at some point. We choose to concentrate such Pauli corrections on the receiver's side at the end of each teleportation. These Pauli corrections are computed from the history of all classical data available, before the evolution or reversal of Π in a block starts, whereas the measurement and decoding Pauli data are exchanged online during the computation. The measurement data are directly transmitted over the noisy classical communication channel and the decoding data are directly taken to be the data received over the noisy channel. If there is no transmission error, the decoding Pauli operation should correspond to the inverse of the effective measurement Pauli operation and cancel out to yield a noiseless quantum channel. Figure 2 depicts the different types of Pauli data in a block corresponding to type +1 for Alice and −1 for Bob. Alice records as her Pauli data in the string FullPA $\in (\Sigma^{3r})^*$, the sequence of Pauli operators that are applied on the quantum register on her side. Alice records her Pauli data in the following order:

> measurement outcome for the first qudit she teleports,
> decoding operation for the first qudit she receives,
> correction operation for the same qudit (the first qudit she receives);
> measurement outcome for the second qudit she sends,
> decoding operation for the second qudit she receives,
> correction operation for the same qudit (the second qudit she receives);
> and so on.

Similarly Bob records as his Pauli data in FullPB, the sequence of Pauli operators applied on his side, but in a different order:

> decoding operation for the first qudit he receives,
> correction operation for the same qudit (the first qudit he receives),
> measurement outcome for the first qudit he teleports;
> decoding operation for the second qudit he receives,
> correction operation for the same qudit (the second qudit he receives),
> measurement outcome for the second qudit he sends;
> and so on.

Notice that the $3r$ symbols in the alphabet set Σ corresponding to Alice's Pauli operations in a block can be decomposed as $\frac{r}{2}$ pieces of six symbols in Σ: two for each measurement outcome, two for each teleportation decoding and two for each Pauli correction. As described above, the measurement outcome and the decoding Pauli operations are available to the sender and the receiver, respectively. Based on the message transcript in Π' so far, Alice maintains her best guess $\widetilde{\mathrm{PB}}$ for Bob's Pauli data and Bob maintains his best guess

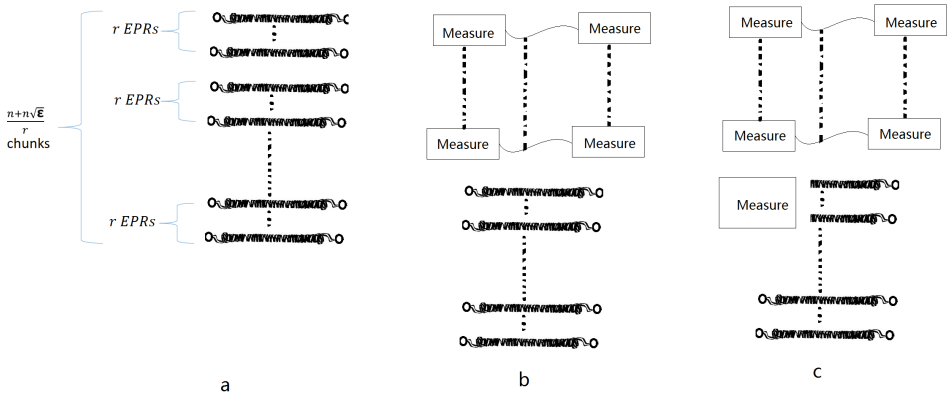

Figure 1: These figures represent the blocks of MES pairs at different stages of the protocol. Those depicted as dots have not been used yet for teleportation, those depicted by squares have been used already. The figure (a) represents them at the beginning of the protocol, when none have been used. The figure (b) represents them when Alice and Bob have used the same number of them; this is the desired situation. The figure (c) represents a situation when Alice and Bob are out of sync; here Alice has used more MES pairs than Bob. They then work to get back in sync before resuming the simulation.

$\widetilde{\text{PA}}$ for Alice's Pauli data. These data also play an important role in the simulation. Before taking any action in Π', Alice checks if her guess $\widetilde{\text{PB}}$ equals FullMB. Bob does the analogous check for his data.

Alice and Bob check and synchronize their classical data, i.e., the metadata and Pauli data by employing the ideas underlying the Haeupler algorithm [36]. Once they agree on each other's metadata and Pauli data, they both possess enough information to compute the content of the quantum register (to their best knowledge).

2.3.4 First Representation of the Quantum Register. A first representation for the content of the quantum registers ABC in Π' can be obtained directly and explicitly from the metadata and the Pauli data, and is denoted JS1, as in Eq. (1) below, with JS standing for "joint state". We emphasize that this is the state conditioned on the outcomes of the teleportation measurements as well as the transcript of classical messages received by the two parties. However, the form JS1 is essentially useless for deciding the next action that the simulation protocol Π' should take, but it can be simplified into a more useful representation. This latter form, denoted JS2, as in Eq. (2) below, directly corresponds to the further actions we may take in order to evolve the simulation of the original protocol or to actively reverse previous errors. For the description of the algorithm, we first consider JS1 or JS2 in the case when $q_{\text{MA}} = q_{\text{MB}}$. Later we also consider the remedial actions the parties take in the case when the two numbers are different, i.e., when Alice and Bob are not synchronized in the number of MESs used.

We sketch how to obtain JS1 from FullMA, FullMB, FullPA and FullPB (when $q_{\text{MA}} = q_{\text{MB}}$). Each block of r MESs which have been used by both Alice and Bob is represented by a bracketed expression $[*i]$ for some content "$*i$" corresponding to the ith block that we describe below. The content of the quantum registers is then the ABC part of

$$\text{JS1} = [*q_{\text{MA}}] \cdots [*2][*1] \, |\psi_{\text{init}}\rangle^{ABCER}, \tag{1}$$

with $|\psi_{\text{init}}\rangle^{ABCER}$ being the initial state of the original protocol. It remains to describe the content $*i$ of the ith bracket. It contains from right to left $\frac{r}{2}$ iterations of the following:

> Alice's unitary operation - Alice's teleportation measurement outcome -
> Bob's teleportation decoding - Bob's Pauli correction - Bob's unitary operation - Bob's teleportation measurement outcome -
> Alice's teleportation decoding - Alice's Pauli correction.

It also allows for an additional unitary operation of Alice on the far left when she is implementing a block of type -1; we elaborate on this later. If Alice's block type is $+1$, all her unitary operations are consecutive unitary operations from the original protocol (with the index of the unitary operations depending on the number of ± 1 in FullMA), while if it is -1, they are inverses of such unitary operations. If Alice's block type is 0, all unitary operations are equal to the identity on registers AC_{A}. Similar properties hold for Bob's unitary operations on registers BC. Alice's block type corresponds to the content of the ith non-C element in FullMA, and Bob's to the content of the ith non-C element in FullMB. Alice's Pauli data corresponds to the content of the ith block in FullPA, and Bob's to the content of the ith block in FullPB. The precise rules by which Alice and Bob determine their respective types for a block in Π', and which blocks of Π (if any) are involved, are deferred to the the full version.

To give a concrete example, suppose from her classical data, Alice determines that in *her* ith non-C block of Π', she should actively reverse the unitary operations of block k of Π to correct some error in the joint state. So her ith non-C block of Π' is of type -1. Suppose Alice's Pauli data in the ith block of FullPA correspond to Pauli operators $p_{\text{A},1}p_{\text{A},2}\cdots p_{\text{A},3r/2}$. Consider Bob's ith non-C block of Π'. Note that this may be a different block of Π' than Alice's ith

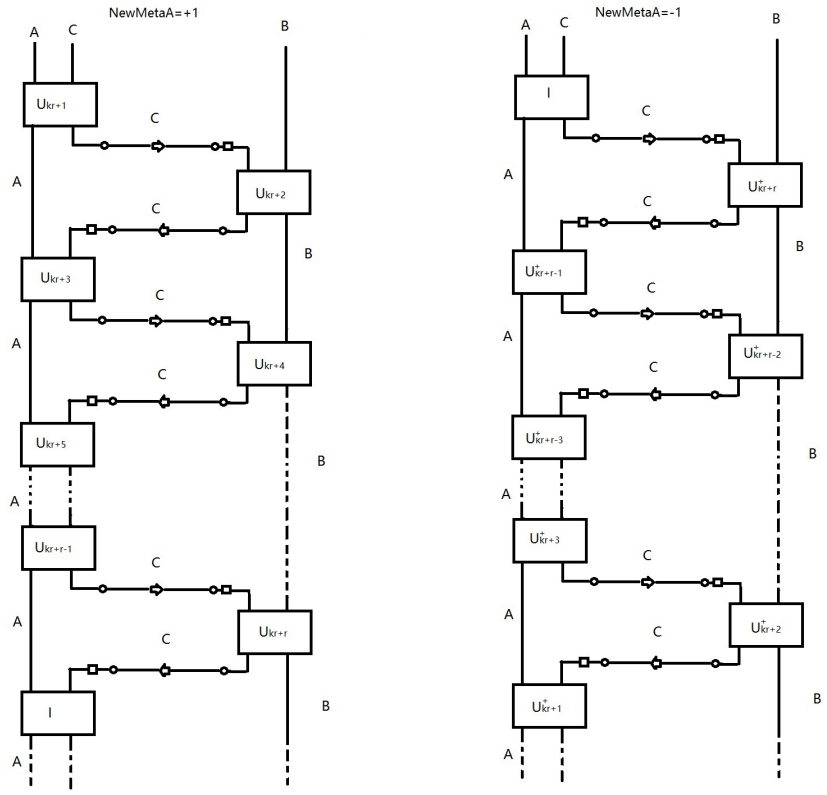

Figure 2: Representation of the teleportation scheme for a size r block. The figure on the left corresponds to Alice and Bob having blocks of type $+1$, the most common block type, and the one on the right to a block of type -1 for both. The large rectangles correspond to unitary operations or their inverses, or even an identity, of the original protocol being applied by Alice or by Bob to AC or BC, respectively. Bob has $r/2$ rectangles and applies a unitary operation or an inverse in each of them whenever he has a block of type ± 1. Alice has $r/2+1$ rectangles and uses the first $r/2$ to apply unitary operations in a block of type $+1$ and apply an identity on the last one, while she applies an identity in the first one and inverses of unitary operations in the $r/2$ last ones in a block of type -1. This is so that a -1 block for Alice can be the inverse of a $+1$ block for Alice, and vice-versa. The small circles correspond to the Pauli operations due to teleportation measurement and teleportation decoding, with the teleportation being from Alice to Bob on odd MES pairs and from Bob to Alice on even MES pairs. The small squares on the receiver side right after the teleportation decoding circle corresponds to the Pauli corrections made in order to try to correct errors in previous blocks.

non-C block. Suppose from *his* classical data, Bob determines that in his ith non-C block of Π', he should apply the unitary operations of block j of Π to evolve the joint state further. So his ith non-C block of Π' is of type $+1$. Suppose Bob's Pauli data in the ith block of FullPB correspond to Pauli operators $p_{\mathrm{B},1}p_{\mathrm{B},2}\cdots p_{\mathrm{B},3r/2}$, respectively. Then from FullMA, FullMB, FullPA, FullPB, we can compute a description of the joint state as in Eq. (1), with $*i$ equal to

$$
\begin{aligned}
&U_{kr+1}^{-1} \\
&\times \left(p_{\mathrm{A},3(r/2-1)+3} \;\; p_{\mathrm{A},3(r/2-1)+2}\right) \\
&\quad \times \left(p_{\mathrm{B},3(r/2-1)+3} \;\; U_{jr+r} \;\; p_{\mathrm{B},3(r/2-1)+2} \;\; p_{\mathrm{B},3(r/2-1)+1}\right) \\
&\quad\quad \times \left(p_{\mathrm{A},3(r/2-1)+1} \;\; U_{kr+3}^{-1}\right) \\
&\times \cdots
\end{aligned}
$$

$$\times \left(p_{\mathrm{A},3(s-1)+3} \;\; p_{\mathrm{A},3(s-1)+2}\right)$$
$$\times \left(p_{\mathrm{B},3(s-1)+3} \;\; U_{jr+2s} \;\; p_{\mathrm{B},3(s-1)+2} \;\; p_{\mathrm{B},3(s-1)+1}\right)$$
$$\times \left(p_{\mathrm{A},3(s-1)+1} \;\; U^{-1}_{kr+(r-2s+3)}\right)$$
$$\times \cdots$$
$$\times \left(p_{\mathrm{A},6} \;\; p_{\mathrm{A},5}\right) \left(p_{\mathrm{B},6} \;\; U_{jr+4} \;\; p_{\mathrm{B},5} \;\; p_{\mathrm{B},4}\right) \left(p_{\mathrm{A},4} \;\; U^{-1}_{kr+(r-1)}\right)$$
$$\times \left(p_{\mathrm{A},3} \;\; p_{\mathrm{A},2}\right) \left(p_{\mathrm{B},3} \;\; U_{jr+2} \;\; p_{\mathrm{B},2} \;\; p_{\mathrm{B},1}\right) \left(p_{\mathrm{A},1} \;\; \mathbb{I}\right) \;\; .$$

Note that Alice and Bob are not necessarily able to compute the state JS1. However, they compute analogous states using their best guess for the other party's meta data and Pauli data. They use these best-guess states to compute states analogous to JS2 using the process below. These in turn determine their course of action in the simulation.

2.3.5 Second Representation. To obtain JS2 from JS1, we first look inside each bracket and recursively cancel consecutive Pauli operators inside the bracket. In case a bracket evaluates to the identity operator on registers $A'B'C'$, we remove it. Once each bracket has been cleaned up in this way, we recursively try to cancel consecutive brackets if their contents correspond to the inverse of one another (assuming that no two U_i of the original protocol are the same or inverses of one another). Once no such cancellation works out anymore, what we are left with is representation JS2, which is of the following form:

$$\mathrm{JS2} = [\#b] \cdots [\#1][U_{gr} \cdots U_{(g-1)r+2} U_{(g-1)r+1}] \cdots \tag{2}$$
$$[U_r \cdots U_2 U_1] \, |\psi_{\mathrm{init}}\rangle^{ABCER} \; . \tag{3}$$

Here, the first g brackets starting from the right correspond to the "good" part of the simulation, while the last b brackets correspond to the "bad" part of the simulation, the part that Alice and Bob have to actively rewind later. The integer g is determined by the left-most bracket such that along with its contents, those of the brackets to the right equal the sequence of unitary operations $U_1, U_2, \ldots, U_{gr}$ from the original protocol Π in reverse. The brackets to the left of the last g brackets are all considered bad blocks. Thus, the content of [#1] is not $[U_{(g+1)r} \cdots U_{gr+1}]$, while the contents of [#2] to $[\#b]$ are arbitrary and have to be actively rewound before Alice and Bob can reverse the content of [#1].

Once Alice and Bob synchronize each other's metadata and Pauli data and compute their best guesses for JS2, if $b > 0$, they actively reverse the incorrect unitary operators in the bad blocks. They start by applying the inverse of $[\#b]$, choosing appropriately whether to have a type ± 1 or 0 block, and also choosing appropriate Pauli corrections. Else, if $b = 0$, they continue implementing unitary operations U_{gr+1} to $U_{(g+1)r}$ of the original noiseless protocol Π to evolve the simulation. (Actually, each player has their independent view of the joint state, and takes actions assuming that their view is correct.)

We describe a few additional subtleties on how the parties access the quantum register in a given block, as represented in Figure 2. First, each block begins and ends with Alice holding register C and being able to perform a unitary operation. In +1 blocks, she applies a unitary operation at the beginning and not at the end, whereas in −1 blocks she applies the inverse of a unitary operation at the end and not at the beginning. This is in order to allow a −1 block to be the inverse of a +1 block, and vice-versa. Second, whenever Alice and Bob are not synchronized in the number of MESs they have used so far, the party who has used more will wait for the other to catch up by creating a new type C block while the party who has used less will try to catch up by creating a type 0 block, sequentially feeding the C register at the output of a teleportation decoding to the input of the next teleportation measurement. (We elaborate on this in Section 2.4 below.) Notice that due to errors in communication, it might happen that +1 blocks are used to correct previous erroneous −1 blocks and 0 blocks are used to correct previous erroneous 0 blocks. As illustrated in Figure 2, the block on the right is the inverse of the one on the left if the corresponding Pauli operators are inverses of each other.

2.3.6 Summary of Main Steps. We now summarize the different steps that Alice and Bob follow in the simulation protocol Π'. (Each of them runs the simulation algorithm based on their view of the communication transcript.) In one iteration of the simulation, only one step involving communication is conducted (and this constitutes one block of operations). We proceed from one step to the next only if the goal of the step has been achieved through the *previous* iterations. The algorithms mentioned in this summary are presented in the full version.

Algorithm 1: Main steps in one iteration of the simulation for the large alphabet teleportation-based model

(1) Agree on the history of the simulation contained in the metadata, i.e., ensure FullMA = $\widetilde{\mathrm{MA}}$ and FullMB = $\widetilde{\mathrm{MB}}$. This involves Algorithm **rewindMD**, and Algorithm **extendMD**.
(2) Synchronize the number of MES pairs used, in particular, ensure $q_{\mathrm{MA}} = q_{\widetilde{\mathrm{MB}}}$ and $q_{\mathrm{MB}} = q_{\widetilde{\mathrm{MA}}}$. This involves Algorithm **syncMES**.
(3) Agree on Pauli data for all the teleportation steps and additional Pauli corrections for addressing channel errors, i.e., ensure FullPA = $\widetilde{\mathrm{PA}}$ and FullPB = $\widetilde{\mathrm{PB}}$. This is done via Algorithm **rewindPD** and Algorithm **extendPD**.
(4) Compute the best guess for JS1 and JS2. If there are any "bad" blocks in the guess for JS2, reverse the last bad block of unitary operations. I.e., implement quantum rewinding so that $b = 0$ in JS2. This is done in Algorithm **Q-simulate**.
(5) If no "bad" blocks remain, implement the next block of rounds of the original protocol. This results in an increase in g in JS2, and is also done through Algorithm **Q-simulate**.

This is also summarized in flowchart form in Figure 3.

Notice that unless there is a transmission error or a hash collision in comparing a given type of data (as in Ref. [36]), Alice and Bob cycle through these steps in tandem.

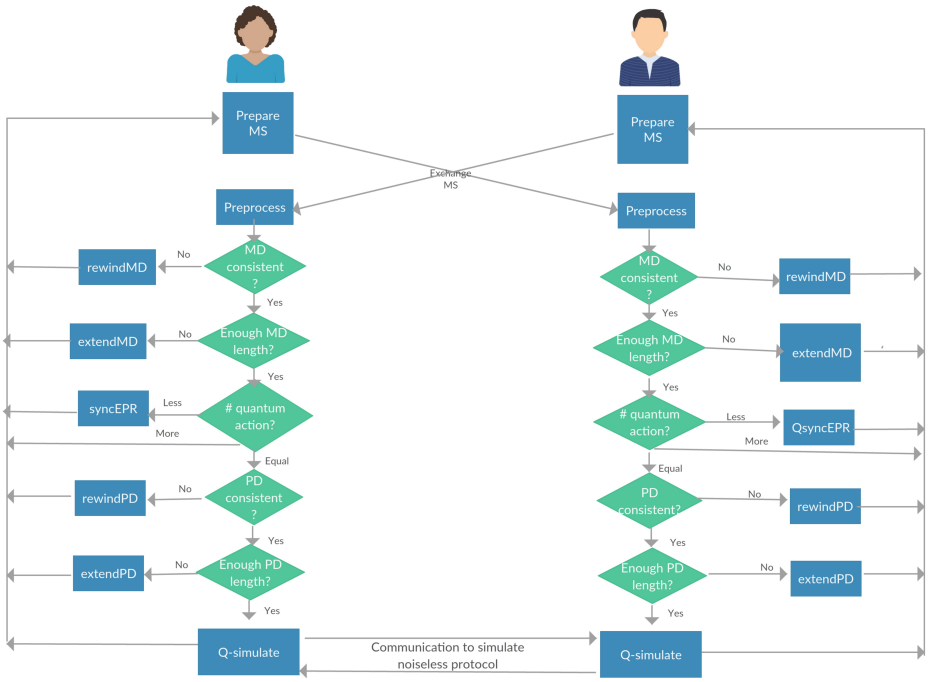

Figure 3: Flowchart of the teleportation-based scheme for high rate noisy interactive quantum communication. Most of the communication is spent actually trying to simulate the protocol, in the Q-simulate part.

2.4 Out-of-Sync Teleportation

Consider an iteration in which Alice believes she should implement a +1 block, while Bob believes he has to resolve an inconsistency in their classical data. Alice will simulate one block of the noiseless protocol Π, consuming the next block of MESs. On the other hand, Bob will try to resolve the inconsistency through classical communication alone, and not access the quantum registers. Thus Alice will treat Bob's messages as the outcomes of his teleportation measurements, and she performs the teleportation decoding operations according to these messages. The situation is even worse, since Alice sends quantum information to Bob through teleportation of which Bob is unaware, and Bob views the teleportation measurement outcomes sent by Alice as classical information about Alice's local Pauli data and metadata corresponding to previous iterations. Note that at this point the quantum state in registers ABC may potentially be lost. This scenario could continue for several iterations and derail the simulation completely. To recover from such a situation, especially to retrieve the quantum information in the unused MESs at his end, it would seem that Alice and Bob would have to rewind the simulation steps in Π' (and not only the steps of the original protocol Π) to an appropriate point in the past. This rewinding itself would be subject to error, and the situation seems hopeless. Nonetheless, we provide a simple solution to address this kind of error, which translates out-of-sync teleportation to errors in implementing the forward simulation or rewinding of the original protocol Π.

As explained in the previous subsection, Alice and Bob first reconcile their view of the history of the simulation stored in their metadata. Through this, suppose they both discover the discrepancy in the number of MESs used. (There are other scenarios as well; for example, they may both think that $q_{\mathrm{MA}} = q_{\mathrm{MB}}$. These scenarios lead to further errors, but the simulation protocol Π' eventually discovers the difference in MESs used.) In the scenario in which Alice and Bob both discover that $q_{\mathrm{MA}} \neq q_{\mathrm{MB}}$, they try to "gather" the quantum data hidden in the partially used MESs back into the registers ABC. In more detail, suppose Bob has used fewer MESs than Alice, and he discovers this at the beginning of the ith iteration. Let $E_1 E_2 \cdots E_r$ be registers with Bob that hold the halves of the *first* block of MESs that Alice has used but Bob has not. Note that $E_1, E_3, \ldots, E_{r-1}$ contain quantum information teleported by Alice, and $E_2, E_4, \ldots, E_r$ are MES-halves intended for teleportation by Bob. The MES-halves corresponding to $E_2, E_4, \ldots, E_r$ have already been used by Alice to "complete" teleportation she assumed Bob has performed. Say Alice used this block of MESs in the i'-th iteration. In the i-th iteration, Bob teleports the qudit E_1 using the MES-half E_2, E_3 with E_4, and so on. That is, Bob teleports qudit E_j using the MES-half E_{j+1} in increasing order of j, for all odd $j \in [r]$, as if the even numbered MESs had not been used by Alice. The effect of this teleportation is the same as if Alice and Bob had *both* tried to simulate the local operations and communication from the original protocol in the i'-th iteration (in the forward direction or to correct the joint state), *except that the following also happened independently of channel error*:

(1) the Pauli operations used by Bob to decode $E_1, E_3, \ldots, E_{r-1}$ were all the identity,
(2) the unitary operations used by Bob on the registers BC were all the identity, and

(3) the Pauli operations applied by Alice for decoding Bob's teleportation were unrelated to the outcome of Bob's teleportation measurements.

This does not guarantee correctness of the joint state in ABC, but has the advantage that quantum information in the MES-halves

$$E_1, E_3, \ldots, E_{r-1}$$

that is required to restore correctness is redirected back into the registers ABC. In particular, the difference in the number of MESs used by the two parties is reduced, while the errors in the joint quantum state in ABC potentially increase. The errors in the joint state are eventually corrected by reversing the incorrect unitary operations, as in the case when the teleportations are all synchronized.

To understand the phenomenon described above, consider a simpler scenario where Bob wishes to teleport a qudit $|\xi\rangle$ in register B_1 to Alice using an MES in registers $E_1'E_1$, after which Alice applies the unitary operation V to register E_1'. If they follow the corresponding sequence of operations, the final state would be $V|\xi\rangle$, stored in register E_1'. Instead suppose they do the following. First, Alice applies V to register E_1', *then* Bob measures registers B_1E_1 in the generalized Bell basis and gets measurement outcome (j,k). He sends this outcome to Alice. We may verify the state of register E_1' conditioned on the outcome is $V(X^jZ^k)|\xi\rangle$. Thus, the quantum information in ξ is redirected to the correct register, albeit with a Pauli error (that is known to Alice because of his message). In particular, Alice may later reverse V to correctly decode the teleported state. The chain of teleportation steps described in the previous paragraph has a similar effect.

3 OVERVIEW OF RECYCLING-BASED PROTOCOL VIA QUANTUM CHANNEL WITH LARGE ALPHABET

3.1 Overview

3.1.1 Teleportation is Inapplicable. Switching from the Cleve-Burhman model to the Yao model, suppose we are given a protocol Π using noiseless quantum communication, and we are asked to provide a protocol Π' using noisy quantum channels under the strongly adversarial model described earlier. In the absence of free entanglement, how can we protect quantum data from leaking to the environment without incurring a non-negligible overhead? First, note that some form of protection is necessary, as discussed in Section 1.2. Second, teleportation would be too expensive to use, since it incurs an overhead of at least 3: we have to pay for the MES as well as the classical communication required.

Surprisingly, an old and relatively unknown idea called the Quantum Vernam Cipher (QVC) [48] turns out to be a perfect alternative method to protect quantum data with negligible overhead as the noise rate approaches 0.

3.1.2 The Quantum Vernam Cipher (QVC) [48]. Suppose Alice and Bob share two copies of MESs, each over two d-dimensional systems. For Alice to send a message to Bob, she applies a controlled X^k Pauli operation with her half of the first MES as control (when the control qudit is in state k), and the message as the target. She applies a controlled Z^k Pauli operation from her half of the second MES to the message. When Bob receives the message, he reverses the controlled operations using his halves of the MESs. (The operations are similar for the opposite direction of communication). A detailed description is provided in the full paper.

The QVC is designed so that **if** Alice and Bob have access to an authenticated classical channel from Alice to Bob, they can determine and correct any error in the transmission. This can simply be done by measuring Z^l type changes to one half of the two MES. They can also run the QVC many times, determine the errors in a large block using a method called "random hashing", and recycle the MESs if the error rate (as defined in our adversarial model) is low. This is a crucial property of QVC and leads to one of the earliest (quantum) key recycling results known. In fact, this was the reason why it was studied in Ref. [48]. What makes QVC particularly suitable for our problem is that encoding and decoding are performed message-wise, while error detection can be done in large blocks, and entanglement can be recycled if no error is detected. It may thus be viewed as a natural quantum generalization to Haeupler's consistency checks.

3.1.3 Adaptations of QVC for the Current Problem. In the current scenario, we have neither free MESs nor an authenticated classical channel. Instead, Alice and Bob start the protocol by generating $O\left(\sqrt{\epsilon}n\right)$ near-perfect MESs, using high rate quantum error correcting codes over the low-noise channel, where n is the total length of the original protocol Π, and ϵ is the noise parameter. Then, they occasionally check for errors and recycle MESs in a communication efficient way, using noisy quantum channels instead of an authenticated classical channel. If they detect an inconsistency, they try to determine the error in a small block in the recent past, and reverse to correct the error. Otherwise, they perform "quantum hashing" [7, 48] to efficiently recycle the entanglement to be reused.

3.1.4 Additional Out-of-Sync Problems. As in the case of the teleportation-based protocol, it is also possible that, in the QVC-based protocol, one of Alice and Bob can make a step forward, and the other a step in reverse. They can also go out of sync about which MESs they are using. Furthermore, the parties may not agree on which MESs to recycle, how much to recycle, and whether they can even recycle! In particular, corruptions that lead only one party to recycle can cause a significant discrepancy in how many MESs the two parties are holding. It is much more involved to analyse the joint quantum state. To tackle these problems, we develop further data structures and adapt the "quantum hashing" procedure of Ref. [7, 48] to our setting.

Surprisingly, once again, the quantum data can be recovered as Alice and Bob reconcile the differences in the data structures developed for the task. This is in spite of the fact that there is no reason to expect the out-of-sync QVC to be sufficient to protect the potentially incorrectly encoded quantum data sent via noisy quantum channels.

We note that entanglement generation of $O\left(\sqrt{\epsilon}n\right)$ MES is sufficient to last through the whole protocol. Intuitively, this amount of MES is still much more than the number of adversarial errors allowed, even after taking into account the entanglement lost due to a single channel error.

A detailed solution to this case can be found in the full paper.

4 TRANSITIONING TO SMALL ALPHABET SIZE

4.1 Overview

We can witness the power of the framework when going from the two previous cases to work with small alphabet size. Great care is taken when establishing the framework in the large alphabet setting so as to make the transition to small alphabet largely seamless. One difficulty of applying the large alphabet coding scheme in the small alphabet case is that $O(\log n)$ messages are now required to exchange position information that is used for resynchronization. Following [36], we instead use a meeting point mechanism.

4.1.1 Haeupler's Meeting Point Mechanism. In Haeupler's meeting point mechanism, a set of positions (called meeting points) is specified, and Alice and Bob can reverse to these. In the presence of an observed inconsistency, the error is more likely to be recent than far back in the past. So, accordingly, the meeting points are spaced more closely near the current position, and are sparse back in the past so Alice and Bob typically only reverse a small number of steps (this is needed to limit the wasted communication caused by one error, as in Haeupler's general template described above). At the same time, there are only two meeting points considered at once by each party (with more distant ones considered iteratively if closer ones are believed to be *invalid*), so, they can be compared with $O(1)$ hashes.

4.1.2 Combining the Meeting Point Mechanism with Our Framework. Combining this meeting point idea with the framework we developed to solve the large alphabet cases leads to solutions for the small alphabet cases. The protocols for the noisy analogue to the Cleve-Buhrman model and the Yao model with full analysis are given in the full paper. When entanglement is free, we have used the given entanglement to generate useful secret keys. In the plain model, we adapt the protocol to prevent the adversary from injecting too many collisions in the hashes.

5 CONCLUSION

Implications of Our Results. In this work, we have studied the capacity of noisy quantum channels to implement two-way communication. In particular, we studied the ability of memoryless quantum channels to simulate interactive two-party communication, with the channel available in both directions, but without any assistance by side resources, e.g. classical side channels. As discussed in Section 1.1.4, this can be seen as a generalization of channel coding (which is discussed in Section 1.1.2), which is then the special case when all communication flows in one direction only. As discussed in Section 1.2.1, coding seems much harder in the interactive setting than in the one-way setting. Not much is known about the two-way quantum capacity. Despite this, it is not the case for all channels that the unassisted one-way capacity is at least as large as the unassisted two-way capacity. For example, the qubit erasure channel with erasure probability $\frac{1}{2}$ has no 1-way quantum capacity [6]. When the channel can be used in either direction, noisy back classical communication becomes possible, and one can lower bound the capacity by $\frac{1}{10}$ [6, 46]. A similar effect happens to the qubit depolarizing channel [7, 15]. Thus, comparing memoryless channels in the classical and the quantum setting, the one-way capacity of classical channels is always an upper bound on its two-way capacity, while we see that this does not hold for all quantum channels. For general memoryless quantum channels, the 2-way capacity is only known to be upper bounded by the entanglement-assisted quantum capacity Q_E [8, 9], which is equal to the quantum feedback capacity [11]. This bound is not tight (for example, for very noisy qubit depolarizing channel, 2-way capacity vanishes but $Q_E > 0$). Moreover, for the qubit depolarizing channel with noise rate ϵ, in the low noise regime, $Q_1 = 1 - H(\epsilon) + \epsilon \log 3 + O(\epsilon^2)$ [45]. We have established an achievable rate for the interactive setting of $1 - \Theta(\sqrt{\epsilon})$. If our conjectured optimality holds, the interactive capacity will be lower then Q_1 in the dependence on ϵ. Other potential quantum advantage due to the interaction include secret key expansion. These effects enrich the subject but also add to the challenge of determining the interactive capacity, and our work presents important progress in the low-noise regime.

A further implication of our result is that quantum communication complexity is very robust against transmission noise at low error rate. In particular, for alternating protocols like those considered in this paper and in most known protocols for quantum communication complexity, the overhead goes to one as the noise goes to zero, allowing one to get the full quantum advantage whenever such an advantage can be obtained.

Open Questions. Two questions stem directly from our work. First, we conjecture that a rate of $1 - O(\sqrt{\epsilon})$ is optimal. Is this conjecture true, and if so, what is the constant hidden in the O notation (up to leading order in ϵ)? Second, what is the optimal rate of communication in the high noise regime, for large ϵ?

Another important direction is concerning the fact that our coding scheme assumes that the protocol to be simulated is alternating, i.e., Alice and Bob alternate in sending qudits to each other. We believe that a lot of the machinery that we have developed should transpose well to study the more general setting where the protocol to be simulated has a more general structure, potentially with messages constructed from different number of qudits in different rounds. Once this is better understood, it would be important to perform a deeper investigation of the relationship between the different flavors of capacities for noisy quantum channels.

In the current work, we already have to deal with many types of synchronization errors at the teleportation, Quantum Vernam Cipher and quantum hashing level, for example. An interesting question from this point is: what about synchronization errors over the channel itself? There has been much interest in the classical interactive coding literature recently towards such type of errors [18, 37, 57]. How useful would the data structures that we develop here be to study the generalization of such errors to the quantum setting.

Many other interesting directions of research in the quantum setting stem from the other exciting directions that have been pursued recently in the classical setting, for example [3, 12–14, 16, 28, 29, 31, 32, 34, 35, 38]. We believe that our framework should be extendable to the study of many of these problems in the quantum setting.

Two other important questions that arise specifically in the quantum setting are the following. First, considering a larger fault-tolerant setting due to the inherently fragile nature of quantum data, can we also perform high rate interactive quantum communication when also the local quantum computation is noisy? Second, does quantum communication allow one to evade the classical no-go results obtained for interactive communication in a cryptographic setting [23, 33]? As we have seen in this work, the unique properties of quantum information can be helpful in the interactive communication setting, since we were able to achieve higher communication rate over fully adversarial binary channels in the plain model than the conjectured upper bound in the corresponding plain classical setting.

ACKNOWLEDGMENTS

D. Leung's research supported in part by an NSERC Discovery grant and a CIFAR research grant via the Quantum Information Science program; A. Nayak's research supported in part by NSERC Canada; A. Shayeghi's research supported in part by NSERC Canada and OGS; D. Touchette's research supported in part by NSERC, partly via PDF program, CIFAR and by Industry Canada; most of the work was done when P. Yao was the Hartree postdoc fellow in Joint Center for Quantum Information and Computer Science, University of Maryland, supported in part by the funding from Department of Defense; N. Yu's research supported in part by the Australian Research Council (Grant No: DE180100156). Part of the work was done while P. Yao visited the Perimeter Institute for Theoretical Physics (PI), and P. Yao thanks PI for its hospitality. Part of the work was done while N. Yu visited the Institute for Quantum Computing (IQC), and N. Yu thanks IQC for its hospitality. IQC and PI are supported in part by the Government of Canada and the Province of Ontario.

REFERENCES

[1] Scott Aaronson and Andris Ambainis. 2003. Quantum search of spatial regions. In *Proceedings of the 2003 IEEE 44th Annual Symposium on Foundations of Computer Science (FOCS '03)*. IEEE, 200–209.

[2] Erdal Arikan. 2009. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory* 55, 7 (July 2009), 3051–3073.

[3] Young-Han Kim Assaf Ben-Yishai, Ofer Shayevitz. 2017. Interactive Coding for Markovian Protocols. In *Proceedings of the 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton '17)*. IEEE, 870–877.

[4] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. 1993. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* 70, 13 (1993), 1895–1899.

[5] Charles H. Bennett, Gilles Brassard, Richard Jozsa, Dominic Mayers, Asher Peres, Benjamin Schumacher, and William K Wootters. 1994. Reduction of quantum entropy by reversible extraction of classical information. *Journal of Modern Optics* 41, 12 (1994), 2307–2314.

[6] Charles H. Bennett, David P. DiVincenzo, and John A. Smolin. 1997. Capacities of Quantum Erasure Channels. *Phys. Rev. Lett.* 78 (Apr 1997), 3217–3220. Issue 16.

[7] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. 1996. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* 54, 5 (1996), 3824–3851.

[8] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. 1999. Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.* 83, 15 (1999), 3081–3084.

[9] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. 2002. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory* 48, 10 (2002), 2637–2655.

[10] Hector Bombin. 2015. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New Journal of Physics* 17, 8 (2015), 083002.

[11] Garry Bowen. 2004. Quantum feedback channels. *IEEE Transactions on Information Theory* 50, 10 (2004), 2429–2434.

[12] Zvika Brakerski and Yael Tauman Kalai. 2012. Efficient interactive coding against adversarial noise. In *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS '12)*. IEEE, 160–166.

[13] Zvika Brakerski, Yael Tauman Kalai, and Moni Naor. 2014. Fast Interactive Coding Against Adversarial Noise. *J. ACM* 61, 6, Article 35 (Dec. 2014), 30 pages.

[14] Zvika Brakerski and Moni Naor. 2013. Fast algorithms for interactive coding. In *Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, 443–456.

[15] Gilles Brassard, Ashwin Nayak, Alain Tapp, Dave Touchette, and Falk Unger. 2014. Noisy interactive quantum communication. In *Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS '14)*. IEEE, 296–305.

[16] Mark Braverman and Klim Efremenko. 2017. List and Unique Coding for Interactive Communication in the Presence of Adversarial Noise. *SIAM J. Comput.* 46, 1 (2017), 388–428.

[17] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. 2015. Near-Optimal Bounds on Bounded-Round Quantum Communication Complexity of Disjointness. In *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS '15)*. IEEE Computer Society, Washington, DC, USA, 773–791.

[18] Mark Braverman, Ran Gelles, Jieming Mao, and Rafail Ostrovsky. 2017. Coding for interactive communication correcting insertions and deletions. *IEEE Transactions on Information Theory* 63, 10 (2017), 6256–6270.

[19] Mark Braverman and Anup Rao. 2014. Toward coding for maximum errors in interactive communication. *IEEE Transactions on Information Theory* 60, 11 (2014), 7248–7255.

[20] Harry Buhrman, Richard Cleve, and Avi Wigderson. 1998. Quantum vs. classical communication and computation. In *Proceedings of the 1998 ACM 30th Annual Symposium on Theory of Computing (STOC' 98)*. ACM, 63–68.

[21] A. R. Calderbank, Eric M. Rains, Peter W. Shor, and Neil J. A. Sloane. 1998. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory* (Jul 1998), 1369–1387.

[22] A. R. Calderbank and Peter W. Shor. 1996. Good quantum error-correcting codes exist. *Phys. Rev. A* 54 (Aug 1996), 1098–1105. Issue 2.

[23] Kai-Min Chung, Rafael Pass, and Sidharth Telang. 2013. Knowledge-preserving interactive coding. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS '13)*. IEEE, 449–458.

[24] Richard Cleve and Harry Buhrman. 1997. Substituting quantum entanglement for communication. *Phys. Rev. A* 56, 2 (1997), 1201–1204.

[25] Igor Devetak. 2005. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory* 51, 1 (2005), 44–55.

[26] Dennis G.B.J. Dieks. 1982. Communication by EPR devices. *Phys. Lett. A* 92, 6 (1982), 271–272.

[27] David DiVincenzo, Peter Shor, and John Smolin. 1998. Quantum-channel capacity of very noisy channels. *Physical Review A* 57, 2 (1998), 830–839.

[28] Klim Efremenko, Ran Gelles, and Bernhard Haeupler. 2015. Maximal Noise in Interactive Communication over Erasure Channels and Channels with Feedback. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science (ITCS '15)*. ACM, New York, NY, USA, 11–20.

[29] Matthew Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard J. Schulman. 2015. Optimal Coding for Streaming Authentication and Interactive Communication. *IEEE Transactions on Information Theory* 61, 1 (Jan 2015), 133–145.

[30] Ran Gelles. 2017. Coding for interactive communication: A survey. *Foundations and Trends in Theoretical Computer Science* 13, 1–2 (2017), 1–157.

[31] Ran Gelles, Ankur Moitra, and Amit Sahai. 2011. Efficient and explicit coding for interactive communication. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS '11)*. IEEE, 768–777.

[32] Ran Gelles, Ankur Moitra, and Amit Sahai. 2014. Efficient Coding for Interactive Communication. *IEEE Transactions on Information Theory* 60, 3 (March 2014), 1899–1913.

[33] Ran Gelles, Amit Sahai, and Akshay Wadia. 2015. Private interactive communication across an adversarial channel. *IEEE Transactions on Information Theory* 61, 12 (2015), 6860–6875.

[34] Mohsen Ghaffari and Bernhard Haeupler. 2014. Optimal error rates for interactive coding ii: Efficiency and list decoding. In *Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science (STOC '14)*. IEEE, 394–403.

[35] Mohsen Ghaffari, Bernhard Haeupler, and Madhu Sudan. 2014. Optimal Error Rates for Interactive Coding I: Adaptivity and Other Settings. In *Proceedings of the 2014 ACM 46th Annual ACM Symposium on Theory of Computing (STOC '14)*. ACM, New York, NY, USA, 794–803.

[36] Bernhard Haeupler. 2014. Interactive Channel Capacity Revisited. In *Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS '14)*. IEEE Computer Society, Washington, DC, USA, 226–235.

[37] Bernhard Haeupler, Amirbehshad Shahrasbi, and Ellen Vitercik. 2017. Synchronization Strings: Channel Simulations and Interactive Coding for Insertions and Deletions. *arXiv preprint arXiv:1707.04233* (2017).

[38] Bernhard Haeupler and Ameya Velingker. 2017. Bridging the Capacity Gap Between Interactive and One-way Communication. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2123–2142.

[39] Matthew B. Hastings. 2009. Superadditivity of communication capacity using entangled inputs. *Nature Physics* 5, 4 (2009), 255.

[40] Alexander S. Holevo. 1998. The Capacity of the Quantum Channel with General Signal States. *IEEE Transactions on Information Theory* 44, 1 (1998), 269–273.

[41] Peter Høyer and Ronald De Wolf. 2002. Improved quantum communication complexity bounds for disjointness and equality. In *Proceedings of the 2002 Symposium on Theoretical Aspects of Computer Science (STACS '02)*. Springer, 299–310.

[42] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. 2003. A lower bound for the bounded round quantum communication complexity of set disjointness. In *Proceedings of the 2003 IEEE 44th Annual Symposium on Foundations of Computer Science (FOCS '03)*. IEEE, 220–229.

[43] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman. 2007. Interaction in quantum communication. *IEEE Transactions on Information Theory* 53, 6 (2007), 1970–1982.

[44] Gillat Kol and Ran Raz. 2013. Interactive channel capacity. In *Proceedings of the 2013 ACM 45th Annual Symposium on Theory of Computing (STOC '13)*. ACM, 715–724.

[45] Felix Leditzky, Debbie Leung, and Graeme Smith. 2017. Quantum and private capacities of low-noise channels. arXiv preprint arXiv:1705.04335.

[46] Debbie Leung, Joungkeun Lim, and Peter Shor. 2009. Capacity of Quantum Erasure Channel Assisted by Backwards Classical Communication. *Phys. Rev. Lett.* 103 (Dec 2009), 240505. Issue 24.

[47] Debbie Leung, Ashwin Nayak, Ala Shayeghi, Dave Touchette, Penghui Yao, and Nengkun Yu. 2018. Capacity approaching coding for low noise interactive quantum communication. To appear on arXiv.

[48] Debbie W. Leung. 2002. Quantum Vernam Cipher. *Quantum Info. Comput.* 2, 1 (Dec. 2002), 14–34.

[49] Seth Lloyd. 1997. Capacity of the noisy quantum channel. *Phys. Rev. A* 55, 3 (1997), 1613–1622.

[50] Ran Raz. 1999. Exponential separation of quantum and classical communication complexity. In *Proceedings of the 1999 ACM 31st Annual Symposium on Theory of Computing (STOC '99)*. ACM, 358–367.

[51] Oded Regev and Boáz Klartag. 2011. Quantum one-way communication can be exponentially stronger than classical communication. In *Proceedings of the 2011 ACM 43rd Annual Symposium on Theory of Computing (STOC '11)*. ACM, 31–40.

[52] Leonard J. Schulman. 1992. Communication on noisy channels: A coding theorem for computation. In *Proceedings of the 1992 IEEE 33rd Annual Symposium on Foundations of Computer Science (FOCS '92)*. IEEE, 724–733.

[53] Leonard J. Schulman. 1993. Deterministic coding for interactive communication. In *Proceedings of the 1993 ACM 25th Annual Symposium on Theory of Computing (STOC '93)*. ACM, 747–756.

[54] Leonard J. Schulman. 1996. Coding for interactive communication. *IEEE Transactions on Information Theory* 42, 6 (1996), 1745–1756.

[55] Benjamin Schumacher and Michael D. Westmoreland. 1997. Sending classical information via noisy quantum channels. *Phys. Rev. A* 56, 1 (1997), 131–138.

[56] Claude E. Shannon. 1948. A mathematical theory of communication. *Bell System Tech. J.* 27 (1948), 379–423, 623–656.

[57] Alexander A. Sherstov and Pei Wu. 2017. Optimal Interactive Coding for Insertions, Deletions, and Substitutions. In *Proceedings of the 2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS '17)*. IEEE, 240–251.

[58] Peter W. Shor. 2002. The quantum channel capacity and coherent information. Lecture notes, MSRI Workshop on Quantum Computation.

[59] Graeme Smith and Jon Yard. 2008. Quantum communication with zero-capacity channels. *Science* 321, 5897 (2008), 1812–1815.

[60] Norbert Stolte. 2002. *Rekursive Codes mit der Plotkin-Konstruktion und ihre Decodierung*. Ph.D. Dissertation. TU Darmstadt, Fachbereich Elektrotechnik und Informationstechnik,.

[61] William K. Wootters and Wojciech H. Zurek. 1982. A single quantum cannot be cloned. *Nature* 299, 5886 (1982), 802–803.

[62] Andrew Chi-Chih Yao. 1993. Quantum circuit complexity. In *Proceedings of the 1993 IEEE 34th Annual Symposium on Foundations of Computer Science (FOCS '93)*. IEEE, 352–361.