Noisy Interactive Quantum Communication

(Extended Abstract)

Gilles Brassard*†, Ashwin Nayak‡, Alain Tapp*, Dave Touchette* and Falk Unger§
*Département d'informatique et de recherche opérationnelle
Université de Montréal
Email: brassard@iro.umontreal.ca, alain.tapp@gmail.com, touchette.dave@gmail.com
†CIFAR and ETH-ITS
‡Department of Combinatorics and Optimization, and
Institute for Quantum Computing
University of Waterloo
Email: anayak@uwaterloo.ca
§No Affiliation
Email: falk.unger@gmail.com

***Abstract*—We study the problem of simulating protocols in a quantum communication setting over noisy channels. This problem falls at the intersection of quantum information theory and quantum communication complexity, and will be of importance for eventual real-world applications of interactive quantum protocols, which can be proved to have exponentially lower communication costs than their classical counterparts for some problems. These are the first results concerning the quantum version of this problem, originally studied by Schulman in a classical setting (FOCS '92, STOC '93). We simulate a length N quantum communication protocol by a length $O(N)$ protocol with arbitrarily small error. Our simulation strategy has a far higher communication rate than a naive one that encodes separately each particular round of communication to achieve comparable success. Such a strategy would have a communication rate going to 0 in the worst interaction case as the length of the protocols increases, in contrast to our strategy, which has a communication rate proportional to the capacity of the channel used. Under adversarial noise, our strategy can withstand, for arbitrarily small $\varepsilon > 0$, error rates as high as $1/2 - \varepsilon$ when parties preshare perfect entanglement, but the classical channel is noisy. We show that this is optimal. Note that in this model, the naive strategy would not work for any constant fraction of errors. We provide extension of these results in several other models of communication, including when also the entanglement is noisy, and when there is no pre-shared entanglement but communication is quantum and noisy. We also study the case of random noise, for which we provide simulation protocols with positive communication rates and no pre-shared entanglement over some quantum channels with quantum capacity $Q = 0$, proving that Q is in general not the right characterization of a channel's capacity for interactive quantum communication. Our results are stated for a general quantum communication protocol in which Alice and Bob collaborate, and hold in particular in the quantum communication complexity settings of the Yao and Cleve-Buhrman models.**

***Keywords*—Coding Theory; Communication Complexity; Quantum Computation and Information;**

I. Introduction

Quantum information theory is well developed for information transmission over noisy quantum channels, dating back to the work of Holevo in the 70's [21], [22], for the transmission of classical information [23], [32], quantum information [25], [34], [14], and even if we allow for pre-shared entanglement between sender and receiver [4], [5]. It describes the ultimate limits for (unidirectional) data transmission over noisy quantum channels without concern for explicit, efficient construction of codes. Closely related is the area of quantum coding theory, which takes a more practical approach toward the construction of quantum error correcting codes [33], [35] by providing explicit and efficient constructions [12], [35], [19], [11], and by providing bounds on their existence [11], [16], [28].

Quantum communication complexity has also been studied in depth since Yao's seminal paper introduced the field in 1993 [41]. It is an idealized setting in which local computation is deemed free and communication noiseless but expensive. Two parties want to compute a classical function of their joint input while minimizing the number of qubits they have to exchange. Exponential separations have been shown for some promise problems between their classical and quantum communication complexity [10], even if we allow bounded error [36]. Moreover, for both classical and quantum communication complexity, interaction has been proved to be a powerful resource: exponential separations in the communication complexity of some functions have also been established between protocols restricted to k messages, and protocols with $k+1$ messages [27], [20]. In 1997, Cleve and Buhrman [13] defined an alternative model for communication complexity in a quantum setting, in which the players are allowed to pre-share an arbitrary entangled state but transmit classical rather than quantum bits. This model is at least as powerful as Yao's (up to a factor of 2), since entanglement can be used to teleport [2] the message qubits with twice as many classical bits. It is still open whether the two models are essentially equivalent, since no good bound on the amount of entanglement required in the Cleve-Buhrman model is known.

Quantum communication, even more so than classical communication, is prone to transmission errors in the real world. With the ubiquity of distributed computing nowadays, it has become increasingly important to develop an information and coding theory for interactive protocols. In the realm of

classical communication, Schulman initiated the field with his pioneering works [29], [30], [31], showing that it is possible to simulate any protocol defined over a noiseless channel with a noisy channel with exponentially small probability of error while only dilating the protocol by a constant factor. This multiplicative dilation factor, in the case of a binary symmetric channel, is proportional to the inverse of the capacity, as in the data transmission case. However, the hidden constant of proportionality does not go to 1 asymptotically. For adversarial errors, Schulman also shows how to withstand corruption up to a rate of $\frac{1}{240}$. Recent work by Braverman and Rao [9] shows how to withstand error rates of $\frac{1}{4} - \varepsilon$ in the case of an adversarial channel, and they also show this is optimal in their model of noisy communication. Even more recently, Franklin, Gelles, Ostrovsky and Schulman [17] were able to show that in an alternative model in which Alice and Bob are allowed to share a secret key unknown to the adversary Eve, they can withstand error rates up to $\frac{1}{2} - \varepsilon$, which is also shown to be optimal in their model. All of the above simulations use *tree codes*, which were introduced by Schulman. Tree codes exist for various parameters, but no efficient construction is known. A relaxation of the tree code condition still strong enough for most applications in interactive coding was proposed by Gelles, Moitra and Sahai [18], and they provided an efficient randomized construction for these so-called *potent* tree codes. Using these in a random error model leads to efficient decoding on the average, hence to efficient simulation protocols (of course, given black-box access to the original protocol, which might be inefficient in itself). In a worst-case adversarial scenario, the decoding might still take exponential time with potent tree codes. It was only recently that an alternative coding strategy developed by Brakerski and Kalai [6] was able to address the adversarial error case efficiently. Their strategy is to cleverly split the communication into blocks of logarithmic length in which tree encoding is used. In addition, they send, in between the blocks, some history information that enables efficient decoding. This construction was further improved by Brakerski and Naor [7]. A survey article by Braverman [8] provides a good overview of results and open questions in the area of classical interactive communication circa 2011, though some of the important questions raised there have been addressed since. In particular, the question of interactive capacity of binary symmetric channels was recently investigated by Kol and Raz [24]. For this channel they find that indeed, in the low noise regime, the communication capacity behaves differently in the asymptotic limit of long interactive protocols than in the data transmission case.

The approach taken in all of the above is inherently classical and does not generalize well to the quantum setting. In particular, the fact that classical information can be copied and resent multiple times is implicitly used, and therefore the fact that the information in the communication register can be destroyed by noise is inconsequential. In contrast, the no-cloning theorem of quantum theory [15], [40] rules out copying of quantum messages. As a result, if the information in some communication register is destroyed, it cannot be resent. A naive strategy, which applies in the quantum as well as in the classical case, would be to encode each round separately. However, in a random error model, a constant dilation of each round would not be sufficient to achieve constant fidelity in the worst case of one-qubit transmission per round, and a super-constant dilation leads to a communication rate of zero asymptotically. Moreover, in the case of adversarial errors, no constant rate of error can be withstood with such a strategy unless the number of rounds is constant: the adversary can always disrupt a whole block. The properties of classical information made it possible for Schulman and his successors to design clever classical simulation protocols that can withstand constant error rates at constant communication rates, and succeed in simulating classical protocols designed for noiseless channels over noisy channels by reproducing the whole transcript of the noiseless protocol. However, it was not obvious that it is possible, given an arbitrary protocol designed for a noiseless bidirectional quantum channel, to simulate it over noisy quantum channels with constant error rate at a constant communication rate. Even for protocols in the Cleve-Buhrman model, in which the communication is classical, it is not clear that we can achieve results similar to those for classical protocols. Indeed, a quantum measurement is in general irreversible. If such a measurement is performed on the shared entangled state and the players later realize that the measurement was based on wrong classical information, the naive adaptation of the classical simulation to the Cleve-Buhrman model fails.

II. Overview of Results

We show that despite the above obstacles, it is indeed possible to simulate arbitrary quantum protocols over noisy quantum channels with good communication rates. We consider two models for interaction over noisy channels. One is analogous to Yao's model, and all communication in it is over noisy quantum channels, but the parties do not pre-share entanglement. The other is analogous to the Cleve-Buhrman model, and all communication in it is over noisy classical channels and parties are allowed to pre-share noiseless entanglement. We call these models the *quantum* and *shared entanglement models*, respectively. We also consider a further variation on the shared entanglement model in which entanglement is also noisy.

This extended abstract focuses on the model with perfect shared entanglement but adversarial noise on the classical communication. In such a context, the number of errors is defined to be the Hamming distance between the transcript of sent messages and the transcript of possibly corrupted received messages. Messages are over a constant size alphabet, and the error rate is the worst-case ratio between the number of errors and the number of such messages sent, i.e. the transcript length. Note that in this model, it is possible for the honest parties to generate a secret key unknown to the adversary by measuring their shared entanglement. Details about the other models of communication appear in Ref. [3]. Most of our technical contribution goes into showing that a constant dilation factor on the communication suffices to withstand an adversarial error rate of $\frac{1}{2} - \varepsilon$ in the shared entanglement model, for arbitrarily small $\varepsilon > 0$. This is optimal, and matches the highest tolerable error rate in the analogous shared secret key model for classical interactive communication [17]. There are two main components going into establishing this result.

First, we need to establish a framework for simulating quantum protocols over noisy channels. To avoid losing quantum information, the approach we take is to teleport [2] the quantum communication register back and forth. When the

register is in some party's possession, this party tries to evolve the simulation by applying one of his unitaries in the noiseless protocol, or one of its inverses if he realizes at some point he applied it wrongly before. The important point is that all operations on the quantum registers are reversible, being a sequence of noiseless protocol unitaries and random (but known) Pauli operators. Of particular importance to our work is the notion of tree codes as introduced by Schulman, which the players use to transmit classical information.

As described in a recent paper on efficient interactive coding [7], the high-level logic of all solutions proposed until now for classical protocol simulation can be summarized as follows: the parties try to evolve the protocol, and if they later realize there has been some error, they try to go back to the point where they last agreed (in a protocol tree representation, this would be their least common ancestor). In our approach for quantum protocols, the parties try to follow roughly the same idea, but for two reasons are not able to do this passively. First, there is no underlying transcript (or protocol tree) that the parties try to synchronize, except that they wish to evolve the correct sequence of unitaries. By the no-cloning theorem [15], [40], the parties cannot restart with a copy of the quantum information received up to some earlier point. Instead they have to actively rewind previous unitaries and wrong teleportation decodings until a suitable point in the protocol. Second, when they try to synchronize in this manner, they actively teleport, potentially leading to more errors on the joint quantum register.

An important ingredient in our simulation is the representation for noisy quantum protocols that we develop. As said before, in quantum protocols there is no direct analogue of a protocol tree representation that enables one to keep track exactly and explicitly of the evolution of the noiseless protocol simulation. The cleaned-up form (2) of our representation provides in some sense a quantum analogue of a protocol tree representation. As the classical representation, it enables an exact and explicit assessment of the evolution of the noiseless protocol simulation, as well as that of the departure from it due to noise.

At this point, it might look like we have reduced our problem to the classical case, since the parties only transmit classical information—the teleportation measurement outcomes. This enables us to reuse tools from classical interactive coding, most notably tree codes, but the design of the quantum simulation protocol needs extra care. Unlike the classical case, agreement by the two parties on a common classical transcript is not sufficient. This transcript consists mostly of random teleportation measurement outcomes and is useless by itself. We additionally need to maintain a joint quantum state that eventually evolves according to the original protocol.

Once we realize the importance of teleportation in the context of noisy communication, and carefully design the simulation protocol, it may not come as a surprise that the simulation incurs only a constant factor overhead. The need for backtracking in the quantum simulation, however, seems to impose serious constraints on the tolerable error rate. *A priori* it is entirely unclear that we could hope to circumvent the low error tolerance seen in simulations with backtracking. The second part of our main contribution is to develop the necessary techniques to prove that we *can* tolerate an error rate as high as $\frac{1}{2} - \varepsilon$. These techniques are indeed novel, and will be used in a forthcoming article to improve on previously known *classical* results; more on this later.

Indeed, all recent classical schemes tolerating high error rates have the property that the parties always go forward with the communication by using the tree structure of classical protocols. In comparison, in the original Schulman tree code based scheme there is some form of backtracking, due to which the scheme could only tolerate a much lower adversarial error rate of $\frac{1}{240}$. This is due to the fact that in a protocol with backtracking [31], the fraction of good rounds, in which both players correctly decode the tree code transmission, must be higher for the simulation to succeed than in a protocol that always goes forward by transmitting edges of a pointer jumping problem [9], [17]. There also is some form of backtracking in the outer level of the computationally efficient protocol of Ref. [6], thus limiting the overall error rate that can be tolerated to a fourth of that of the inefficient protocol used at the inner level. Hence, known computationally efficient protocols in the shared secret key communication model can only tolerate error rate up to $\frac{1}{8}$ [17]. In light of these results, it is clear that previously used techniques would not suffice to tolerate error rates as high as $\frac{1}{2} - \varepsilon$ for our protocol, which requires backtracking. The new techniques we develop are thus unavoidable.

To achieve higher error tolerance, we follow Ref. [17] and use a *blueberry code* to effectively turn most adversarial errors into erasures. Concatenating such a code on top of a tree code yields a tree code with an erasure symbol. Since general transmission errors are twice as harmful as erasures for the tree code condition, which is stated in terms of Hamming distance, it was shown in Ref. [17] that if the error rate is below $\frac{1}{2} - \varepsilon$, then the large number of rounds in which both parties correctly decode a long enough prefix is sufficient to imply success of the simulation. Once again due to backtracking, this condition is not sufficient for our purpose and in particular blueberry codes by themselves are not sufficient to improve error tolerance up to $\frac{1}{2}$ here. For us, the number of rounds in which both parties decode correctly even the whole string could be high, but if these rounds alternate with rounds in which at least one of the parties makes a decoding error, then the protocol could stall, and simulation would fail. To circumvent this possibility, we need to bound the number of rounds with bad tree code decoding. Previously known bounds on this [31] can be used to show success of our simulation, but are far from enabling us to tolerate up to $\frac{1}{2}$ error rate. We develop a new bound on tree codes with an erasure symbol, Lemma 2, which might be of independent interest for classical interactive coding. This bound enables us to tightly control this quantity. Once we control the number of rounds with bad decoding, it is also important to insure that even when there is a corruption detected as an erasure in a round, as long as there is no bad decoding, the protocol will not need to spend a good round to correct for this previous erasure round.

In fact, the techniques that we develop are not only powerful enough to prove that our quantum protocol can tolerate the maximum error rate of $\frac{1}{2} - \varepsilon$, but they can be used to improve on known classical results in the classical setting. Indeed, we will show in upcoming works [37] how Lemma 2 can be used to obtain a strengthening of the theorem of Ref. [17]

in the *classical* shared secret key model, and then how our techniques can be applied with this strengthened theorem and the techniques of Ref. [6] to obtain computationally efficient simulation protocols in this model that can also tolerate error rate up to $\frac{1}{2}$. To the best of our knowledge, this will provide the first example of a computationally efficient protocol that can tolerate maximum adversarial error rate in some classical communication model, hence demonstrating the power of our techniques.

We can adapt the techniques that we develop in the shared entanglement model for the quantum communication model: we first distribute a linear amount of entanglement using standard quantum information and coding theory techniques. This leads to a tolerable adversarial error rate of up to $\frac{1}{6}$ in the quantum model, close to the best achievable for perfect quantum data transmission at $\frac{1}{4}$. This is better than the factor of two drop that might be expected if we compare classical interactive coding to unidirectional coding. We can also adapt our techniques for an adversarial error model to the case of a random error model. Then, dilation factors proportional to $\frac{1}{Q}$ for a depolarizing channel of quantum capacity Q in the quantum model, and proportional to $\frac{1}{C}$ for a binary symmetric channel of capacity C in the shared entanglement model, are sufficient. We also show that the result in the shared entanglement model is asymptotically optimal: there exists a family of binary functions for which a dilation factor proportional to $\frac{1}{C}$ is necessary. When considering noisy entanglement in the form of noisy EPR pairs in a Werner state [38], we give, for any non-separable Werner state, simulation protocols with linear noisy classical communication and noisy EPR pair consumption. The techniques developed in this case can be adapted to show that the use of depolarizing channels in both directions enables the simulation to succeed whenever the quantum capacity with two-way classical communication, Q_2, is strictly positive. For some range of the depolarizing parameter, $Q = 0$ but $Q_2 > 0$, so this proves that Q does not characterize a quantum channel's capacity for interactive quantum communication.

Due to the use of tree codes, the protocols presented in this paper are not computationally efficient. However, it is possible to extend classical results on efficient interactive coding tolerating maximum error to noisy quantum communication. The representation of noisy protocols mentioned above is quite powerful and will be used in forthcoming papers to adapt classical results on computationally efficient interactive computation over adversarial channels [6] and on the interactive capacity of random noise channels [24] to the quantum regime.

Organization: The paper is structured as follows: in section III, we set up the notation and state the relevant definitions, in particular for the different models of communication. In section IV, we state and prove our main result for the adversarial case in the shared entanglement model. Section V shows how to adapt the result of the previous section to obtain various other interesting results, in particular for the quantum model, the noisy shared entanglement model, and in the case of a random error model. We conclude with a discussion of our results and further research directions. The full version of this article will contain technical details; a draft is already available [3].

III. Preliminaries

A. Quantum Mechanics and Quantum Communication Complexity

We briefly review some notions necessary for the remainder of the paper. A more detailed preliminary section can be found in Ref. [3]. We alternate between two standard formalisms for quantum theory: the pure state formalism is used when discussing noiseless quantum protocols, and the more general density operator formalism is used when discussing noisy quantum protocols. The notation used is quite standard and mostly follows that of Refs [26], [39].

As a building block for our simulation protocols, we use the standard teleportation protocol [2], in which the necessary decoding at the receiver's side is given by the Pauli operators X and Z. We denote the evolution under the consecutive action of unitaries U_j's as $\prod_{j=1}^{\ell} U_j |\psi\rangle = U_\ell \cdots U_1 |\psi\rangle$. We measure the success of the simulation against some adversary by comparing the induced noisy channel with the one induced by the noiseless protocol. An appropriate measure of distance between two channels $\mathcal{N}$ and $\mathcal{M}$ uses the diamond norm [1]: $\|\mathcal{N} - \mathcal{M}\|_\diamond$.

As discussed in the introduction, the two models for quantum communication complexity that are most commonly studied in the literature are the one due to Yao [41] and the one due to Cleve and Buhrman [13]. To bring protocols in these models into a form that fits the framework of section III-B, we replace all irreversible operations by their coherent version: measurements are replaced by pseudo-measurements, classically controlled operations by quantumly controlled ones, and then classical communication is replaced by quantum communication. At this point, the main difference between the two models is that one permits an arbitrary entangled initial state and the other does not.

B. Quantum Communication Model

We give a succinct treatment of our communication models. A *noiseless* protocol Π is defined by a sequence of unitaries $U_1^{AC}, U_2^{BC} \cdots, U_{N+1}$. We need $N+1$ unitaries in order to have N messages since a first unitary is applied before the first message is sent and a last one after the final message is received. Such a protocol is run on an input state $|\psi_{\text{init}}\rangle^{A\tilde{B}CE}$, with the following registers: A is held by Alice, B is held by Bob, C is the communication register exchanged back-and-forth between Alice and Bob, and E is a reference register that might be held by an adversary Eve. At the end of the protocol, the output state is $\Pi(|\psi_{\text{init}}\rangle) = \text{Tr}_E(|\psi_{\text{final}}\rangle\langle\psi_{\text{final}}|^{ABCE})$, for $|\psi_{\text{final}}\rangle = U_{N+1} \cdots U_1 |\psi_{\text{init}}\rangle$. We abuse notation and also denote the induced quantum channel by Π. We restrict ourselves to the case of a single-qubit communication register C, which is the worst case for noisy interactive communication. Every protocol can be converted into such a form by increasing the communication by a factor of at most two.

We later *embed* length N noiseless protocols into others of larger length $N' > N$. To do so, we define some dummy registers $\tilde{A}, \tilde{B}, \tilde{C}$ isomorphic to A, B, C, respectively. $\tilde{A}$ and $\tilde{C}$ are part of Alice's registers and $\tilde{B}$ is part of Bob's registers. Then, for any isomorphic quantum registers $D, \tilde{D}$, let $\text{SWAP}_{D \leftrightarrow \tilde{D}}$ denote the quantum unitary that swaps

the $D, \tilde{D}$ registers. In a noiseless protocol embedding, for $i \in \{1, 2, \cdots N-1\}$, we leave U_i untouched. We replace U_N by $\text{SWAP}_{B\leftrightarrow\tilde{B}} U_N$ and U_{N+1} by $\text{SWAP}_{AC\leftrightarrow\tilde{A}\tilde{C}} U_{N+1}$. Finally, for $i \in \{N+2, N+3, \cdots N'+1\}$, we define $U_i = I$, the identity operator.

We refer later to the *unidirectional* model; in this noiseless model, there is a unique communication of some large quantum register, so a unidirectional protocol $\mathcal{U}$ is defined by two quantum channels, $\mathcal{M}_1$ acting jointly on Alice's side and on the communication register, and $\mathcal{M}_2$ acting similarly on Bob's side after reception of the communication register. On input a state $|\psi\rangle$, the output of $\mathcal{U}$ is the state of the ABC subsystems of $\mathcal{M}_2\mathcal{M}_1(|\psi\rangle)$, and is denoted $\mathcal{U}(|\psi\rangle)$. We abuse notation and also denote by $\mathcal{U}$ the induced quantum channel.

For simplicity, we define below what we refer to as *alternating* communication models, in which Alice and Bob take turn in transmitting the communication register to each other. The definitions easily extend to somewhat more general communication models referred to as *oblivious* models, in which Alice and Bob speak in a fixed order, but not necessarily in alternation.

A *simulation* protocol Q in the quantum model is defined by a sequence of quantum channels $\mathcal{M}_1^{A'C'}, \mathcal{M}_2^{B'C'}, \cdots, \mathcal{M}_{N'+1}$, in which the A' system contains all of Alice's local registers, B' contains those of Bob, and C' is the quantum communication register exchanged back-and-forth between Alice and Bob by passing through Eve's hand. Similarly, an *adversary* E^Q is modelled by a sequence of quantum channels $\mathcal{N}_1^{E'C'}, \cdots, \mathcal{N}_{N'}^{E'C'}$, with E' containing all of Eve's local registers. When running the simulation protocol Q with black-box access to a noiseless protocol Π against adversary E^Q on input $|\psi\rangle$, the output is the $\tilde{A}\tilde{B}\tilde{C}$ subsystems (of the embedded noiseless protocol) of $Q^\Pi(E^Q(|\psi\rangle)) = \mathcal{M}^\Pi_{N'+1}\mathcal{N}_{N'}\cdots\mathcal{N}_1\mathcal{M}^\Pi_1(|\psi\rangle)$, and we denote the induced quantum channel by $Q^\Pi(E^Q)$. We consider two noise models. In a *random* error model (analogous to that studied in quantum information theory, à la Shannon), Eve is a non-malicious passive environment, and $\mathcal{N}_i = \mathcal{N}^Q$ for some fixed quantum channel $\mathcal{N}^Q$. In an *adversarial* error model (analogous to that studied in quantum coding theory, à la Hamming), Eve is a malicious adversary who wants to make the protocol fail, and we are interested in adversaries with a bound δ on the fraction of communications of the C' register they corrupt. See Ref. [3] for a precise definition of the error model.

A simulation protocol S and an adversary E^S in the shared entanglement model are defined analogously, with C' being instead a classical communication register that passes through Eve's hand, and that can be copied perfectly without inducing any error.

C. Classical Communication Protocols and Online Codes

Our simulation protocols have an important classical component. To make them resilient to noise, we use two different online classical codes that can perform encoding and decoding round by round. *Tree* codes were introduced by Schulman [31] for the purpose of interactive communication, and have a self-healing property that enables them to correct errors if sufficiently many error-free transmissions are received subsequently. They are parameterized by the message alphabet size $d > 1$, the transmission alphabet size q, the number of rounds of communication N and a distance parameter $0 < \alpha < 1$. The larger α, the stronger the self-healing property. In each round, a message from the message set $[d] = \{1, \cdots, d\}$ is encoded, and a symbol from the transmission alphabet is sent. Schulman proved that for any d and α, a constant size transmission alphabet suffices to generate a family of tree codes of any length N. We also use a randomized error detection code called the *blueberry* code [17]. Alice and Bob need to share a secret key unknown to Eve to use this code, and then each corruption of Eve is detected as an erasure with probability β. For any message set size and parameter $0 < \beta < 1$, there exists a large enough transmission alphabet size and corresponding secret key size sufficient to obtain a blueberry code with erasure parameter β. That is, for any transmitted symbol corrupted by the channel, the probability of detection as an erasure by the receiver is at least β in any round, independently of other rounds.

IV. Tolerating Maximal Error Rates

A. Results

We focus on the shared entanglement model. Techniques to distribute entanglement in both random [25], [34], [14] and adversarial [11], [16], [28] error models are well-studied. We can combine our findings with these entanglement distribution techniques to translate results in the shared entanglement model to the quantum model. We first focus on an adversarial error model, and then adapt these results to a random error model. Such extensions to other communication models are explored in section V.

We describe a simulation protocol that tolerates up to $\frac{1}{2} - \varepsilon$ error rate, for arbitrarily small $\varepsilon > 0$, in the shared entanglement model. This is optimal: we also prove that no interactive protocol can withstand an error rate of $\frac{1}{2}$ in this model. Our protocol achieves asymptotically positive communication rate and entanglement consumption linear in the communication. This provides an interactive analogue of a family of good quantum codes tolerating maximal error. Formal statements along with a detailed description of the protocol and proofs can be found in Ref. [3].

Theorem 1: Given any two-party quantum protocol of length N in the noiseless model, no simulation protocol in the shared entanglement model can tolerate an error rate of $\frac{1}{2}$ and succeed in simulating the noiseless protocol with lower worst-case error than the best unidirectional protocol. This result holds in the oblivious as well as the alternating communication models.

Theorem 2: Given an adversarial channel in the shared entanglement model with error rate strictly smaller than $\frac{1}{2}$, we can simulate any noiseless protocol of length N with negligible error over this channel using a number of constant-size transmissions linear in N, and consuming a linear number of EPR pairs.

To prove Th. 1, the argument of Ref. [17] in the classical case applies here as well: we only need to notice that if the error rate is $\frac{1}{2}$ with oblivious communication in the shared

entanglement model, then an adversary can completely corrupt all of the transmissions of either Alice or Bob, whoever talks at most half the time.

Theorem 2 is proven below.

B. Proof of Achievability

1) Description of the Simulation: Let us first give some intuition on how to succeed in simulating a noiseless quantum protocol over a noisy channel. The strategy to avoid losing the quantum information in the communication register over the noisy channel is to teleport the C register of the noiseless protocol back and forth, creating a virtual C register that is either in Alice's or in Bob's hand. They use their shared entanglement to do so, as well as the provided noisy classical channels to transmit their teleportation measurement outcomes. Whenever Alice possesses the virtual C register she can try to evolve the simulation of the noiseless protocol by applying one of her noiseless protocol unitaries on the virtual AC register, and similarly for Bob on the virtual BC register. If they later realize that there has been some error in the teleportation decoding, they might have to apply inverses of these operations, but overall, all operations on the virtual ABC quantum register can be described as an intertwined sequence of Pauli operators acting on the C register and noiseless protocol unitaries (and their inverses) acting on the AC and the BC registers. There are two important things to notice here. First, the sequence of operations acting on the joint register is a sequence of reversible unitaries. Hence, if the parties keep track of the sequence of operations on the joint register, at least one of the parties can reverse any of his operations when he is in possession of the virtual C register. Second, both parties know the order in which these operators have been applied while only one knows exactly which one was applied: for Pauli operators, both parties know $\pm X^x Z^z$ is applied at some point, but only one knows for sure the value of $xz \in \{0,1\}^2$, and similarly both know U_j^M (with $U_j^{+1} = U_j, U_j^{-1} = U_j^\dagger, U_j^0 = I$) is applied at some point, but only one knows for sure the values of $j \in \{1, \cdots, N'+1\}$ and $M \in \{-1, 0, +1\}$. This is the classical information they try to transmit each other so that both can know exactly the sequence of operations that have been applied to the joint register. The tree codes of Schulman are particularly well suited for protecting against noise in this interactive scenario.

More concretely, in each round the parties first need to decode the teleportation before trying to evolve the simulation of the quantum protocol and finally teleporting back the communication register to the other party. The goal is that the parties know exactly where they are in the simulation of the protocol (i.e., the sequence of unitaries that have been applied to the virtual protocol registers) when they are able to correctly decode all the classical messages sent by the other party. To enable a party to learn exactly what action was taken by the other party in the earlier rounds, the message sent in each round is in $\{0,1\}^2 \times \{-1,0,+1\} \times \{0,1\}^2$, encoded with a tree code. The first pair of bits corresponds to the teleportation decoding operation done at the beginning of a party's turn. The trit is associated with the evolution in the noiseless protocol: $+1$ stands for going forward with the protocol, a unitary of the noiseless protocol was applied to the joint state of the party's local register and the communication register; -1 stands for going backward with the protocol, the inverse of a unitary of the noiseless protocol applied by that party to the joint state was performed; 0 stands for holding the protocol idle, no action is taken by that party to evolve the protocol in that round. Note that the index j of the unitary U_j^M a party applies can be computed solely from the sequence of trits sent by that party. Finally, the last pair of bits corresponds to the outcome of the measurement in the teleportation of the communication register, to enable the other party to correctly decode the teleportation.

For each party, we call his *history* at some point the sequence of these triplets of messages he transmitted up to that point. If a party succeeds in correctly decoding the history of the other party, he then possesses all the information about the operations that were applied on the joint quantum register, and can choose his next move accordingly. Note that the information about which Pauli operator was used to decode the teleportation might appear to be redundant, but it is not when there are decoding errors. This is a bit of a subtle and important point, so let us explain in more detail what we mean here. In the case of decoding errors, the wrong Pauli operator might be applied to do the teleportation decoding. Even though the party who applied the wrong Pauli operator will later realize his mistake (when the self-healing property of the tree code eventually enables him to decode this message correctly), the other party still needs to be informed of this previous error in decoding. Sending the information about which Pauli operator was used to do the teleportation decoding provides that information, and even enables the other party to correct this wrong teleportation decoding by himself if need be. It is indeed a property that we use in an essential way in the simulation since, when there is a corruption detected as an erasure, the teleportation decoding operation applied is the trivial one, which is the wrong one three quarter of the time on average. Note that another approach that would also work would be to let the other party know what information was received, and then let each party correct for their own previous decoding error. The problem with this is that the tolerable error rate would have to be much lower than $\frac{1}{2} - \varepsilon$: in the terms used in the analysis, we would need a good round to recover from an erasure round, which is undesirable.

Now, back to our simulation protocol. Since the parties have access to shared entanglement, they do not need to distribute it at the beginning of the protocol, and they can also use it to generate a secret key unknown to the adversary Eve. The secret key is used to generate a blueberry code with erasure parameter $\beta = 1 - (|\Sigma| - 1)/(|\Gamma| - 1)$, where Σ is the tree code alphabet and Γ is the blueberry code alphabet. Each of the tree code transmission alphabet symbols is then reencoded with the blueberry code before transmission over the noisy channel. A corruption caused by the adversary is then detected as an erasure with probability β.

The choice of tree code parameter α and the blueberry code parameter β depends on the parameter ε of the tolerable error rate $1/2 - \varepsilon$. For concreteness, we fix them as follows: $\varepsilon_\alpha = 1 - \alpha \leq \varepsilon/20$ and $\varepsilon_\beta = 1 - \beta \leq \varepsilon/40$. We take arity $d = 48$ for the tree code, since the message set consists of $\{0,1\}^2 \times \{-1,0,+1\} \times \{0,1\}^2 \cong [4] \times [3] \times [4] \cong [48]$. The length $N' = \ell N$ of the simulation protocol depends on ε; taking $\ell \geq \frac{2}{\varepsilon}(1 + \frac{1}{N})$ is sufficient. From Schulman [31], we

know that there exists a $q \in \mathbb{N}$ independent of N' such that an alphabet Σ of size q suffices to label the arcs of a distance α, d-ary tree code of any depth $N' \in \mathbb{N}$. Both parties agree before the protocol begins on such a tree code of depth N' (each party uses a separate instance of the same tree code to transmit her/his messages to the other party).

The convention we use for the variables describing the protocol is the following. On Alice's side, in round i, $x_i^{\mathsf{AD}} z_i^{\mathsf{AD}} \in \{0,1\}^2$ correspond to the bits she uses for the teleportation decoding on the X and Z Pauli operators, respectively, $x_i^{\mathsf{AM}} z_i^{\mathsf{AM}} \in \{0,1\}^2$ correspond to the bits of the teleportation measurement on the corresponding Pauli operators, $j_i^{\mathsf{A}} \in \mathbb{Z}$ and $M_i^{\mathsf{A}} \in \{-1, 0, +1\}$ correspond respectively to the index of the unitary she uses in round i, and to whether she applies $U_{j_i^{\mathsf{A}}}^{+1} = U_{j_i^{\mathsf{A}}}$, its inverse $U_{j_i^{\mathsf{A}}}^{-1} = U_{j_i^{\mathsf{A}}}^{\dagger}$, or simply the identity channel $U_{j_i^{\mathsf{A}}}^{0} = I$, on the AC quantum registers. On Bob's side, we use a similar set of variables, with superscripts B instead of A. All Pauli operators are acting on the C register. When discussing variables obtained from decoding in round i, a superscript i is added to account for the fact that this decoding might be wrong and could be corrected in later rounds. Similarly, the superscript i is used when discussing other variables that are round-dependent.

When an erasure is detected by either party in a round, that party does not try to evolve the protocol in that particular round, so the corresponding trit sent is 0, and the teleportation decoding bits are 00. Otherwise, the actions Alice and Bob take in round i are based on the following two representations for the form of the state $|\psi_i\rangle$ of the joint register at the beginning of round i (with $|\psi_1\rangle = |\psi_{\text{init}}\rangle$) that can be classically computed from the information in their two histories. The first one can be directly computed from the information in Alice's and Bob's histories, up to irrelevant operations of Eve on the E register, as

$$|\psi_i\rangle^{ABCE} = \prod_{\ell=1}^{i-1} (X^{x_\ell^{\mathsf{BM}}} Z^{z_\ell^{\mathsf{BM}}} U_{j_\ell^{\mathsf{B}}}^{M_\ell^{\mathsf{B}}} Z^{z_\ell^{\mathsf{BD}}} X^{x_\ell^{\mathsf{BD}}} \times X^{x_\ell^{\mathsf{AM}}} Z^{z_\ell^{\mathsf{AM}}} U_{j_\ell^{\mathsf{A}}}^{M_\ell^{\mathsf{A}}} Z^{z_\ell^{\mathsf{AD}}} X^{x_\ell^{\mathsf{AD}}}) |\psi_{\text{init}}\rangle^{ABCE}. \tag{1}$$

This first representation of the form of the state $|\psi_i\rangle$ is not too informative in itself, but from it we can classically compute a second one by recursively cleaning it up. The cleanup is performed by collapsing together as many of the operators as possible (Pauli operators together, U_ℓ's with U_ℓ^{-1}'s) to obtain something in the form:

$$|\psi_i\rangle^{ABCE} = \hat{\sigma}^i \, \tilde{U}_{t_i}^i \, \tilde{\sigma}_{t_i}^i \, \tilde{U}_{t_{i-1}}^i \, \tilde{\sigma}_{t_{i-1}}^i \cdots \tilde{U}_2^i \, \tilde{\sigma}_2^i \times \tilde{U}_1^i \, \tilde{\sigma}_1^i \, U_{r_i} \, U_{r_i-1} \cdots U_2 \, U_1 \, |\psi_{\text{init}}\rangle^{ABCE} \tag{2}$$

with $\hat{\sigma}^i = \pm X^{\hat{x}^i} Z^{\hat{z}^i}, \tilde{\sigma}_\ell^i = X^{x_\ell^i} Z^{z_\ell^i}$ for $\hat{x}^i \hat{z}^i, x_\ell^i z_\ell^i \in \{0,1\}^2$, and $\tilde{U}_\ell^i = U_{\ell'}^{\pm 1}$ for some $r_i - 2t_i \leq \ell' \leq r_i + 2t_i$. The rules to be used recursively to perform the cleanup are the following: in the case that $\tilde{\sigma}_\ell^i = I$, we require, if $\ell > 1$, that $\tilde{U}_\ell^i \neq (\tilde{U}_{\ell-1}^i)^{-1}$, and if $\ell = 1$, that $\tilde{U}_1^i \neq U_{r_i+1}$. This last rule is what determines the cut between U_{r_i} and the first error $\tilde{U}_1^i \tilde{\sigma}_1^i$. The parameter r_i determines the number of noiseless protocol unitaries the parties have been able to successfully apply on the joint register before errors start to arise on it, and the parameter t_i determines the number of errors the parties have to correct before being able to evolve the state as in the noiseless protocol. This second representation is then a powerful one, being the analogue in our setting of the protocol tree representation of classical protocols, enabling to exactly keep track of the evolution of the noiseless protocol simulation. This is the reason why Alice and Bob will always base their actions upon their best estimate of this representation.

To decide which action to take in round i, Alice starts by decoding the tree code layer of the possibly corrupted messages $f_1', \cdots, f_{i-1}' \in \Sigma \cup \{\perp\}$ received from Bob ($\perp$ is a special erasure symbol) up to this point to obtain her best guess s_B^i for his history s_B. Along with her history s_A, she uses it to compute her best guess of the form (2) of the joint state. If her decoding of Bob's history is *good* (error-free), then she has all the information she needs to compute the correct form of the joint state $|\psi_i\rangle$. She can then choose the right actions to take to evolve the simulation. She takes the following actions based on the assumption that her decoding is good. If it is not, errors might accumulate on the joint register ABC, which she will later have to correct. Alice's next move, after decoding $\hat{\sigma}_i$, depends on whether (she thinks) $t_i = 0$ or not: if it is the case, she applies U_{r_i+1} if she is the one to apply it, else she corrects $\tilde{U}_{t_i}^i$ if she is the one who applied it. Bob takes similar actions, considering the state

$$(X^{x_i^{\mathsf{AM}}} Z^{z_i^{\mathsf{AM}}} U_{j_i^{\mathsf{A}}}^{M_i^{\mathsf{A}}} Z^{z_i^{\mathsf{AD}}} X^{x_i^{\mathsf{AD}}}) |\psi_i\rangle \tag{3}$$

after Alice's communication. After these $N'/2$ rounds, Alice and Bob take the particular registers $\tilde{A}, \tilde{B}$ and $\tilde{C}$ specified by the noiseless protocol embedding (see section III-B), and use them as their respective outcomes for the protocol. If the simulation is successful, the output quantum state corresponds to the ABC subsystem of $|\psi_{\text{final}}\rangle^{ABCE}$ specified by the original noiseless protocol.

2) Analysis: The analysis is carried conditionally on some respective views of Alice and Bob of the transcript at each round, averaging over the shared secret key used for the blueberry code, and also conditionally on some classical state z of the Z register of Eve. In particular, if the adversary has an adaptive and probabilistic strategy, we condition on some strategy consistent with the transcript already conditioned on. The conclusion we seek holds for all such strategies and transcripts.

The total number of rounds is $\frac{N'}{2}$, with two transmissions per rounds, for a total of N' transmissions. To analyse this protocol, we define a function $P(i)$ such that we know the protocol succeeds whenever $P(\frac{N'}{2}+1) \geq N+1$ at the end of the simulation. We refer to the form of the state $|\psi_i\rangle$ on the joint register $ABCE$ at the beginning of round i rewritten as in (2), and define $P(i) = r_i - 2t_i$. The factor of 2 in front of t_i is due to the fact that, in the worst case, all remaining $\tilde{U}_\ell^i$'s are applied by the same party who applied U_{r_i-1}, and $\tilde{U}_{t_i}^i = U_{r_i-1-2(t_i-1)}^{-1}$. Then, if $P(\frac{N'}{2}+1) \geq N+1$, any remaining $\tilde{U}$ at the end of the simulation will be an identity operator as defined by the noiseless protocol embedding, and the output is correct.

We have three kinds of rounds: *good* rounds in which both parties can decode correctly the other party's history, *bad* rounds in which at least one party makes a decoding

error, and *erasure* rounds, in which no party makes a decoding error, but at least one of them decodes an erasure from the blueberry code. (In an erasure round, the party detecting an erasure applies the identity operator on the quantum register before teleporting it back.) If we define, at the end of round i, $N_g^i = |\{j : j \leq i, \text{round } j \text{ was good}\}|$, and similarly N_b^i and N_e^i for bad and erasure rounds, respectively, then we get the following technical lemma and corollary.

Lemma 1: With the above definitions,

$$P(i+1) \geq N_g^i - 4N_b^i.$$

Corollary 1: If $P(\frac{N'}{2}+1) \geq N+1$, then the simulation succeeds.

Note that it is important, in order to be able to tolerate error rate $\frac{1}{2}-\varepsilon$, that N_e^i does not appear in the lower bound for $P(i+1)$. Then, to bound the fraction of bad rounds as a function of the corruption rate, we need the corollary of the following technical lemma, which derives a new bound on tree codes with an erasure symbol. This result only talks about the structure of such codes independently of our application, and hence might have applications in a classical interactive coding setting as well. In particular, it is part of the toolkit used to prove the existence of a computationally efficient classical simulation protocol tolerating maximum error of $\frac{1}{2}-\varepsilon$ [37] in the shared secret key model. We consider a tree code of distance parameter $\alpha = 1-\varepsilon_\alpha$ and a blueberry code of erasure parameter $\beta = 1-\varepsilon_\beta$.

Lemma 2: If there is a bound δ on the fraction of the total number of transmissions N' that are corrupted and not detected as erasures by the blueberry code, then the number N_b of bad rounds in the whole simulation is bounded by $N_b \leq (2\delta+\varepsilon_\alpha)N'$.

Corollary 2: If the corruption rate c satisfies $0 \leq c < \frac{1}{2}$, then except with probability smaller than $2^{-\Omega(N')}$ for N' the length of the simulation protocol, the total number of bad rounds in the simulation is bounded by $N_b \leq (2\varepsilon_\beta+\varepsilon_\alpha)N'$.

With the above results in hand, we show that if the corruption rate is below $\frac{1}{2}-\varepsilon$ and we take $\varepsilon_\alpha, \varepsilon_\beta, \ell$ as stated in the description of the protocol, then except with negligible probability, the simulation succeeds:

$$\begin{aligned} P(\frac{N'}{2}+1) &\geq N_g - 4N_b \\ &= \frac{N'}{2} - N_e - 5N_b \\ &\geq \varepsilon N' - 5N_b \\ &\geq \varepsilon N' - 5(2\varepsilon_\beta+\varepsilon_\alpha)N' \\ &\geq N+1. \end{aligned}$$

The first inequality is from Lemma 1, the equality is by definition of N_g, N_b, N_e, i.e. $\frac{N'}{2} = N_g + N_b + N_e$, the second inequality is from the fact that the number of erasure rounds is bounded by the number of corruptions, i.e. $N_e \leq (\frac{1}{2}-\varepsilon)N'$, the third inequality is from our bound on N_b due to Corollary 2, which holds except with negligible probability, and the last inequality is from our choice of parameters.

V. Results in Other Models

By adapting the results we have obtained in the shared entanglement model for an adversarial error setting, we can obtain several other interesting results. We first complete our study of the shared entanglement model with results in a random error setting. We show that in the regime where we use binary symmetric channels of classical capacity close to 0, it is not possible to do much better than what we achieve, up to a multiplicative constant on top of the $\frac{1}{C}$ dilation factor. We then consider the quantum model and obtain results for both adversarial and random error settings. We also prove that the standard forward quantum capacity of the quantum channels used does not characterize their communication capacity in the interactive communication scenario. We consider a variation on the shared entanglement model in which, along with the noisy classical communication, the shared entanglement is also noisy. Formal statements, discussions about optimality and proof ideas appear in Ref. [3].

Theorem 3: Given a two-party quantum protocol of length N in the noiseless model and any $C > 0$, there exists a simulation protocol in the shared entanglement model that is of length $O(\frac{1}{C}N)$ and succeeds in simulating the original protocol with negligible error over classical binary symmetric channels of capacity C.

Theorem 4: There exists a sequence of two-party quantum protocols of increasing length N in the noiseless model such that for $C > 0$, any corresponding sequence of simulation protocols of length $o(\frac{1}{C}N)$ in the shared entanglement model with classical binary symmetric channels of capacity C fails at outputting the final state with low error on some input. Moreover, the family of quantum protocols can be chosen to be one computing a distributed binary function.

Theorem 5: Given an adversarial channel in the quantum model with error rate strictly smaller than $\frac{1}{6}$, we can simulate with arbitrary small error any noiseless protocol of length N over this channel using a linear number of constant-size transmissions.

Theorem 6: Given a two-party quantum protocol of length N in the noiseless model and any $Q > 0$, there exists a simulation protocol in the quantum model that is of length $O(\frac{1}{Q}N)$ and succeeds in simulating the original protocol with arbitrarily small error over quantum depolarizing channels of quantum capacity Q.

Theorem 7: There exists a sequence of two-party quantum protocols of increasing length N in the noiseless model such that for $Q_B > 0$, any corresponding sequence of simulation protocols of length $o(\frac{1}{Q_B}N)$ in the quantum model with quantum depolarizing channels of quantum capacity Q_B with classical feedback fails at outputting the final state with low error on some input. Moreover, the family of quantum protocols can be chosen to be one computing a distributed binary function.

Theorem 8: Given a two-party quantum protocol of length N in the noiseless model, there exists a quantum depolarizing channel of unassisted forward quantum capacity $Q = 0$ and a simulation protocol in the quantum model with asymptotically positive rate of communication that succeeds in simulating the

original protocol with arbitrarily small error over that quantum channel.

Theorem 9: Given noisy EPR pairs in a Werner state [38] of fidelity $F > \frac{1}{2}$, there is a constant error rate $\delta_F > 0$ such that for any adversarial classical channel with error rate δ_F, we can simulate any noiseless protocol of length N with negligible error over this channel using a number of transmissions linear in N, and consuming a linear number of noisy EPR pairs. Note that Werner states of fidelity $\frac{1}{2}$ are separable.

VI. Conclusion: Discussion and Open Questions

In this work, we proposed a simulation of interactive quantum protocols intended for noiseless communication over noisy channels. Our approach is to replace irreversible measurements by reversible pseudo-measurements in the Cleve-Buhrman model (with shared entanglement and classical communication). Then, in the noisy version of the model, we teleport back and forth the corresponding quantum communication register to avoid losing quantum information. We develop a representation for such noisy quantum protocols that gives an analogue of Schulman's protocol tree representation for classical protocols. We prove that with this approach, it is possible to simulate the evolution of quantum protocols designed for noiseless quantum channels over noisy channels with only a linear dilation factor.

In the case of adversarial channel errors in which the parties are allowed to pre-share a linear amount of entanglement, we prove that the error rate of $\frac{1}{2} - \varepsilon$ that our simulation tolerates is optimal for oblivious protocols. To get the tolerable error rate as high as $\frac{1}{2} - \varepsilon$, we develop new techniques along with a new bound on tree codes with an erasure symbol, Lemma 2. We will show in upcoming work that these new techniques are powerful enough to improve on known classical results, and in particular to develop a computationally efficient protocol tolerating the maximum error rate possible in the shared secret key model. To simplify the exposition, we chose not to optimize different parameters, such as communication and entanglement consumption rates and communication register size.

We adapt our findings to a random error model in which parties are allowed to share entanglement but communicate over binary symmetric channels of capacity $C > 0$. We obtain communication rates proportional to C. We show that, up to a hidden constant, this is optimal for some family of distributed binary functions, for example the inner product functions $IP_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, defined as $IP_n(x,y) = \oplus_{i=1}^n x_i \cdot y_i$. Our findings can also be adapted to obtain similar (though not optimal) results for the quantum model (the noisy version of Yao's model). Here, the simulation protocols run in two phases. In the first, a preprocessing phase, a linear amount of entanglement is distributed with standard techniques from quantum Shannon theory for random noise and from quantum coding theory for adversarial noise. This is followed by a simulation phase in which the actions of the parties parallel those in the shared entanglement model. In the case of adversarial noise, we show that we can tolerate an error rate of $\frac{1}{6} - \varepsilon$ in the quantum model. In the case of random noise in which the parties communicate over depolarizing channels of capacity $Q > 0$, we obtain rates proportional to Q. Perhaps surprisingly, we show that the use of depolarizing channels in both directions enables the simulation to succeed even for some quantum channels of unassisted forward quantum capacity $Q = 0$. This proves that Q does not characterize a quantum channel's capacity for interactive quantum communication. We extend our ideas to perform simulation in an extension of the shared entanglement model in which not only is the classical communication noisy, but also the entanglement is noisy.

A direction of research that immediately falls out of this work is characterizing the communication rates in all of the models discussed. In particular, the precise interactive capacity of the depolarizing channel with a specified noise parameter remains open. The question of interactive capacity for the binary symmetric channel was raised in the classical context by Schulman [31] and brought back to attention recently by Braverman in a survey article on the topic of interactive coding [8]. Recent developments provide tight lower and upper bounds for this quantity [24]. In the classical setting, a particular problem with worst case interaction of one bit transmissions to which all classical interactive protocols can be mapped was proposed for the study of such a quantity. Since every interactive quantum protocol can be mapped onto our general problem, it would be natural to study such a quantity in the quantum domain. Would the interactive capacity of the binary symmetric channel (with entanglement assistance) for quantum protocols be the same as that for classical protocols [24], up to a factor of two for teleportation? We show in upcoming articles that for small bit flip probability ε, the lower bound of $\frac{1}{2} - O(\sqrt{H(\varepsilon)})$ holds, and even extends to a lower bound of $1 - O(\sqrt{H(\varepsilon)})$ for depolarizing channels. Do the techniques developed in Ref. [24] adapt to the quantum setting to obtain matching upper bounds of $\frac{1}{2} - \Omega(\sqrt{H(\varepsilon)})$ and $1 - \Omega(\sqrt{H(\varepsilon)})$, respectively? What about other channels?

Another question that remains open is that of the highest tolerable adversarial error rate that can be withstood in the quantum model. To study this question, it is likely that a fully quantum approach with new kinds of quantum codes needs to be developed. In particular, ideas from fault-tolerant quantum computation might be necessary. Furthermore, the important question of integrating our results into a larger fault-tolerant framework, in which the local operations are also noisy, remains open. Yet another important question for interactive quantum coding is what would happen in a shared entanglement setting if along with the noisy classical communication, the entanglement provided were also noisy; we investigated this question for a depolarizing noise model for the entanglement, but other models would also be interesting to study. In particular, what about adversarial noise on the shared EPR pairs above the unidirectional binary error rate limit? Note that below that bound, we can adapt the techniques we use here for distillation. Finally, the question of computationally efficient simulation also remains open, and we will show in upcoming works how to merge the techniques developed here with those of Brakerski and Kalai [6] to efficiently process the classical communication in our simulation protocols.

Acknowledgements

The authors are grateful to Louis Salvail, Benno Salwey and Mark M. Wilde for useful discussions. G.B. is supported in part by the Natural Sciences and Engineering Research Council

of Canada (NSERC), the Canada Research Chair program, the Canadian Institute for Advanced Research (CIFAR) and the Institute for Theoretical Studies of ETH Zurich. A.N.'s research was conducted in part at Perimeter Institute and supported in part by NSERC Canada, CIFAR, an ERA (Ontario), QuantumWorks, MITACS, and ARO (USA). Research at Perimeter Institute for Theoretical Physics is supported in part by the Government of Canada through Industry Canada and by the Province of Ontario through MRI. A.T. was supported by NSERC and CIFAR. D.T. is supported by a Fonds de Recherche Québec – Nature et Technologies B2 Doctoral research scholarship. F.U.'s research was conducted in part at UC Berkeley.

REFERENCES

[1] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. *Quantum Circuits with Mixed States.* Proceedings of the 30th Annual ACM Symposium on Theory of Computing (1997): 20-30.

[2] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wooters. *Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels.* Physical Review Letters 70.13 (1993): 1895-1899.

[3] Gilles Brassard, Ashwin Nayak, Alain Tapp, Dave Touchette, Falk Unger. *Noisy Interactive Quantum Communication.* arXiv e-print quant-ph/1309.2643v2.

[4] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. *Entanglement-assisted classical capacity of noisy quantum channels.* Physical Review Letters 83.15 (1999): 3081-3084.

[5] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. *Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem.* IEEE Transactions on Information Theory 48.10 (2002): 2637-2655.

[6] Zvika Brakerski, and Yael Tauman Kalai. *Efficient Interactive Coding Against Adversarial Noise.* Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (2012): 160-166.

[7] Zvika Brakerski, and Moni Naor. *Fast Algorithms for Interactive Coding.* Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms (2013): 443-456.

[8] Mark Braverman. *Coding for Interactive Computation: Progress and Challenges.* Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing (2012): 1914:1921.

[9] Mark Braverman, and Anup Rao. *Towards Coding for Maximum Errors in Interactive Communication.* Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (2011): 159-166.

[10] Harry Buhrman, Richard Cleve, and Avi Wigderson. *Quantum vs. classical communication and computation.* Proceedings of the 30th Annual ACM Symposium on Theory of Computing (1998): 63-68.

[11] A. Robert Calderbank, Eric M. Rains, Peter W. Shor, and Neil. J. A. Sloane. *Quantum error correction via codes over GF(4).* IEEE Transactions on Information Theory 44.4 (1998): 1369-1387.

[12] A. Robert Calderbank, and Peter W. Shor. *Good Quantum Error-Correcting Codes Exist.* Physical Review A 54.2 (1996): 1098-1105.

[13] Richard Cleve, and Harry Buhrman. *Substituting quantum entanglement for communication.* Physical Review A 56.2 (1997): 1201-1204.

[14] Igor Devetak. *The Private Classical Capacity and Quantum Capacity of a Quantum Channel.* IEEE Transactions on Information Theory 51.1 (2005): 44-55.

[15] Dennis Dieks. *Communication by EPR devices.* Physics Letters A 92.6 (1982):271-272.

[16] Keqin Feng, and Zhi Ma. *A finite Gilbert-Varshamov bound for pure stabilizer quantum codes.* IEEE Transactions on Information Theory 50.12 (2004): 3323-3325.

[17] Matthew Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard Schulman. *Optimal Coding for Streaming Authentication and Interactive Communication.* Advances in Cryptology-CRYPTO 2013. Springer Berlin Heidelberg (2013): 1-20.

[18] Ran Gelles, Ankur Moitra, and Amit Sahai. *Efficient and Explicit Coding for Interactive Communication.* Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (2011): 768-777.

[19] Daniel Gottesman. *A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound.* Physical Review A 54.3 (1996): 1862-1868.

[20] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman. *Interaction in quantum communication.* IEEE Transactions on Information Theory 53.6 (2007): 1970-1982.

[21] Alexander. S. Holevo. *Towards the mathematical theory of quantum communication channels.* Probl. Peredachi Inform. 8 (1972): 63-71 (in Russian).

[22] Alexander S. Holevo. *Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel.* Probl. Peredachi Inform. 9 (1973): 177-183 (in Russian).

[23] Alexander S. Holevo. *The Capacity of the Quantum Channel with General Signal States.* IEEE Transactions on Information Theory 44.1 (1998): 269-273.

[24] Gillat Kol, and Ran Raz. *Interactive Channel Capacity.* Proceedings of the 45th Annual ACM Symposium on Theory of Computing (2013): 715-724.

[25] Seth Lloyd. *Capacity of the Noisy Quantum Channel.* Physical Review A 55.3 (1997): 1613-1622.

[26] Michael A. Nielsen, and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press (2000).

[27] Noam Nisan, and Avi Widgerson. *Rounds in communication complexity revisited.* Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (1991): 419-429.

[28] Eric M. Rains. *Nonbinary quantum codes.* IEEE Transactions on Information Theory 45.6 (1999): 1827-1832.

[29] Leonard J. Schulman. *Communication on Noisy Channels: A Coding Theorem for Computation.* Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science (1992): 724-733.

[30] Leonard J. Schulman. *Deterministic Coding for Interactive Communication.* Proceedings of the 25th Annual ACM Symposium on Theory of Computing (1993): 747-756.

[31] Leonard J. Schulman. *Coding for Interactive Communication.* IEEE Transactions on Information Theory 42.6 (1996): 1745-1756.

[32] Benjamin Schumacher, and Michael D. Westmoreland. *Sending Classical Information via Noisy Quantum Channels.* Physical Review A 56 (1997): 131-138.

[33] Peter W. Shor. *Scheme for reducing decoherence in quantum computer memory.* Physical Review A 52.4 (1995): 2493-2496.

[34] Peter W. Shor. *The Quantum Channel Capacity and Coherent Information.* Lecture Notes, MSRI Workshop on Quantum Computation (2002).

[35] Andrew Steane. *Multiple Particle Interference and Quantum Error Correction.* Proceedings of the Royal Society of London. Series A (1996): 2551-2577.

[36] Ran Raz. *Exponential Separation of Quantum and Classical Communication Complexity.* Proceedings of the 31st Annual ACM Symposium on Theory of Computing (1999): 358-367.

[37] Dave Touchette. *Authenticated Interactive Coding.* In preparation.

[38] Reinhard F. Werner. *Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model.* Physical Review A 40.8 (1989): 4277-4281.

[39] Mark M. Wilde. *Quantum Information Theory.* Cambridge University Press (2013), Preliminary version available as: arXiv e-print quant-ph/1106.1445.

[40] William K. Wootters, and Wojciech H. Zurek. *A single quantum cannot be cloned.* Nature 299.5886 (1982): 802-803.

[41] Andrew C.-C. Yao. *Quantum circuit complexity.* Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science (1993): 352-361.