Electronic Colloquium on Computational Complexity, Report No. 335 (2026)

Two-Way Quantum Codes with Optimal Erasure Resilience

Klim Efremenko* Ben-Gurion University

Gillat Kol† Princeton University

Sergey Komech‡ Ben-Gurion University

Raghuvansh R. Saxena§ Tata Institute of Fundamental Research

Zhijun Zhang¶ INSAIT, Sofia University "St. Kliment Ohridski"

Abstract

The *no-cloning theorem* imposes a fundamental limit on quantum error correction. It implies that no code is resilient to a half fraction of adversarial erasures: otherwise, we can clone by decoding from two disjoint halves of the encoding. This argument works because the encoding does not depend on the receiver, allowing the two halves to be decoded by different decoders.

We initiate the study of *two-way quantum codes*, codes in which the receiver participates in the now-interactive encoding process, and show that interaction substantially improves resilience. Our main result shows that this improvement is achievable even when the receiver's return channel is purely classical and controlled by the same adversary as the sender's quantum channel. For this *quantum–classical channel*, we prove a sharp $3/5$ resilience threshold: we design an efficient, constant-rate code over a constant-size alphabet achieving this resilience, and prove that higher resilience is impossible.

We then ask how much more can be gained when the receiver's return channel is quantum rather than classical. We show that in the *quantum–quantum channel*, the maximum resilience increases to $2/3$. For the more general task of *interactive coding*, we prove that the optimal erasure resilience is $1/2$.

*klimefrem@gmail.com. Supported by the European Research Council Grant number: 949707.

†gillat.kol@gmail.com.

‡sergey.komech@gmail.com. Supported by European Research Council Grant number: 949707.

§raghuvansh.saxena@gmail.com. Supported by the Department of Atomic Energy, Government of India, under project no. RTI4014.

¶zhijun.zhang@insait.ai. This research was partially funded by the Ministry of Education and Science of Bulgaria (support for INSAIT, part of the Bulgarian National Roadmap for Research Infrastructure).

ISSN 1433-8092

Contents

1 Introduction **1**
- 1.1 Our Results . . . 2
  - 1.1.1 The Erasure Resilience of the Quantum–Classical Channel . . . 2
  - 1.1.2 The Erasure Resilience of the Quantum–Quantum Channel . . . 3
- 1.2 Related Work . . . 4

2 Proof Sketch **5**
- 2.1 A Two-Way Code with Resilience $3/5$ . . . 5
- 2.2 The 3/5 Upper Bound . . . 7

3 Model and Preliminaries **9**
- 3.1 The Quantum Communication Model with Erasures . . . 9
  - 3.1.1 Pseudo-Measurements . . . 11
- 3.2 Error-Correcting Codes . . . 11

4 Impossibility Results for Two-Way Codes **12**
- 4.1 The case $f_{\mathsf{A},\mathsf{p}} \leq f_{\mathsf{A},\mathsf{s}}$ . . . 13
- 4.2 The case $f_{\mathsf{A},\mathsf{p}} > f_{\mathsf{A},\mathsf{s}}$ . . . 14

5 Two-Way Code for the Quantum-Classical Channel **17**
- 5.1 Analysis . . . 18

6 Two-Way Code for the Quantum-Quantum Channel **24**
- 6.1 Analysis . . . 26

7 Optimally Resilient Quantum Interactive Coding **26**
- 7.1 Analysis . . . 27
- 7.2 The Structure of Algorithms 5 and 6 . . . 27
- 7.3 Finishing the Proof . . . 34

A Proof of Theorem 3.1 **39**

B Two-Way Code with Free Noiseless Classical Feedback **43**
- B.1 Analysis . . . 43

1 Introduction

The no-cloning barrier. In the traditional quantum error-correction setting, Alice holds an unknown quantum state that she wishes to transmit to Bob. The *no-cloning theorem* rules out a code that would allow Bob to reconstruct Alice's state from any half of the communication, as otherwise Alice's unknown state can be cloned by decoding from two disjoint halves of the encoding. This implies that no quantum erasure code can be resilient to a half fraction of adversarial erasures.[1]

Interaction as an antidote. Observe that the above argument relies crucially on the fact that a traditional code produces a single fixed encoding of the input state that can be split between two receivers. Thus, to go beyond the usual $1/2$ no-cloning limit, the encoding cannot simply be a fixed function of Alice's input.

A natural way to move beyond static encoding is to let Alice's later transmissions also depend on information Bob obtains during the execution, such as which of Alice's previous messages were erased. This requires the parties to interact over a bidirectional communication channel. Such channels are already built into many communication systems: receivers often send acknowledgments, synchronization information, or other control messages back to the sender, sometimes through a channel that is itself noisy.

Once Bob can communicate back to Alice, the simple splitting argument no longer applies. To see this concretely, imagine running an interactive encoding protocol between Alice and Bob_1, and giving all Alice-to-Bob messages erased for Bob_1 to a second receiver, Bob_2. The messages seen by Bob_2 may not form a transcript that could arise from any valid execution between Alice and Bob_2. The reason is that Alice's later transmissions may depend on the feedback she received from Bob_1, while Bob_1's feedback depends on which earlier transmissions he received. Those differ from the earlier transmissions received by Bob_2.[2] Therefore, the correctness guarantee of the code does not imply that Bob_2 can decode, and the no-cloning argument no longer applies directly.

Two-way quantum codes. The discussion above motivates the question of *how much erasure resilience can be gained from interaction*. We initiate the study of the resilience of *two-way quantum codes*, which are interactive protocols over noisy communication channels in which Alice and Bob may send messages back and forth, while the goal remains the same as in traditional quantum error correction—the reliable transmission of an unknown quantum state from Alice to Bob. Prior work on two-way codes has only considered the classical communication setting [GKZ22, EKSZ22, GZ22, GZ23].

[1] In this channel, an adversary replaces some of the communicated qudits by a special symbol $|\perp\rangle$.

[2] For example, suppose Alice's first message reaches Bob_1 and is therefore not given to Bob_2. Bob_1's feedback may acknowledge receipt, while Bob_2's feedback would have reported a failed reception. Alice's later messages in the actual execution are generated according to Bob_1's acknowledgment, not according to the failure report that Bob_2 would have sent. Thus, Bob_2 receives a transcript that is inconsistent with his own view.

1.1 Our Results

1.1.1 The Erasure Resilience of the Quantum–Classical Channel

To demonstrate the power of interaction, we first consider quantum codes with a very limited form of return communication: Bob's return channel is *classical* and, like Alice's quantum channel, is subject to *adversarial erasures* under the same global budget. Our main result, stated informally in Theorem 1.1 (see Theorems 4.1 and 5.1 for formal statements), shows that even this weak form of feedback already suffices to substantially improve quantum erasure resilience.

Classical return channels are well studied in the quantum-information literature, *e.g.*, [Bow04, Bow05, BN05, Ske04, Leu08, LLS09, DQSW19]; see also the discussion in Section 1.2. They are also natural from a practical perspective, as many quantum communication tasks already include classical acknowledgments, synchronization, or post-processing messages.[3]

One of the main motivations for studying erasure resilience with a classical return channel is that this model is the most direct quantum analogue of the classical feedback channel, where after each transmission Alice learns the symbol received by Bob. Such feedback gives Alice complete information about the noise pattern and allows her future transmissions to adapt to what Bob actually received. Feedback for quantum channels is more subtle as Bob cannot give Alice complete information about the received quantum systems by simply sending back a copy of a received quantum state due to the no-cloning theorem.

However, for quantum erasure channels, the noise pattern observed by Bob is classical: for each transmission, Bob knows whether he received a quantum message or an erasure flag. A classical return channel is therefore expressive enough to carry the full erasure-pattern information to Alice. At the same time, restricting the return channel to be classical prevents Bob from sending Alice quantum states unrelated to the witnessed noise pattern, such as EPR halves or quantum states that Alice previously sent him. Thus, for quantum erasure channels, a classical return channel is especially well motivated: it allows Bob to communicate the complete noise information, as in the classical feedback setting, while still ruling out additional quantum resources.

Theorem 1.1 (Main theorem, formal version in Theorems 4.1 and 5.1)**.** *The maximum erasure resilience of two-way codes over the quantum–classical channel is* $3/5$*. Moreover, this resilience is achieved by a computationally efficient, constant-rate code over a constant sized alphabet.*

We mention that our protocol has zero decoding error, and our impossibility result relies on the no-cloning theorem. Analogues of the no-cloning theorems are known for small constant error [HB97, KW99], and may be used to extend our impossibility result to rule out sufficiently small constant decoding error.

[3] For example, quantum key distribution uses a quantum channel to transmit quantum signals and a classical channel for post-processing, including basis sifting, error-correction verification, privacy amplification, and key verification.

The statement of Theorem 1.1 uses the simplest erasure budget: erasing one Alice-to-Bob quantum symbol and erasing one Bob-to-Alice classical symbol both cost the adversary one unit. Since the two directions carry different kinds of information, it is natural to ask whether classical and quantum erasures should instead be charged differently.[4] In Remarks 4.4 and 5.2 we show that the $3/5$ bound in Theorem 1.1 is robust under any fixed constant weighting of the two directions.

We give a detailed sketch of the proof of Theorem 1.1 in Section 2.

For completeness, we also study the erasure resilience of two-way codes where the (classical) messages from Bob are noiseless and do not count towards the communication budget. This model is well studied in the quantum information literature, see Section 1.2. For this model, Theorem B.1 shows that the erasure resilience is 1.

1.1.2 The Erasure Resilience of the Quantum–Quantum Channel

Two-way codes over the quantum–quantum channel. The proof of the impossibility result in Theorem 1.1 identifies the resource needed to go beyond $3/5$. It applies not only to classical feedback, but more generally to any return communication from Bob that does not create fresh quantum correlations with Alice.[5] Thus, any improvement beyond $3/5$ must use Bob's ability to create fresh entanglement with Alice.

Shared entanglement is useful because it can turn quantum transmission into classical communication: with shared EPR pairs, Alice can teleport her message and then protect the classical teleportation string using a classical erasure code with resilience approaching 1, even in the traditional setting were there is no feedback from Bob.

Interestingly, our proof shows that allowing Bob to generate EPR pairs and sharing its halves with Alice is strictly better that having Alice share EPR halves with Bob, as the latter is possible even over a quantum–classical channel. Intuitively, if Alice sends EPR halves to Bob, she must rely on Bob's noisy feedback to learn which halves were actually received; teleporting using an EPR pair whose other half is not held by Bob would simply lose the teleported state. By contrast, if Bob creates EPR pairs and sends halves to Alice, then every half Alice receives is automatically safe in this sense: Bob necessarily holds the other half. Hence Alice can use any of the halves she receives to teleport her message, and the indices of the pairs she uses can be included in the teleportation string.

Theorem 1.2 (Informal, formal version in Theorems 4.2 and 6.1)**.** *The maximum erasure resilience of two-way codes over the quantum–quantum channel is $2/3$. Moreover, this resilience is achieved by a computationally efficient, constant-rate code over a constant sized alphabet.*

[4] For example, in the presence of pre-shared entanglement, teleportation and superdense coding show that one d-dimensional quantum symbol is closely related to two classical symbols from an alphabet of size d.

[5] More concretely, the proof continues to hold provided that, before Bob has received any quantum information from Alice, his messages back to Alice are not entangled with his private state. In particular, allowing Bob to send quantum states only after he has received something from Alice does not overcome the $3/5$ barrier.

Interactive coding over the quantum–quantum channel. The field of *interactive coding*, pioneered by [Sch92, Sch93, Sch96], studies a more general task than two-way message transmission: rather than transmitting a single message, the goal is to robustly simulate an arbitrary noiseless protocol over a noisy channel. Quantum interactive coding was initiated by [BNT+19], who gave protocols for several quantum communication models. In particular, they obtained simulations over the quantum–quantum channel tolerating a $1/6$ fraction of adversarial corruptions with exponentially small error.

We design an interactive code over the quantum–quantum channel with optimal resilience approaching $1/2$ against adversarial erasures and zero decoding error. The proof of optimality is easy: one of the parties must speak for at most half the rounds, and the adversary can fail the protocol by erasing all messages sent by this party.

Theorem 1.3 (Informal, formal version in Theorem 7.1)**.** *The maximum erasure resilience of quantum interactive codes is $1/2$. Moreover, this resilience is achieved by a computationally efficient, constant-rate code over a constant sized alphabet (actually, 5).*

1.2 Related Work

Classical two-way codes. Two-way codes have recently been studied in the classical binary setting [GKZ22, EKSZ22, GZ22, GZ23]. Over the binary erasure channel, [GKZ22] constructed a two-way code with resilience $3/5$, improving on the optimal $1/2$ resilience of one-way erasure codes, and also proved a $2/3$ upper bound on the resilience of any such two-way code. Later, [GZ22] obtained a two-way erasure code that is constant-rate and computationally efficient, albeit with resilience $6/11$. For the binary corruption (bit-flip) channel, the maximum resilience of a one-way code is $1/4$ by the Plotkin bound. [EKSZ22] constructed a two-way code resilient to a $1/4 + 10^{-5}$ fraction of adversarial corruptions. An upper bound of $2/7$ on the resilience of any binary two-way corruption code was shown by [GKZ22] and later improved to $13/47$ by [GZ23].

Classical feedback channels. Shannon studied *feedback channels* [Sha56], where after each use of the channel Alice learns the symbol received by Bob, and showed that feedback does not increase the capacity of *stochastic* memoryless channels. For adversarial channels, however, feedback can strictly increase resilience. For the adversarial binary corruption channel with noiseless feedback, a code with optimal resilience of $1/3$ dates back to [Ber64, Zig76] (recall that the maximum resilience of this channel with no feedback is only $1/4$). More recent work has considered partial, highly constrained, or noisy feedback [HKV15, GGZ23, BEK+25, WQC17].

Conceptually, two-way codes can be viewed as codes with noisy feedback. Unlike in the noiseless-feedback setting, however, Bob's transmissions pass through the same adversarial channel as Alice's and count against the same global budget for the adversary. Moreover, Bob's messages may be arbitrary and need not simply repeat the last symbol he received.

Quantum channels with feedback. As discussed above, feedback is more subtle in the quantum setting, because the no-cloning theorem prevents the channel from simply giving Alice a copy of the state received by Bob. Accordingly, the quantum-information literature has developed several notions of "feedback," usually modeled as idealized noiseless return channels from Bob to Alice. These include noiseless quantum return channels, noiseless classical return channels, unrestricted two-way classical assistance, and more specialized notions such as passive and coherent feedback [Bow04, Bow05, BN05, Ske04, Win06, Leu08, LLS09, DSW16, DW18, DQSW19].

Most of this work studies stochastic memoryless channels and asks how such perfect feedback resources affect asymptotic communication rates. To the best of our knowledge, prior work on quantum coding with feedback does not address adversarial noisy channel coding. Since our model considers adversarial erasures on both the quantum channel and the return channel, it is a noisy-feedback version of quantum error correction rather than a capacity problem with ideal feedback assistance.

Quantum channels with classical feedback. Noiseless classical feedback for stochastic quantum channels has been studied as the closest quantum analogue of Shannon's feedback model, and several capacities have been considered in this setting. These include classical capacity, the rate at which classical messages can be transmitted over this channel with vanishing error [BN05, Ske04, DW18, DQSW19]; quantum capacity, the rate at which quantum information can be transmitted with vanishing error; and entanglement-generation capacity, the rate at which the parties can generate shared entanglement with fidelity tending to one [BDSS06, Leu08, LLS09]. Related work also studies zero-error communication, where messages must be transmitted with no probability of error, and identification, where the receiver is asked only whether the sent message equals a specified candidate message [Win06, DSW16].

2 Proof Sketch

In this section, we sketch the proof of Theorem 1.1, showing that $3/5$ is the sharp erasure-resilience threshold for two-way codes over the quantum–classical channel.

2.1 A Two-Way Code with Resilience $3/5$

We sketch the construction of our two-way code over the quantum–classical channel, achieving erasure resilience approaching $3/5$.

Let X be the unknown input state of length n that Alice wishes to communicate to Bob. The protocol has length $T = \Theta(n/\epsilon^2)$ and it proceeds in iterations that each have Alice speaking for $2L$ rounds, and then Bob speaking for L rounds, where $L = \Theta(n/\epsilon)$. In every iteration, Bob's feedback is an encoding of a Boolean vector indicating, for every Alice

transmission so far, whether Bob received it. This continues for the first $3T/5$ rounds; after that, only Alice speaks. Thus, in total, Alice speaks for $4T/5$ rounds and Bob speaks for $T/5$ rounds.

Since the adversary has fractional budget $3/5 - \epsilon$, it can erase all of Bob's communication and still have budget to erase almost half of Alice's communication. Erasing all communication from Bob puts Alice back in the traditional coding setting. Since the adversary can additionally erase almost half of Alice's transmissions, in the case where Alice never receives any transmission from Bob, her transmissions must constitute an encoding of X by some quantum code C^{Q} with nearly optimal erasure resilience $1/2$. Thus, without loss of generality, we can assume that Alice computes $W = \mathsf{C}^{\mathsf{Q}}(X)$ at the start of the protocol and, as long as she receives no transmission from Bob, her default behavior is to transmit the next symbol of W, together with additional items such as one half of a fresh EPR pair.

If, at some point, Alice does receive a transmission from Bob, she decodes Bob's message and considers two cases. The first case is when Bob's message indicates that he received at least n of Alice's messages. Then Alice and Bob share at least n EPR pairs. Alice uses these EPR pairs to teleport her message, and encodes the resulting classical teleportation string using a classical error-correcting code with erasure resilience approaching 1. Alice then spends the rest of her transmissions sending this encoding.

The interesting case is when Bob's message indicates that he received fewer than n of Alice's transmissions so far. In this case, the adversary may already have obtained some coordinates of W, and Alice must be careful not to give away half or more of the codeword. Otherwise, the information about X remaining with Alice, together with the information held by Bob, may no longer be enough to reconstruct X, and the state X would be lost. Note that the adversary can erase more than half of Alice's communication if it does not try to erase Bob's communication. Thus, at some point, Alice must stop sending coordinates of the current W in order not to lose the ability to recover X.

We first observe that, if Bob has received fewer than n of Alice's transmissions by the current iteration r, then the adversary has spent at least $2Lr - n \approx 2Lr$ erasures so far. These erasures occur within the first $r(2L + L) = 3Lr$ rounds, so roughly a $2/3 > 3/5$ fraction of the rounds so far have been erased. Therefore, after this iteration, we are left "playing the same message-transmission game" with a smaller fractional budget for the adversary. That is, Alice still needs to communicate X to Bob, but the adversary's remaining budget is noticeably less than a $3/5 - \epsilon$ fraction.

The remaining question is how Alice can *restart* a "clean" transmission game if the adversary already has part of W that Alice cannot retrieve. To this end, we observe that, as long as the adversary has less than half of the coordinates of W, it has no information about X in the relevant sense. The reason is that Alice still holds more than half of W, and therefore can decode it to recover X. When Alice restarts the protocol, her first step is to *re-encode* X and obtain a fresh codeword W.

The above decoding and re-encoding of X are possible only as long as Alice still holds more than half of the coordinates of W. We next argue that this will always be the case

whenever Alice restarts. If not, then Alice must have sent more than half of the coordinates of W without restarting. Thus, while sending this half, she did not receive useful feedback from Bob. Informally, this means that the adversary has spent many erasures blocking the communication that would have allowed Alice either to restart earlier or to switch to teleportation. Since Bob speaks half as often as Alice, and Alice speaks for a total of $4T/5$ rounds, by the time Alice sends half of her total transmissions, $2T/5 + T/5 = 3T/5$ rounds have passed. The adversary cannot erase all the relevant communication up to this point, since their budget is less than $3T/5$. Thus Alice never restarts after losing the ability to recover X from the unsent part of the current codeword.

2.2 The $3/5$ Upper Bound

We sketch why no two-way code over the quantum–classical channel can correct a $3/5$ fraction of adversarial erasures.

Fix a two-way code and suppose toward contradiction that the code corrects every erasure pattern of size at most $3T/5$. Let T be the total number of transmissions, let A be the number of Alice-to-Bob quantum transmissions, and let B be the number of Bob-to-Alice classical transmissions, so $A + B = T$.

We first note two simple constraints. We must have $A > 3T/5$, since otherwise the adversary can erase every Alice-to-Bob transmission, and Bob receives no information about Alice's input. We must also have $B + \frac{A}{2} > 3T/5$, or equivalently $A < 2(1 - 3/5)T = 4T/5$, as otherwise the adversary can erase all Bob-to-Alice feedback and also erase an arbitrary half of Alice's quantum transmissions. The protocol then reduces to a traditional quantum code that corrects arbitrary half erasures, which, as discussed in Section 1, is forbidden by no-cloning.

Now place a *cut* after the first $P = 3T/5$ transmissions. Let a be the number of Alice-to-Bob transmissions before the cut, and let b be the number of Bob-to-Alice transmissions before the cut, so $a + b = P$.

We consider two cases.

Case 1: $a < A/2$**.** Consider the adversary that erases all Alice-to-Bob transmissions before the cut, all Bob-to-Alice transmissions after the cut, and an arbitrary half of the Alice-to-Bob transmissions after the cut. The cost of this attack is at most $3T/5$,[6] so the attack is valid.

Since Alice's prefix transmissions are erased, Bob's local view up until the cut is independent of X. In particular, Bob's messages up until the cut are classical and independent of Alice's input. We may therefore think of these messages as creating an input-independent shared classical string (shared side information) between Alice and Bob that is available at the cut.

[6]The attack costs $a+(B-b)+\frac{A-a}{2}$. Using $b = P-a$, this equals $a+\big(B-(P-a)\big)+\frac{A-a}{2} = T-P-\frac{A}{2}+\frac{3a}{2}$. Since $a < \frac{A}{2}$, the cost is at most $T - P + \frac{A}{4}$. Using $A < \frac{4T}{5}$ and $P = \frac{3T}{5}$, this is at most $\frac{2T}{5} + \frac{T}{5} = \frac{3T}{5}$.

After the cut, Bob's feedback is erased, so the remaining communication relevant to transmitting X goes only from Alice to Bob. Conditioned on the classical shared string from the prefix, the suffix therefore becomes a traditional quantum code from Alice to Bob. Correctness of the original two-way code under the attack above would imply that this traditional code corrects arbitrary erasures of half of Alice's suffix transmissions. This contradicts the half-erasure/no-cloning barrier.

We note that this is the only place where we use that Bob's return channel is classical. If the return channel were quantum, Bob could have sent quantum states to Alice before the cut, for example halves of EPR pairs. Then the suffix would no longer be an (unassisted) traditional quantum code; it could be an entanglement-assisted code. The half-erasure/no-cloning barrier would no longer be the right obstruction in that setting.

We also note that the argument in this case continues to hold under a more general condition, where Bob is able to send quantum states. However, as discussed in Section 1, we require that before Bob has received any message from Alice, the states he sends back to Alice are not entangled with his private state. So, for instance, we are not allowing Bob to send halves of fresh EPR pairs before hearing from Alice.

Case 2: $a \geq A/2$**.** Consider two valid erasure patterns. In Pattern I, the adversary erases the entire prefix before the cut. This is a valid attack, as it costs $P = 3T/5$. Since no Alice-to-Bob prefix transmission reaches Bob, Bob's local state at the cut is independent of X. Therefore, by correctness, Alice must be able to recover X from her local state at the cut; otherwise X would be lost.

In Pattern II, the adversary erases all Bob-to-Alice transmissions before the cut and all Alice-to-Bob transmissions after the cut. The cost of this attack is at most $3T/5$,[7] so the attack is valid. Since after the cut all Alice-to-Bob transmissions are erased, but Bob can still recover X at the end of the protocol, Bob must be able to recover X from his local state at the cut.

The key step is to define a *hybrid* execution in which both the Alice-side and Bob-side recovery maps apply to the same cut state. Let H be the prefix execution in which the Alice-to-Bob transmissions before the cut are delivered to Bob, but all Bob-to-Alice transmissions before the cut are erased. Bob's view at the cut in H is the same as in Pattern II, since in both executions Bob receives Alice's prefix transmissions and Bob's own prefix transmissions to Alice are erased.

We also claim that Alice's view at the cut in H is the same as in Pattern I. Indeed, in Pattern I Alice's prefix transmissions are erased, while in H they are delivered to Bob. However, in both executions Alice sends the same messages and receives no feedback from Bob before the cut. Thus, from Alice's perspective, the only possible difference would have to come from Bob's reaction to receiving her messages. But Bob's prefix transmissions to Alice are erased in both executions, so Bob cannot signal this difference back to Alice. This can be viewed as a *no-signaling* statement: even though Bob can distinguish the two cases

[7] The attack costs $b + (A - a) = P - a + A - a = P + A - 2a \leq P \leq 3T/5$, where we used $a \geq A/2$.

and may perform different local operations, these local operations cannot change Alice's local state when no communication from Bob reaches her (see also Section 3.1.1).

Therefore, Alice's cut state in H is the same as in Pattern I, so the Alice-side recovery map from Pattern I also applies in H. Similarly, Bob's cut state in H is the same as in Pattern II, so the Bob-side recovery map from Pattern II also applies in H. Thus, in the same hybrid cut state, both Alice's system and Bob's system admit recovery maps for the same unknown input X. Applying these two recovery maps in parallel gives two recoveries of X, contradicting no-cloning. Hence Case 2 is impossible.

Since both cases lead to contradictions, the upper bound follows.

3 Model and Preliminaries

Notation. For $n \in \mathbb{N}$, $[n]$ denotes the set of integers $\{1, \ldots, n\}$. For $m \geq n$, we write $[n, m]$ as a shorthand for $\{n, \ldots, m\}$. $[n, m), (n, m]$ are similarly defined. For $S \subset \mathbb{N}$, X_S denotes the coordinates of X indexed by S. For a set $S \subset \mathbb{N}$ and $n \in \mathbb{N}$, $S_{\leq n}$ denotes $S \cap [n]$ and $S_{<n}$, $S_{>n}$, $S_{\geq n}$ are similarly defined. Hamming distance is denoted by $\Delta(\cdot, \cdot)$. Throughout, we use an EPR pair to denote two qubits in the state $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. We use I_R to denote the identity map on register R.

3.1 The Quantum Communication Model with Erasures

Let q denote the size of the channel alphabet, so the channel Hilbert space is $\mathbb{C}^q$. We use $|\perp\rangle$ to denote an additional basis state representing an erasure. We occasionally write $\perp$ instead of $|\perp\rangle$. A protocol over this channel is specified by a tuple:

$$\Pi = \left(n, T, A, B, \mathsf{p}, (M_t)_{t\in[T]}, \left(\mathcal{K}_t^{\mathsf{P}}, \left(\mathcal{I}^{\mathsf{P}}_{t,K^{\mathsf{P}}_{<t}} \right)_{K^{\mathsf{P}}_{<t} \in \mathcal{K}^{\mathsf{P}}_{<t}} \right)_{\mathsf{P}\in\{\mathsf{A},\mathsf{B}\}, t\in[T+1]}, \tau \right). \tag{1}$$

Here, (1) n denotes the number of qubits in Alice's and Bob's inputs. (2) T denotes the number of rounds in the protocol. (3) A denotes Alice's local quantum registers. These are partitioned into registers A_{inp}, A_{anc}, and A_{out} representing Alice's input, ancillas, and output respectively. The registers A_{anc} and A_{out} are initialized to $|0\rangle$. B is analogous to A but for Bob. (4) $\mathsf{p} : [T] \to \{\mathsf{A}, \mathsf{B}\}$ is a function that determines who transmits in any given round. Thus, $\mathsf{p}^{-1}(\mathsf{A})$ and $\mathsf{p}^{-1}(\mathsf{B})$ denote the set of rounds rounds where Alice and Bob (respectively) transmit. (5) M_t is the message register transmitted in round t, with state space $\mathbb{C}^q$. (6) $\mathcal{K}_t^{\mathsf{P}}$ is the set of classical outcomes of the instruments used by party P in rounds t. We define $\mathcal{K}^{\mathsf{P}}_{<t} = \prod_{t'<t} \mathcal{K}^{\mathsf{P}}_{t'}$ and $\mathcal{K}^{\mathsf{P}}_{\leq t} = \prod_{t'\leq t} \mathcal{K}^{\mathsf{P}}_{t'}$. (7) $\mathcal{I}^{\mathsf{P}}_{t,K^{\mathsf{P}}_{<t}}$ is a quantum instrument that acts on the registers held by party P before round t given that the classical outcomes of the instruments used so far is $K^{\mathsf{P}}_{<t}$. When $t \in [T]$ and $\mathsf{p}(t) \neq \mathsf{P}$, party P is not transmitting in round t and we assume that $\mathcal{I}^{\mathsf{P}}_{t,K^{\mathsf{P}}_{<t}}$ is the trivial instrument consisting of the identity channel and a single

outcome. When $t = T + 1$, these instruments are used by the parties to compute the output at the end of the protocol. (8) $\tau \in \{0\} \cup [T]$ is called the classicality prefix and denotes the length of the protocol prefix during which Bob communicates classically. That is, M_t is restricted to be classical for all $t \in \mathsf{p}^{-1}(\mathsf{B}) \cap [\tau]$.

Execution of Π in the presence of an adversary. Let Π a protocol as above. An adversary for Π is defined by a set $\mathsf{Adv} \subseteq [T]$ representing the set of rounds erased by the adversary. We now describe the execution of Π in the presence of adversary Adv. Assume an arbitrary reference register R. The protocol starts with the registers $A_{\mathsf{inp}}B_{\mathsf{inp}}R$ in the initial (pure) state $|\psi\rangle$. This state is not assumed to be known to Alice and Bob. The protocol runs for T rounds. Before round $t \in [T]$, Alice holds the registers $AM_{\mathsf{p}^{-1}(\mathsf{A})_{\geq t}}\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})_{<t}}$ and has classical outcomes $K^{\mathsf{A}}_{<t} \in \mathcal{K}^{\mathsf{A}}_{<t}$. Similarly, Bob holds the registers $BM_{\mathsf{p}^{-1}(\mathsf{B})_{\geq t}}\tilde{M}_{\mathsf{p}^{-1}(\mathsf{A})_{<t}}$ and has classical outcomes $K^{\mathsf{B}}_{<t} \in \mathcal{K}^{\mathsf{B}}_{<t}$. Here, for all $t \in [T]$, we use $\tilde{M}_t$ to denote the register with the received message. These registers have state space $\mathbb{C}^{q+1}$ with the extra dimension for the possibility of receiving the erasure symbol $|\perp\rangle$.

Round t then proceeds as follows. Alice applies the instrument[8] $\mathcal{I}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$ on the registers $AM_{\mathsf{p}^{-1}(\mathsf{A})_{\geq t}}\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})_{<t}}$. We let K^{A}_t denote the obtained classical outcome. She sends the register M_t over the channel. This register is then intercepted by the adversary. If $t \in \mathsf{Adv}$, the adversary discards this register and sends $\tilde{M}_t = |\perp\rangle$ to Bob. Otherwise, the adversary forwards M_t to Bob unchanged, and we relabel this as $\tilde{M}_t$. After T rounds, Alice applies the instrument $\mathcal{I}^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}$ on the registers $A\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})}$ to populate her output registers. Bob's execution is analogous. The final output state of the protocol is the reduced state on the registers OR, where $O = A_{\mathsf{out}}B_{\mathsf{out}}$.

A noiseless execution. An execution is said to be noiseless if $\mathsf{Adv} = \emptyset$. That is, none of the messages sent during the protocol are erased. We say a protocol is noiseless if we only consider its noiseless execution.

The message transfer task. In this task, Alice starts with an (unknown) quantum state as input, possibly entangled with an arbitrary reference register R, while Bob starts with no input, and the goal is for Bob to output Alice's input state at the end of the protocol (Alice does not have an output). For $\theta > 0$, we say that a protocol Π solves the message transfer task with resilience θ if for all pure input states $|\psi\rangle_{A_{\mathsf{inp}}R}$ and any adversary Adv such that $|\mathsf{Adv}| \leq \lceil \theta T \rceil$, we have that the reduced state on $B_{\mathsf{out}}R$ when the protocol ends is $|\psi\rangle_{B_{\mathsf{out}}R}$.

Two-way code. Protocols designed specifically for the message transfer task are referred to as two-way codes. Thus, instead of saying that a protocol Π solves the message transfer task with resilience θ, we may say that Π is a two-way code with resilience θ. If a two-way code has classicality prefix $\tau = T$, we call it a two-way code for the quantum–classical channel

[8] Recall that this instrument is the trivial instrument if Alice is not transmitting in round t.

and if it has classicality prefix $\tau = 0$, we call it a two-way code for the quantum–quantum channel. In Appendix B, we consider a setting for message transfer where Bob's messages are never corrupted, and not counted in the communication budget. We term our protocol here a two-way code with free noiseless classical feedback.

An interactive coding scheme. The goal of an interactive coding scheme is to transform an arbitrary noiseless protocol Π into another protocol Π' that works even in the presence of noise. For an adversary Adv' for Π', we say that Π' simulates Π in the presence of Adv' if Π and Π' have the same input registers and, for any inputs of Alice and Bob and any reference register R, the output state produced by an execution of Π' in the presence of Adv' is identical to the output state produced by a noiseless execution of Π. For $\theta > 0$, we say that an interactive coding scheme has erasure resilience θ if, given any protocol Π of length T, there exists a protocol Π' of length T' such that for every adversary Adv' for Π' satisfying $|\mathsf{Adv}'| \leq \lceil \theta T' \rceil$, the protocol Π' simulates Π in the presence of Adv'. The worst-case ratio T'/T is called the overhead of the interactive coding scheme.

3.1.1 Pseudo-Measurements

The work [BNT+19] introduces the concept of pseudo-measurements and shows that if Alice and Bob can communicate quantum registers, then the instruments in Equation (1) may be assumed to be unitary operators on a larger Hilbert space with a trivial outcome. In our formulation, Bob is restricted to communicate classically until round τ, and is unrestricted afterwards. Using a similar argument, we show an analogous claim for the instruments used after round τ, including those used for the final output operation.

Theorem 3.1. *Let Π be a protocol of length T and $\tau \in \{0\} \cup [T]$ be such that the classicality prefix of Π is at most τ. There exists an equivalent[9] protocol Π' with the same classicality prefix such that for all $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$, $t \in (\tau, T+1]$, and all $K^{\mathsf{P}}_{<t} \in \mathcal{K}^{\mathsf{P}}_{<t}$, the instrument $\mathcal{I}^{\mathsf{P}}_{t,K^{\mathsf{P}}_{<t}}$ consists of a single unitary operator. It follows that the set $\mathcal{K}^{\mathsf{P}}_t$ is singleton.*

The proof of Theorem 3.1 is in Appendix A.

3.2 Error-Correcting Codes

We use the following (classical) codes that can efficiently encode and decode from a fraction of erasures approaching 1.

Lemma 3.2 ([GI05], Theorem 3)**.** *For all $0 < R < 1$ and all sufficiently small $\epsilon > 0$, there exists an explicitly specified family of codes of rate R and relative distance at least $1 - R - \epsilon$ over an alphabet of size $K_{\mathsf{C}} = O_{R,\epsilon}(1)$ such that codes from the family can be encoded and decoded in linear time from $(1 - R - \epsilon)$-fraction of erasures.*

[9] That is, Π and Π' have the same length and induce the same input-output map for every adversary.

Following is an analogous result for quantum codes that can efficiently encode and decode from a fraction of erasures approaching $\frac{1}{2}$.

Lemma 3.3 ([BGG22], Corollary 5.3)**.** *For all $0 < R < 1$ and all sufficiently small $\epsilon > 0$, there exists an explicit infinite family of quantum LDPC CSS codes of rate R and relative distance $\frac{1-R-\epsilon}{2}$ over an alphabet of size $K_{\mathsf{Q}} = O_\epsilon(1)$ such that codes from the family can be encoded and decoded in polynomial time from $(1-R-\epsilon)$-fraction of erasures.*

Note that Corollary 5.3 in [BGG22] does not talk about polynomial time encodability and decodability from erasures, but these are standard, see [CG97, Got97, KO26]. It follows from the no-cloning theorem that the $\frac{1}{2}$ resilience above is tight.

Theorem 3.4 (No-cloning theorem, [WZ82, Die82])**.** *Let A, B, E be registers. There does not exist a unitary U such that for any state $|\psi\rangle_A$, there exists a state $|\rho_\psi\rangle_E$ satisfying $U(|\psi\rangle_A |0\rangle_{BE}) = |\psi\rangle_A |\psi\rangle_B |\rho_\psi\rangle_E$.*

Proof. We include a short proof for completeness. If such a unitary exists, then, in particular,

$$U(|0\rangle_A |0\rangle_{BE}) = |0\rangle_A |0\rangle_B |\rho_0\rangle_E \qquad\qquad U(|+\rangle_A |0\rangle_{BE}) = |+\rangle_A |+\rangle_B |\rho_+\rangle_E .$$

This means that

$$\langle 0|+\rangle_A \langle 0|0\rangle_{BE} = (\langle 0|_A \langle 0|_{BE}) U^\dagger U (|+\rangle_A |0\rangle_{BE}) = \langle 0|+\rangle_A \langle 0|+\rangle_B \langle \rho_0|\rho_+\rangle_E .$$

However, as $\langle 0|+\rangle = \frac{1}{\sqrt{2}}$, we derive that $\sqrt{2} = \langle \rho_0|\rho_+\rangle_E$, which is impossible for any two quantum states, a contradiction. □

Lemma 3.5. *Any quantum code (regardless of its alphabet size and rate) is resilient to at most $1/2$ fraction of adversarial erasures.*

We also need the standard quantum primitive of teleportation.

Lemma 3.6 (Teleportation [BBC+93])**.** *Given one pre-shared EPR pair, one qubit can be transmitted by sending two classical bits.*

4 Impossibility Results for Two-Way Codes

In this section, we prove Theorems 4.1 and 4.2. They are the formal versions of the impossibility results stated in Theorems 1.1 and 1.2.

Theorem 4.1. *No two-way code for the quantum–classical channel is resilient to a $3/5$-fraction of adversarial erasures, regardless of its alphabet size and rate.*

Theorem 4.2. *No two-way code for the quantum–quantum channel is resilient to a $2/3$-fraction of adversarial erasures, regardless of its alphabet size and rate.*

Fix an arbitrary protocol Π of length T. Let $\hat{f}$ be its erasure resilience. Throughout, $f_{\mathsf{A}}, f_{\mathsf{B}}$ denote the fractions of Alice's and Bob's communication respectively, so $f_{\mathsf{A}} + f_{\mathsf{B}} = 1$.

As a warm-up, we start by showing the following Lemma 4.3, which immediately implies that resilience beyond $2/3$ cannot be achieved regardless of the type of the backward channel from Bob to Alice, by maximizing $\min(f_{\mathsf{A}}, f_{\mathsf{A}}/2 + f_{\mathsf{B}})$ subject to $f_{\mathsf{A}} + f_{\mathsf{B}} = 1$. Theorem 4.2 then follows.

Lemma 4.3. *It holds that* $\hat{f} \leq \min(f_{\mathsf{A}}, f_{\mathsf{A}}/2 + f_{\mathsf{B}})$.

Proof. Consider two possible strategies for the adversary. For the first one, the adversary simply erases all of Alice's communication. Bob cannot learn any information about the input. For the second one, the adversary erases all of Bob's communication. Thus, the model reduces to the one-way setting. By Lemma 3.5, the adversary can prevent Bob from learning the input by erasing half of Alice's communication. The lemma statement then follows. □

In the rest of this section, we focus on the case of a classical backward channel. We refer to the first $f_{\mathsf{p}} = \frac{3}{5}$ fraction of communication as the prefix, and the remaining $f_{\mathsf{s}} = \frac{2}{5}$ fraction as the suffix. The point between the prefix and the suffix is called the cutoff. Let $f_{\mathsf{A,p}}, f_{\mathsf{A,s}}$ be the fractions of Alice's communication in the prefix and the suffix respectively, so $f_{\mathsf{A,p}} + f_{\mathsf{A,s}} = f_{\mathsf{A}}$. Also let $f_{\mathsf{B,p}}, f_{\mathsf{B,s}}$ be the fractions of Bob's communication in the prefix and the suffix respectively, so $f_{\mathsf{B,p}} + f_{\mathsf{B,s}} = f_{\mathsf{B}}$. By definition, it must be that $f_{\mathsf{A,p}} + f_{\mathsf{B,p}} = f_{\mathsf{p}} = \frac{3}{5}$ and $f_{\mathsf{A,s}} + f_{\mathsf{B,s}} = f_{\mathsf{s}} = \frac{2}{5}$.

In Section 4.1, we prove that $\hat{f} \leq 3/5$ if $f_{\mathsf{A,p}} \leq f_{\mathsf{A,s}}$. On the other hand, Section 4.2 shows that $f_{\mathsf{A,p}} > f_{\mathsf{A,s}}$ is actually impossible due to the no-cloning theorem [WZ82]. Combining the two cases proves Theorem 4.1.

Remark 4.4. *The impossibility of resilience beyond* $3/5$ *is robust to different weighting of quantum and classical communication. In particular, for any* $\gamma > 0$*, Theorem 4.1 still holds if each qudit of communication and erasure has weight* 1 *while each classical symbol of communication and erasure has weight* γ*. That is, any two-way code over the quantum-classical channel has erasure resilience at most* $(\beta_{\mathsf{Q}} + \gamma \cdot \beta_{\mathsf{C}})/(\alpha_{\mathsf{Q}} + \gamma \cdot \alpha_{\mathsf{C}}) \leq 3/5$*, where* $\alpha_{\mathsf{Q}}, \alpha_{\mathsf{C}}$ *are the total number of quantum and classical communication rounds respectively and* $\beta_{\mathsf{Q}}, \beta_{\mathsf{C}}$ *are the total number of quantum and classical erasures respectively. This can be proved by considering the weighted version of the fractions* $\hat{f}, f_{\mathsf{A}}, f_{\mathsf{B}}, f_{\mathsf{p}}, f_{\mathsf{s}}$*, etc. Arguments similar to the analysis in Sections 4.1 and 4.2 still hold.*

4.1 The case $f_{\mathsf{A,p}} \leq f_{\mathsf{A,s}}$

Consider the adversary that erases all of Alice's communication in the prefix. Since all of Alice's communication in the prefix is erased, Bob's local state at the cutoff, as well as all his communication in the prefix, is independent of the input, as Alice and Bob do not have pre-shared entanglement.

Let Π' be another protocol consisting only of the suffix of Π, where both Alice and Bob start with their local states at the cutoff[10]. Note that Bob can only send via a classical[11] channel to Alice, so Alice and Bob cannot have any shared entanglement at the beginning of the Π'. This means that Π' is also a valid protocol with $f'_{\mathsf{A}} = f_{\mathsf{A,s}}/f_{\mathsf{s}}$ and $f'_{\mathsf{B}} = f_{\mathsf{B,s}}/f_{\mathsf{s}}$. By Lemma 4.3, Π' is resilient to at most $\hat{f}' \le f'_{\mathsf{A}}/2 + f'_{\mathsf{B}}$ fraction of adversarial erasures. Overall, the erasure resilience of Π is at most

$$\begin{aligned}
\hat{f} &\le f_{\mathsf{A,p}} + f_{\mathsf{s}} \cdot \hat{f}' \\
&\le f_{\mathsf{A,p}} + f_{\mathsf{s}} \cdot (f'_{\mathsf{A}}/2 + f'_{\mathsf{B}}) \\
&= f_{\mathsf{A}} - f_{\mathsf{A,s}} + f_{\mathsf{A,s}}/2 + f_{\mathsf{B,s}} && (\text{as } f_{\mathsf{A,p}} = f_{\mathsf{A}} - f_{\mathsf{A,s}}) \\
&= \frac{2}{5} + f_{\mathsf{A}} - 3f_{\mathsf{A,s}}/2 && (\text{as } f_{\mathsf{B,s}} = f_{\mathsf{s}} - f_{\mathsf{A,s}} = \tfrac{2}{5} - f_{\mathsf{A,s}}) \\
&\le \frac{2}{5} + f_{\mathsf{A}}/4 && (\text{as } f_{\mathsf{A,s}} \ge f_{\mathsf{A}}/2 \text{ due to } f_{\mathsf{A,p}} \le f_{\mathsf{A,s}})
\end{aligned}$$

This implies that $\hat{f} \le \frac{2}{5} + f_{\mathsf{A}}/4$. By Lemma 4.3, maximizing $\min(f_{\mathsf{A}}/2 + f_{\mathsf{B}}, \frac{2}{5} + f_{\mathsf{A}}/4)$ subject to $f_{\mathsf{A}} + f_{\mathsf{B}} = 1$ shows $\hat{f} \le 3/5$, as claimed.

It is worth noting that the maximum $\hat{f} = 3/5$ is attained only when $f_{\mathsf{A}} = 4/5$. In fact, the argument above further implies that in order to achieve $\hat{f} = 3/5$, it must be that $f_{\mathsf{A,p}} = f_{\mathsf{A,s}} = 2/5$, and thus $f_{\mathsf{B,p}} = 1/5$ and $f_{\mathsf{B,s}} = 0$. In other words, Alice should send twice as much as Bob in the first $3/5$ fraction and Bob should remain silent in the last $2/5$ fraction. As we will see in Section 5, this is exactly what our protocol does.

4.2 The case $f_{\mathsf{A,p}} > f_{\mathsf{A,s}}$

In this case, we show that even a quantum–quantum protocol (namely, one with classicality prefix $\tau = 0$) cannot have resilience $3/5$. Indeed, suppose that Π is such a protocol and consider the protocol Π' where all the $f_{\mathsf{B,p}}$ rounds where Bob speaks in the prefix are always erased. If Π has resilience $3/5$, then Π' solves the message transfer even if $f_{\mathsf{A,p}}T$ of its rounds are erased. Moreover, as Π has classicality prefix $\tau = 0$, so does Π', we have from Theorem 3.1 that we can assume without loss of generality that Alice's and Bob's instruments in Π' have a single unitary operation and a fixed outcome. We need the following lemma.

Lemma 4.5. *Consider registers $A_1, A_2, B_1, B'_1, B_2, B'_2$. There do not exists unitaries U on the register A_1A_2, V_1 on the registers $A_1B_1B'_1$, and V_2 on the registers $A_2B_2B'_2$ such that for*

[10] Technically, Alice's and Bob's local states at the cutoff and Bob's communication in the prefix might be random due to local randomness (e.g., from local measurement). Nevertheless, since the protocol is always successful, the correctness guarantee must hold even conditioned on any such randomness. Then, for the purpose of constructing Π', it is without loss of generality to assume that the protocol is deterministic in the prefix. In particular, Alice's local state at the cutoff is a function of the input and Bob has a fixed local state at the cutoff regardless of input, so Π' is well-defined.

[11] This is the only place where the proof relies on the classicality of the backward channel.

any state $|\psi\rangle_{A_1}$*, there exist* $|\rho_{\psi,1}\rangle_{A_1A_2B_1'B_2B_2'}$ *and* $|\rho_{\psi,2}\rangle_{A_1A_2B_1B_1'B_2'}$ *satisfying both the following:*

$$\big(V_1 \otimes \mathsf{I}_{A_2B_2B_2'}\big)\Big(\big(U\,|\psi,0\rangle_{A_1A_2}\big)\,|0\rangle_{B_1B_1'B_2B_2'}\Big) = |\psi\rangle_{B_1}\,|\rho_{\psi,1}\rangle_{A_1A_2B_1'B_2B_2'}\,,$$
$$\big(\mathsf{I}_{A_1B_1B_1'} \otimes V_2\big)\Big(\big(U\,|\psi,0\rangle_{A_1A_2}\big)\,|0\rangle_{B_1B_1'B_2B_2'}\Big) = |\psi\rangle_{B_2}\,|\rho_{\psi,2}\rangle_{A_1A_2B_1B_1'B_2'}\,.$$

Proof. Assume there are such unitaries. We first use a standard inner product argument to show that $\rho_{\psi,1}$ is independent of ψ. A similar argument shows that $\rho_{\psi,2}$ is independent of ψ. As U and V_1 are unitary, for any ψ, ψ', we have:

$$\langle\psi|\psi'\rangle_{A_1}\,\langle 0|0\rangle_{A_2}\,\langle 0|0\rangle_{B_1B_1'B_2B_2'} = \langle\psi|\psi'\rangle_{B_1}\,\langle\rho_{\psi,1}|\rho_{\psi',1}\rangle_{A_1A_2B_1'B_2B_2'}$$

This means that for non-orthogonal ψ, ψ', we have $\langle\rho_{\psi,1}|\rho_{\psi',1}\rangle_{A_1A_2B_1'B_2B_2'} = 1$ implying that $\rho_{\psi,1} = \rho_{\psi',1}$. The argument extends to orthogonal ψ, ψ' by taking a ψ'' in their superposition that is not orthogonal to either of them. As $\rho_{\psi,1}$ and $\rho_{\psi,2}$ are independent of ψ, we simply write ρ_1 and ρ_2 respectively.

Next, note that $V_1 \otimes V_2 = \big(V_1 \otimes \mathsf{I}_{A_2B_2B_2'}\big)\big(\mathsf{I}_{A_1B_1B_1'} \otimes V_2\big) = \big(\mathsf{I}_{A_1B_1B_1'} \otimes V_2\big)\big(V_1 \otimes \mathsf{I}_{A_2B_2B_2'}\big)$. Thus, for all $|\psi\rangle_{A_1}$, we have:

$$\big(V_1 \otimes \mathsf{I}_{A_2B_2B_2'}\big)\,|\psi\rangle_{B_2}\,|\rho_2\rangle_{A_1A_2B_1B_1'B_2'} = \big(\mathsf{I}_{A_1B_1B_1'} \otimes V_2\big)\,|\psi\rangle_{B_1}\,|\rho_1\rangle_{A_1A_2B_1'B_2B_2'}\,.$$

Let $R = A_1A_2B_1'B_2'$ and define $|\rho_1'\rangle_{RB_1} = \big(V_1 \otimes \mathsf{I}_{A_2B_2'}\big)\,|\rho_2\rangle_{RB_1}$ and $|\rho_2'\rangle_{RB_2} = \big(\mathsf{I}_{A_1B_1'} \otimes V_2\big)\,|\rho_1\rangle_{RB_2}$. We get:

$$|\rho_1'\rangle_{RB_1}\,|\psi\rangle_{B_2} = |\rho_2'\rangle_{RB_2}\,|\psi\rangle_{B_1}\,.$$

As these are pure states, this is possible only if there exists ρ such that they are both equal to $|\rho\rangle_R\,|\psi\rangle_{B_1}\,|\psi\rangle_{B_2}$. Overall, we get that:

$$(V_1 \otimes V_2)\Big(\big(U\,|\psi,0\rangle_{A_1A_2}\big)\,|0\rangle_{B_1B_1'B_2B_2'}\Big) = |\rho\rangle_R\,|\psi\rangle_{B_1}\,|\psi\rangle_{B_2}\,.$$

We finish with a standard no-cloning argument like in Theorem 3.4. Taking the inner product when $|\psi\rangle = |0\rangle$ and when $|\psi\rangle = |+\rangle$, we get $\langle\rho|\rho\rangle_R = \sqrt{2}$, a contradiction. □

Corollary 4.6. *Consider registers* A_1, A_2, B, B'*. There do not exists unitaries* U *on the register* A_1A_2*,* V_1 *on the registers* A_1BB'*, and* V_2 *on the registers* A_2BB' *such that for any state* $|\psi\rangle_{A_1}$*, there exist* $|\rho_{\psi,1}\rangle_{A_1A_2B'}$ *and* $|\rho_{\psi,2}\rangle_{A_1A_2B'}$ *satisfying both the following:*

$$(V_1 \otimes \mathsf{I}_{A_2})\big(\big(U\,|\psi,0\rangle_{A_1A_2}\big)\,|0\rangle_{BB'}\big) = |\psi\rangle_B\,|\rho_{\psi,1}\rangle_{A_1A_2B'}\,,$$
$$(\mathsf{I}_{A_1} \otimes V_2)\big(\big(U\,|\psi,0\rangle_{A_1A_2}\big)\,|0\rangle_{BB'}\big) = |\psi\rangle_B\,|\rho_{\psi,2}\rangle_{A_1A_2B'}\,.$$

Proof. Consider registers C, C'. The two equations imply

$$(V_1 \otimes \mathsf{I}_{A_2CC'})\big(\big(U\,|\psi,0\rangle_{A_1A_2}\big)\,|0\rangle_{BB'CC'}\big) = |\psi\rangle_B\,|\rho_{\psi,1}\rangle_{A_1A_2B'}\,|0\rangle_{CC'}\,,$$

$$(\mathsf{I}_{A_1CC'} \otimes V_2)\left(\left(U\left|\psi,0\right\rangle_{A_1A_2}\right)\left|0\right\rangle_{BB'CC'}\right) = \left|\psi\right\rangle_B \left|\rho_{\psi,2}\right\rangle_{A_1A_2B'} \left|0\right\rangle_{CC'}.$$

Relabelling the second equation, we get,

$$(V_1 \otimes \mathsf{I}_{A_2CC'})\left(\left(U\left|\psi,0\right\rangle_{A_1A_2}\right)\left|0\right\rangle_{BB'CC'}\right) = \left|\psi\right\rangle_B \left|\rho_{\psi,1}\right\rangle_{A_1A_2B'} \left|0\right\rangle_{CC'},$$
$$(\mathsf{I}_{A_1BB'} \otimes V_2)\left(\left(U\left|\psi,0\right\rangle_{A_1A_2}\right)\left|0\right\rangle_{BB'CC'}\right) = \left|\psi\right\rangle_C \left|\rho_{\psi,2}\right\rangle_{A_1A_2C'} \left|0\right\rangle_{BB'}.$$

This contradicts Lemma 4.5. □

Suppose that Alice's input register A_{inp} in Π' is initialized to some pure state $\left|\psi\right\rangle_{A_{\mathsf{inp}}}$. Let M denote all the message registers used in Π'. Partition the registers M into the registers M_{p} used before the prefix and registers M_{s} used after the prefix. Further partition M_{s} into registers $M_{\mathsf{s}}^{\mathsf{A}}$ and $M_{\mathsf{s}}^{\mathsf{B}}$ sent by Alice and Bob respectively. Define $A' = AM_{\mathsf{s}}^{\mathsf{A}}$ and $B' = BM_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{B}}$. As only Alice speaks in the prefix Π', there exists a unitary U on the registers $AM_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}$ such that state at the cutoff is $\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}$.

Now, consider an adversary Adv_1 that erases all of Alice's messages after the cutoff. As $f_{\mathsf{A},\mathsf{p}} > f_{\mathsf{A},\mathsf{s}}$, the protocol Π' should solve message transfer in the presence of Adv_1. As Bob does not receive anything after the cutoff, this means that there exists unitaries U_1^{A} and U_1^{B} on the registers $A'M_{\mathsf{s}}^{\mathsf{B}}$ and B' respectively such that the joint state at the end of the protocol is $\left(U_1^{\mathsf{A}} \otimes \mathsf{I}_{BM_{\mathsf{p}}}\right)\left(\mathsf{I}_{A'} \otimes U_1^{\mathsf{B}}\right)\left(\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}\right)$.

Next, consider an adversary Adv_2 that erases all of Alice's messages before the cutoff. The protocol Π' should solve message transfer in the presence of Adv_2 as well. This means that there exists a unitary U_2 on the register $A'BM_{\mathsf{s}}^{\mathsf{B}}$ such that the joint state at the end of the protocol is $\left(U_2 \otimes \mathsf{I}_{M_{\mathsf{p}}}\right)\left(\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}\right)$.

These states are both pure states and Bob computes his output $\left|\psi\right\rangle_{A_{\mathsf{inp}}}$ by tracing out registers other than B_{out}. As tracing out a part of a pure state gives another pure state only if the original state factors, we have for some $\left|\rho_{\psi,1}\right\rangle_{AMB_{\mathsf{anc}}}$ and $\left|\rho_{\psi,2}\right\rangle_{AMB_{\mathsf{anc}}}$ that:

$$\left(U_1^{\mathsf{A}} \otimes \mathsf{I}_{BM_{\mathsf{p}}}\right)\left(\mathsf{I}_{A'} \otimes U_1^{\mathsf{B}}\right)\left(\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}\right) = \left|\psi\right\rangle_{B_{\mathsf{out}}}\left|\rho_{\psi,1}\right\rangle_{AMB_{\mathsf{anc}}},$$
$$\left(U_2 \otimes \mathsf{I}_{M_{\mathsf{p}}}\right)\left(\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}\right) = \left|\psi\right\rangle_{B_{\mathsf{out}}}\left|\rho_{\psi,2}\right\rangle_{AMB_{\mathsf{anc}}}.$$

Multiplying the first equation by $\left(U_1^{\mathsf{A},\dagger} \otimes \mathsf{I}_{BM_{\mathsf{p}}}\right)$ and reparameterizing

$$\left(\mathsf{I}_{A'} \otimes U_1^{\mathsf{B}}\right)\left(\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}\right) = \left|\psi\right\rangle_{B_{\mathsf{out}}}\left|\rho_{\psi,1}\right\rangle_{AMB_{\mathsf{anc}}},$$
$$\left(U_2 \otimes \mathsf{I}_{M_{\mathsf{p}}}\right)\left(\left(U\left|\psi\right\rangle_{A_{\mathsf{inp}}}\left|0\right\rangle_{A_{\mathsf{anc}}M_{\mathsf{p}}M_{\mathsf{s}}^{\mathsf{A}}}\right)\left|0\right\rangle_{BM_{\mathsf{s}}^{\mathsf{B}}}\right) = \left|\psi\right\rangle_{B_{\mathsf{out}}}\left|\rho_{\psi,2}\right\rangle_{AMB_{\mathsf{anc}}}.$$

This contradicts Corollary 4.6.

5 Two-Way Code for the Quantum-Classical Channel

In this section, we present the protocol for proving Theorem 5.1, which is the formal version of achievability stated in Theorem 1.1. Its analysis is given in Section 5.1.

Theorem 5.1. *For all $\epsilon > 0$, there exists a two-way code for the quantum–classical channel with resilience $(3/5 - \epsilon)$ over an alphabet of size $q = O_\epsilon(1)$, constant rate $\Omega_\epsilon(1)$, and runs in polynomial time.*

Notation and parameters. Let A_{inp} and B_{out} be n-qubit registers[12] for input and output respectively, and $3/5 - \epsilon$ the target erasure resilience. Set $L = 100n/\epsilon$ and $R = 10/\epsilon$. Let K'_{C} be the constant claimed by Lemma 3.2 for rate $\epsilon/100$ and relative distance $1 - \epsilon/10$, and set $K_{\mathsf{C}} = \max(K'_{\mathsf{C}}, 2^{400R/\epsilon})$. Let K_{Q} be the constant claimed by Lemma 3.3 for rate $\epsilon/100$ and relative distance $1/2 - \epsilon/10$.

The protocol consists of $2R$ iterations. Alice first sends $2L$ qudits over an alphabet of size $K = 10R \cdot \max(K_{\mathsf{Q}}, K_{\mathsf{C}})$ in every iteration. In each of the first R iterations, Bob also sends L classical symbols over an alphabet of size K_{C}, after receiving Alice's messages (or erasures). The overall length of the protocol is thus $T = 5LR = O_\epsilon(n)$.

One-way coding primitives. For $r \in [R+1]$, set $T_r = 2L \cdot (2R - r + 1)$ and let C^{Q} be a one-way quantum erasure code with n-qubit inputs and T_r-qudit codewords over an alphabet of size K_{Q}, that has resilience $1/2 - \epsilon/10$. Their existence is guaranteed by Lemma 3.3 as $T_r \geq 2LR \geq L$.

Let C^{B} be a one-way classical erasure code with $4LR$-bit inputs, which can be equivalently viewed as n symbols over an alphabet of size $2^{400R/\epsilon}$, and L-symbol codewords over an alphabet of size K_{C}, that has resilience $1 - \epsilon/10$. Meanwhile, for $r \in [R+1]$, let $\mathsf{C}^{\mathsf{A}}_r$ be a one-way classical erasure code with $2n$-bit inputs and T_r-symbol codewords over an alphabet of size K_{C}, that has resilience $1 - \epsilon/10$. Their existence is guaranteed by Lemma 3.2 as $T_r \geq 2LR \geq L$.

Let $\mathsf{D}^{\mathsf{A}}, \mathsf{D}^{\mathsf{B}}, \mathsf{D}^{\mathsf{Q}}$ be the decoding functions corresponding to $\mathsf{C}^{\mathsf{A}}, \mathsf{C}^{\mathsf{B}}, \mathsf{C}^{\mathsf{Q}}$ respectively. A classical erasure is denoted $\perp$ and a quantum erasure is denoted $|\perp\rangle$.

The protocol. The Alice's and Bob's sides of the protocol are given in Algorithms 1 and 2 respectively. Capital letters W, X, Y, Z are reserved for quantum registers. All other variables are classical. If some variable var appears in both sides of the protocol, we may use superscripts A, B to avoid confusion when necessary. That is, we write $\mathsf{var}^{(\mathsf{A})}$ for Alice's copy and $\mathsf{var}^{(\mathsf{B})}$ for Bob's copy. Similarly, if the same variable var is used across multiple iterations, we write $\mathsf{var}^{(r)}$ to denote its value at the end of the r-th (outer) iteration. The superscripts are omitted when they are clear from context.

[12] We assume the input and the output are binary, instead of having the same dimension $O_\epsilon(1)$ as the channel. This is without loss of generality up to a $\Theta_\epsilon(1)$ factor in rate.

Algorithm 1 Alice's side of the protocol with input register A_{inp}.

Initialize teleport variable $\mathsf{tp} \leftarrow 0$, restart variable $\mathsf{rst} \leftarrow 1$, and $\mathsf{iter} \leftarrow 1$.
Encode $W^{(\mathsf{iter})} \leftarrow \mathsf{C}^{\mathsf{Q}}_{\mathsf{iter}}(A_{\mathsf{inp}})$.
for $r \in [2R]$ **do**
    for $\ell \in [2L]$ **do**
        Initialize a fresh EPR pair $(Z^{(\mathsf{A})}_{2L\cdot(r-1)+\ell}, Z^{(\mathsf{B})}_{2L\cdot(r-1)+\ell})$.
        Send $|\mathsf{tp}\rangle \otimes |\mathsf{iter}\rangle \otimes Z^{(\mathsf{B})}_{2L\cdot(r-1)+\ell} \otimes W^{(\mathsf{iter})}_{2L\cdot(r-\mathsf{iter})+\ell}$ (as one qudit) to Bob.
    if $2L \cdot (r - \mathsf{iter} + 1) \geq (1/2 - \epsilon/10) \cdot T_{\mathsf{iter}}$ **then**
        Set $\mathsf{rst} \leftarrow 0$.
    if $r \in [R]$ **then**
        Receive an L-symbol string $B^{(r)}$ from Bob.
        Decode $b^{(r)} \leftarrow \mathsf{D}^{\mathsf{B}}(B^{(r)})$.
        if $\mathsf{rst} = 1$ **and** $b^{(r)} \neq \perp$ **then**
            Decode $A_{\mathsf{inp}} \leftarrow \mathsf{D}^{\mathsf{Q}}_{\mathsf{iter}}(|\perp\rangle^{\otimes 2L\cdot(r-\mathsf{iter}+1)} \otimes W^{(\mathsf{iter})}_{(2L\cdot(r-\mathsf{iter}+1),T_{\mathsf{iter}}]})$.
            Set $\mathsf{iter} \leftarrow r + 1$.
            if $b^{(r)}$ has at least n bits "1" **then**
                Set $\mathsf{tp} \leftarrow 1$ and $\mathsf{rst} \leftarrow 0$.
                Teleport A_{inp} using EPR halves $Z^{(\mathsf{A})}$ indexed by the first n bits "1" in $b^{(r)}$, resulting in $2n$ teleportation bits a.
                Encode $W^{(\mathsf{iter})} \leftarrow |\mathsf{C}^{\mathsf{A}}_{\mathsf{iter}}(a)\rangle$.
            else
                Encode $W^{(\mathsf{iter})} \leftarrow \mathsf{C}^{\mathsf{Q}}_{\mathsf{iter}}(A_{\mathsf{inp}})$.

Remark 5.2. *The achievability of $3/5-\epsilon$ resilience is robust to different weighting of quantum and classical communication. In particular, for any $\gamma > 0$, Theorem 5.1 still holds if each qudit of communication and erasure has weight 1 while each classical symbol of communication and erasure has weight γ. That is, there exists a two-way code over the quantum-classical channel that has erasure resilience at least $(\beta_{\mathsf{Q}} + \gamma \cdot \beta_{\mathsf{C}})/(\alpha_{\mathsf{Q}} + \gamma \cdot \alpha_{\mathsf{C}}) \geq 3/5 - \epsilon$, where $\alpha_{\mathsf{Q}}, \alpha_{\mathsf{C}}$ are the total number of quantum and classical communication respectively and $\beta_{\mathsf{Q}}, \beta_{\mathsf{C}}$ are the total number of quantum and classical erasures respectively. This can be proved by adjusting the length of Bob's classical communication in Algorithm 2 by a factor of $1/\gamma$. Arguments similar to the analysis in Section 5.1 still hold.*

5.1 Analysis

Fix an arbitrary n-qubit input state of A_{inp} for Alice, and any adversary with at most $(3/5-\epsilon)\cdot T$ erasures. We show that Bob's output B_{out} at the end of the protocol always has exactly the same state, hence proving Theorem 5.1.

We first verify that the protocol is well-defined, starting with a couple of basic properties of the classical variables.

Lemma 5.3. *For $r \in [2R]$, it holds that*

Algorithm 2 Bob's side of the protocol with output register B_{out}.

Initialize $\mathsf{end} \leftarrow 0$, $b^{(0)} \leftarrow 0^{4LR}$, and $Z^{(\mathsf{B})} \leftarrow |\perp\rangle^{\otimes 4LR}$.
for $r \in [2R]$ **do**
    Set $b^{(r)} \leftarrow b^{(r-1)}$.
    if $r \in [R+1]$ **then**
        Initialize $A^{(r)} \leftarrow \perp^{T_r}$ and $W^{(r)} \leftarrow |\perp\rangle^{\otimes T_r}$.
    for $\ell \in [2L]$ **do**
        Receive $|\mathsf{tp}\rangle \otimes |\mathsf{iter}\rangle \otimes Z' \otimes W'$ (as one qudit) from Alice.
        if $\mathsf{end} = 0$ **and** $|\mathsf{tp}\rangle \otimes |\mathsf{iter}\rangle \otimes Z' \otimes W' \neq |\perp\rangle$ **then**
            Set $b^{(r)}_{2L\cdot(r-1)+\ell} \leftarrow 1$.
            Relabel Z' as $Z^{(\mathsf{B})}_{2L\cdot(r-1)+\ell}$.
            if $\mathsf{tp} = 1$ **then**
                Set $A^{(\mathsf{iter})}_{2L\cdot(r-\mathsf{iter})+\ell} \leftarrow s$ where $W' = |s\rangle$.
                if $A^{(\mathsf{iter})}$ has at least $\epsilon/10 \cdot T_{\mathsf{iter}}$ non-erasure symbols **then**
                    Decode $a \leftarrow \mathsf{D}^{\mathsf{A}}_{\mathsf{iter}}(A^{(\mathsf{iter})})$.
                    Recover B_{out} from EPR halves $Z^{(\mathsf{B})}$ indexed by the first n "1"-s in $b^{(r)}$, corrected by $2n$ teleportation bits a.
                    Set $\mathsf{end} \leftarrow 1$.
            else
                Relabel W' as $W^{(\mathsf{iter})}_{2L\cdot(r-\mathsf{iter})+\ell}$.
                if $W^{(\mathsf{iter})}$ has at least $(1/2 + \epsilon/10) \cdot T_{\mathsf{iter}}$ non-erasure qudits **then**
                    Decode $B_{\mathsf{out}} \leftarrow \mathsf{D}^{\mathsf{Q}}_{\mathsf{iter}}(W^{(\mathsf{iter})})$.
                    Set $\mathsf{end} \leftarrow 1$.
    if $r \in [R]$ **then**
        Send the L-symbol string $\mathsf{C}^{\mathsf{B}}(b^{(r)})$ to Alice.

1.
$$\mathsf{tp}^{(\mathsf{A},r-1)} \leq \mathsf{tp}^{(\mathsf{A},r)}.$$

2.
$$\mathsf{rst}^{(r-1)} \geq \mathsf{rst}^{(r)}.$$

3.
$$\mathsf{iter}^{(\mathsf{A},r-1)} \leq \mathsf{iter}^{(\mathsf{A},r)} \leq \max(r, R) + 1.$$

4.
$$\mathsf{end}^{(r-1)} \leq \mathsf{end}^{(r)}.$$

5.
$$\forall j \in [4LR], \qquad b_j^{(\mathsf{B},r-1)} \leq b_j^{(\mathsf{B},r)} \leq \mathbb{1}[j \leq 2Lr].$$

Proof. For Item 1, note that $\mathsf{tp}^{(\mathsf{A})} \in \{0,1\}$ and it starts with value 0 in Line 1. Once setting $\mathsf{tp}^{(\mathsf{A})} \leftarrow 1$ in Line 16, it keeps at value 1.

For Item 2, note that $\mathsf{rst}^{(\mathsf{A})} \in \{0,1\}$ and it starts with value 1 in Line 1. Once setting $\mathsf{rst}^{(\mathsf{A})} \leftarrow 0$ in either Line 16 or Line 8, it keeps at value 0.

Regarding Item 3, suppose Line 14 is not executed by Alice in the current iteration. Then, by induction, we can get $\mathsf{iter}^{(\mathsf{A},r)} = \mathsf{iter}^{(\mathsf{A},r-1)} \leq (r-1)+1 < r+1$. Otherwise, it must be that $\mathsf{iter}^{(\mathsf{A},r)} = r+1 > (r-1)+1 \geq \mathsf{iter}^{(\mathsf{A},r-1)}$. To see $\mathsf{iter}^{(\mathsf{A},r)} \leq R+1$, note that Line 14 is executed by Alice only if $r \in [R]$.

For Item 4, note that $\mathsf{end}^{(\mathsf{B})} \in \{0,1\}$ and it starts with value 0 in Line 21. Once setting $\mathsf{end}^{(\mathsf{B})} \leftarrow 1$ in either Line 36 or Line 41, it keeps at value 1.

As to Item 5, fix $j \in [4LR]$. Lines 21, 23 and 29 altogether imply that $b_j^{(\mathsf{B})} \in \{0,1\}$ and it starts with value 0. Once setting $b_j^{(\mathsf{B})} \leftarrow 1$, it keeps at value 1. Furthermore, this happens in the r-th iteration only for $j \in (2L \cdot (r-1), 2Lr]$, hence proving the second inequality. □

We also need to ensure that all codes and alphabet sizes are compatible. Note that by definition, $T_r = 2L \cdot (2R - r + 1)$ is exactly the number of qudits that Alice sends from the r-th iteration onwards. Then, it suffices to show that Alice sends qudits over an alphabet of size at most K in Line 6. To this end, note that $\mathsf{tp} \in \{0,1\}$, $\mathsf{iter} \in [2R+1]$, and that $Z^{(\mathsf{B})}_{2L\cdot(r-1)+\ell}$ is half of an EPR pair. Also note that $W^{(\mathsf{iter})}$ uses an alphabet of size at most $\max(K_{\mathsf{Q}}, K_{\mathsf{C}})$ due to Lines 2, 18 and 20. The overall dimension is thus at most $2 \cdot (2R+1) \cdot 2 \cdot \max(K_{\mathsf{Q}}, K_{\mathsf{C}}) \leq K$ as claimed.

As to the quantum registers, we point out that in Lines 30 and 38, by relabeling, the protocol is not cloning quantum registers but simply swapping the received registers with the local registers. It is also worth noting that quantum measurement is performed only for two purposes (other than detecting erasures). One is for Bob to extract classical information from the received qudit in Lines 27 and 32. The other is for Alice to teleport in Line 17. All other quantum steps are unitary operations (or CPTP maps to be more precise).

In the first case, for any fixed iteration, the qudit received by Bob in Line 27 must be the same as the qudit sent by Alice in Line 6, unless there is an erasure. Therefore, whenever the qudit is not erased, Bob can always extract $\mathsf{tp}^{(\mathsf{B},r)} = \mathsf{tp}^{(\mathsf{A},r-1)}$ and $\mathsf{iter}^{(\mathsf{B},r)} = \mathsf{iter}^{(\mathsf{A},r-1)}$ by measurement in the standard basis[13]. This means all quantum registers remain in the same state after extracting $\mathsf{tp}, \mathsf{iter}$. The same applies to extracting s in Line 32. Indeed, by the "if" condition in Line 31, Line 32 is executed by Bob only if $\mathsf{tp}^{(\mathsf{B},r)} = 1$. As $\mathsf{tp}^{(\mathsf{A},r-1)} = \mathsf{tp}^{(\mathsf{B},r)} = 1$, by the proof of Item 1 in Lemma 5.3, this further implies that Alice has executed the "then" branch starting from Line 15 and that W' is one of the qudits in $W^{(\mathsf{A},\mathsf{iter}^{(\mathsf{A},r-1)})}$ by the encoding in Line 18. As a result, W' must be in one of the basis state $|s\rangle$ and Bob can also extract s by measurement in the standard basis, without changing any quantum register.

Besides, also observe that whenever Lines 32 and 38 are executed by Bob, Item 3 in Lemma 5.3, together with $\mathsf{iter}^{(\mathsf{B},r)} = \mathsf{iter}^{(\mathsf{A},r-1)}$, ensures that $A^{(\mathsf{B},\mathsf{iter}^{(\mathsf{B},r)})}, W^{(\mathsf{B},\mathsf{iter}^{(\mathsf{B},r)})}$ have already been properly initialized in Line 25 (of a previous iteration).

In the second case, Alice's teleportation of A_{inp} in Line 17 only involves her EPR halves $Z^{(\mathsf{A})}$. Once Bob completes teleportation in Line 35 (of a later iteration) using his EPR halves $Z^{(\mathsf{B})}$, the state of B_{out} remains unchanged till the end of the protocol. This is because of Item 4 in Lemma 5.3, as well as the fact that no further measurement could change any quantum register, due to the above analysis of the first case.

Now, we are ready to show that in Line 13, Alice can indeed recover A_{inp} in the same state as input.

Lemma 5.4. *In every execution of Line 13, Alice always decodes A_{inp} to the same state as input.*

Proof. Note that Line 13 is executed by Alice only if $\mathsf{rst}^{(r-1)} = 1$. Consider Alice's execution starting from the most recent time when either of Lines 1 and 14 is executed (in the $(\mathsf{iter}^{(\mathsf{A},r-1)} - 1)$-th iteration). By Item 2 in Lemma 5.3, together with Line 16, $\mathsf{rst}^{(r-1)} = 1$ then implies that $W^{(\mathsf{A},\mathsf{iter}^{(\mathsf{A},r-1)})}$ is by the encoding in either Line 2 or Line 20 (but not Line 18), and thus is a codeword of $\mathsf{C}^{\mathsf{Q}}_{\mathsf{iter}^{(\mathsf{A},r-1)}}$. Recall that $\mathsf{C}^{\mathsf{Q}}_{\mathsf{iter}^{(\mathsf{A},r-1)}}$ produces $T_{\mathsf{iter}^{(\mathsf{A},r-1)}}$-qudit codewords and has erasure resilience $1/2 - \epsilon/10$. Up to the current r-th iteration, the first $2L \cdot (r - \mathsf{iter}^{(\mathsf{A},r-1)} + 1)$ qudits of $W^{(\mathsf{A},\mathsf{iter}^{(\mathsf{A},r-1)})}$ have been sent to Bob while Alice still holds the remaining qudits. Furthermore, it must be that $2L \cdot (r - \mathsf{iter}^{(\mathsf{A},r-1)} + 1) < (1/2 - \epsilon/10) \cdot T_{\mathsf{iter}^{(\mathsf{A},r-1)}}$, as otherwise there is a contradiction to $\mathsf{rst}^{(r-1)} = 1$, due to the "if" condition in Line 7. Consequently, by induction on all executions of Line 13, Alice can always decode A_{inp} to the same state as input. □

Intuitively, Alice can teleport A_{inp} once she learns that Bob has received enough EPR halves. Otherwise, either Bob has never received enough EPR halves, meaning that most of Alice's communication has been erased, or Alice has never learned that Bob already

[13]Recall that $\mathsf{var}^{(r-1)}$ represents the value of var at the end of the $(r-1)$-th iteration, or equivalently at the beginning of the r-th iteration. We remark that $\mathsf{tp}^{(\mathsf{B},r)} = \mathsf{tp}^{(\mathsf{A},r)}$ and $\mathsf{iter}^{(\mathsf{B},r)} = \mathsf{iter}^{(\mathsf{A},r)}$ do not necessarily hold here.

receives enough EPR halves, meaning that most of Bob's communication has been erased. In both cases, Alice should be able to commit to simply sending some fixed one-way quantum erasure code (and not resetting anymore) in the rest of the protocol. This is formalized by the following Lemma 5.5 (and Item 2 in Lemma 5.3).

Lemma 5.5. *It holds that*

$$\mathsf{rst}^{(2R)} = 0.$$

Proof. Note that $\mathsf{iter}^{(\mathsf{A},2R)}-1$ is the last iteration in which either of Lines 1 and 14 is executed by Alice. By Item 3 in Lemma 5.3, it must be that $\mathsf{iter}^{(\mathsf{A},2R)}-1 \leq R$. It further implies that $2L \cdot (2R - \mathsf{iter}^{(\mathsf{A},2R)} + 1) \geq 2LR = 1/2 \cdot 4LR \geq 1/2 \cdot T_{\mathsf{iter}^{(\mathsf{A},2R)}}$. The lemma statement then follows from the "if" condition in Line 7. □

Lemma 5.5 essentially means that Alice should eventually start to teleport or commit to sending some fixed one-way quantum erasure code. In other words, Bob always gets a chance to decode. Ideally, on the other hand, we do not want Bob to have more than one chance to decode. Otherwise, Bob may not be able to decide which decoding is the correct one to output. Indeed, Lemma 5.6 shows that Bob can never mistakenly decode from what Alice has sent before teleporting or committing to sending some fixed one-way quantum erasure code.

Lemma 5.6. *If Bob executes Line 40, then Line 8 is executed by Alice in the same iteration.*

Proof. If Line 40 is executed by Bob in the r-th iteration, then $W^{(\mathsf{B},\mathsf{iter}^{(\mathsf{B},r)})}$ has at least $(1/2+\epsilon/10) \cdot T_{\mathsf{iter}^{(\mathsf{B},r)}}$ non-erasure qudits by the "if" condition in Line 39. Since Alice sends to Bob via an erasure channel, it must be that $\mathsf{iter}^{(\mathsf{A},r-1)} = \mathsf{iter}^{(\mathsf{B},r)}$. The lemma statement thus follows from the "if" condition in Line 7. □

The remainder of the proof boils down to show that Bob can always successfully decode once having the unique chance, by analyzing erasures depending on the value of $\mathsf{tp}^{(\mathsf{A},2R)}$. As discussed before Lemma 5.4, the following Lemmas 5.7 and 5.8 are sufficient for proving Theorem 5.1 as the state of B_{out} remains unchanged till the end of the protocol once it is recovered by Bob.

Lemma 5.7. *If* $\mathsf{tp}^{(\mathsf{A},2R)} = 1$*, then* B_{out} *has the same state as input.*

Proof. Let $r_1 \in [R]$ be the unique iteration in which Alice executes Line 16. This is well-defined because of $\mathsf{tp}^{(\mathsf{A},2R)} = 1$, as well as Items 1 and 2 in Lemma 5.3. By the "if" condition in Line 15, Line 16 is executed by Alice only if $b^{(\mathsf{A},r_1)}$ has at least n bits "1". Since $b^{(\mathsf{B},r_1)}$ is encoded by a classical erasure code and sent via a classical erasure channel, it must be that $b^{(\mathsf{A},r_1)} = b^{(\mathsf{B},r_1)}$. By Item 5 in Lemma 5.3, as well as Line 29, Bob must have already received at least n EPR halves up to the r_1-th iteration.

Let $r_0 \in [r_1]$ be the first iteration in which Bob have already received at least n EPR halves, or equivalently $b^{(\mathsf{B},r_0)}$ has at least n bits "1". By definition of r_0, Bob has received

less than n EPR halves up to the (r_0-1)-th iteration, so all but at most n qudits sent by Alice in the first r_0-1 iterations are erased, implying at least $2L\cdot(r_0-1)-n$ erasures.

For every iteration r between r_0 and $\min(r_1-1,R)=r_1-1$, it must be that $\mathsf{rst}^{(r-1)}=1$ as otherwise by Item 2 in Lemma 5.3, Line 16 cannot be executed by Alice in the r_1-th iteration. Recall that C^{B} has erasure resilience $1-\epsilon/10$. This further implies that less than $\epsilon/10$ fraction of symbols sent by Bob are received by Alice, because Line 16 is not executed by Alice.

Suppose for the sake of contradiction that B_{out} is in a different state from input. By definition of r_1, as well as Item 1 in Lemma 5.3, Bob cannot execute Line 35 in the first r_1 iterations. Meanwhile, Bob has not yet executed Line 40 in the first r_1 iterations due to Lemma 5.6, as otherwise it would contradict the "if" condition in Line 12. Note that Lemma 5.4 ensures that the protocol always encodes the correct input A_{inp}. As $\mathsf{C}^{\mathsf{A}}_{r_1+1}$ has erasure resilience $1-\epsilon/10$, the adversary could stop teleportation only if it erases more than $1-\epsilon/10$ fraction of qudits sent by Alice from the (r_1+1)-th iteration onwards. Overall, the total number of erasures is at least

$$\begin{aligned}
&2L\cdot(r_0-1)-n+(1-\epsilon/10)\cdot L\cdot(r_1-r_0)+(1-\epsilon/10)\cdot 2L\cdot(2R-r_1)\\
&\quad\geq 2L\cdot(r_0-2)+(1-\epsilon/10)\cdot L\cdot(r_1-r_0)+(1-\epsilon/10)\cdot 2L\cdot(2R-r_1) && (\text{as } n\leq L)\\
&\quad\geq (1-\epsilon/10)\cdot L\cdot(r_1-2)+(1-\epsilon/10)\cdot 2L\cdot(2R-r_1)\\
&\quad= (1-\epsilon/10)\cdot L\cdot(4R-r_1-2)\\
&\quad\geq (1-\epsilon/10)\cdot L\cdot(3R-2) && (\text{as } r_1\leq R)\\
&\quad> (3/5-\epsilon)\cdot T,
\end{aligned}$$

a contradiction. □

Lemma 5.8. *If $\mathsf{tp}^{(\mathsf{A},2R)}=0$, then B_{out} has the same state as input.*

Proof. Let $r_0=\mathsf{iter}^{(\mathsf{A},2R)}$. By Item 3 in Lemma 5.3, it must be that $r_0\in[R+1]$. We claim that all but at most n qudits sent by Alice in the first r_0-1 iteraions are erased. Indeed, the case of $r_0=1$ is trivial. For $r_0>1$, it must be that Alice has executed Line 14 in the (r_0-1)-th iteration. By the "if" condition in Line 12, it further implies $b^{(\mathsf{A},r_0-1)}=b^{(\mathsf{B},r_0-1)}$. Due to $\mathsf{tp}^{(\mathsf{A},2R)}=0$, as well as Item 1 in Lemma 5.3, Bob must have received less than n EPR halves up to the (r_0-1)-th iteration, as claimed.

Let r_1 be the first iteration in which Alice executes Line 8. This is well-defined because of Lemma 5.5. Meanwhile, it must be that $r_0\leq r_1$ because of $\mathsf{rst}^{(r_0-1)}=1$, as well as Item 2 in Lemma 5.3. Furthermore, for every iteration between r_0 and $\min(r_1-1,R)$, it must be that $\mathsf{rst}^{(r)}=1$ by definition of r_1. Recall that C^{B} has erasure resilience $1-\epsilon/10$. This further implies that less than $\epsilon/10$ fraction of symbols sent by Bob are received by Alice, because Line 14 is not executed by Alice.

In addition, by the "if" condition in Line 7, it must be that

$$2L\cdot(r_1-r_0+1)\geq(1/2-\epsilon/10)\cdot T_{r_0}=(1/2-\epsilon/10)\cdot 2L\cdot(2R-r_0+1).$$

This implies that

$$r_1 \geq r_0 - 1 + (1/2 - \epsilon/10) \cdot (2R - r_0 + 1) \geq (1/2 - \epsilon/10) \cdot 2R = (1 - \epsilon/5) \cdot R. \tag{2}$$

Suppose for the sake of contradiction that B_{out} is in a different state from input. Due to $\mathsf{tp}^{(\mathsf{A},2R)} = 0$, as well as Item 1 in Lemma 5.3, Bob cannot execute Line 35. Meanwhile, Bob has not yet executed Line 40 in the first $r_1 - 1 \geq r_0 - 1$ iterations due to Lemma 5.6, as otherwise it would contradict the definition of r_1. Note that Lemma 5.4 ensures that the protocol always encodes the correct input A_{inp}. As $\mathsf{C}^{\mathsf{Q}}_{r_0}$ is a quantum erasure code with resilience $1/2 - \epsilon/10$, the adversary could stop decoding only if it erases more than $1/2 - \epsilon/10$ fraction of qudits sent by Alice from the r_0-th iteration onwards. Overall, the total number of erasures is at least

$$\begin{aligned}
&2L \cdot (r_0 - 1) - n + (1 - \epsilon/10) \cdot L \cdot (\min(r_1, R+1) - r_0) + (1/2 - \epsilon/10) \cdot 2L \cdot (2R - r_0 + 1) \\
&\quad \geq 2L \cdot (r_0 - 2) + (1 - \epsilon/10) \cdot L \cdot (\min(r_1, R+1) - r_0) + (1 - \epsilon/5) \cdot L \cdot (2R - r_0 + 1) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{as } n \leq L) \\
&\quad \geq (1 - \epsilon/10) \cdot L \cdot (\min(r_1, R+1) - 2) + (1 - \epsilon/5) \cdot L \cdot (2R - 1) \\
&\quad \geq (1 - \epsilon/10) \cdot L \cdot ((1 - \epsilon/5) \cdot R - 2) + (1 - \epsilon/5) \cdot L \cdot (2R - 1) \qquad (\text{by Equation (2)}) \\
&\quad > (3/5 - \epsilon) \cdot T,
\end{aligned}$$

a contradiction. □

6 Two-Way Code for the Quantum-Quantum Channel

We now turn to the case when Bob can send quantum messages to Alice throughout the protocol. In terms of the notation in Section 3.1, this corresponds to the case when the classicality parameter $\tau = 0$.

Theorem 6.1. *For all $\epsilon > 0$, there exists a two-way code for the quantum–quantum channel with resilience $(2/3 - \epsilon)$ over an alphabet of size $q = O_\epsilon(1)$, constant rate $\Omega_\epsilon(1)$, and runs in polynomial time.*

To prove Theorem 6.1, we consider the protocol described in Algorithms 3 and 4. Let $n > 0$ be the length (in qubits) of Alice's input and let $\epsilon > 0$ be a parameter. Define $R = \epsilon/200$ and let K'_{C} and C^{A} be the alphabet size and the code promised by Lemma 3.2 for inputs of at most[14] $100n \cdot \log(1/\epsilon)$ bits, which can be equivalently viewed as $100n$ symbols over an alphabet of size $K_{\mathsf{C}} = \max(K'_{\mathsf{C}}, 1/\epsilon)$, with rate $50R$ and distance $1 - \epsilon/2$. Similarly, let K_{Q} and C^{Q} be the alphabet size and the code promised by Lemma 3.3 for inputs of length n with rate $R/2$ and distance $1/2 - \epsilon/2$. Let D^{A} and D^{Q} be the decoding functions corresponding to C^{A} and C^{Q} respectively.

[14] We can assume that C^{A} encodes shorter inputs by a standard padding trick.

We describe a protocol of length $T = \frac{3n}{R}$, classicality parameter $\tau = 0$, and using an alphabet of size $q = 2 \cdot \max(K_{\mathsf{Q}}, K_{\mathsf{C}})$. Our protocol is described in Algorithms 3 and 4.

Algorithm 3 Alice's side of the protocol. She starts with an input register A_{inp}.

Phase 1: *Receiving entanglements from Bob.*

Listen for $T/3$ rounds. Let $\tilde{M}_1, \ldots, \tilde{M}_{T/3}$ be the received message registers.

Let $\mathcal{E} \subseteq [T/3]$ be the subset of messages erased by the adversary.

Phase 2: *Sending input to Bob.*

if $|\mathcal{E}| \leq \frac{T}{3} \cdot (1 - \epsilon)$ **then**

  Let $J \subseteq [T/3] \setminus \mathcal{E}$ be of size $\frac{n}{\log q}$. View $\tilde{M}_J$ as n halves of EPR pairs.

  Do Bell measurements on A_{inp} and $\tilde{M}_J$, to get teleportation outcomes $\sigma \in \{0,1\}^{2n}$.

  Encode (σ, J) using C^{A} and obtain $C_{T/3+1}, \ldots, C_T \in [q/2]$.

  For all $t \in (T/3, T]$, send $|0\rangle \otimes |C_t\rangle$ in round t.

else

  Apply the encoding map C^{Q} to A_{inp}, obtaining output registers $\mathsf{C}_{T/3+1}, \ldots, \mathsf{C}_T$.

  For all $t \in (T/3, T]$, prepare a register F_t in state $|1\rangle$ and send $\mathsf{F}_t \otimes \mathsf{C}_t$ in round t.

Algorithm 4 Bob's side of the protocol.

Phase 1: *Sending entanglements to Alice.*

For all $t \in [T/3]$, independently prepare a qudit pair in the state $|M_t N_t\rangle = \frac{1}{\sqrt{q}} \sum_{i \in [q]} |ii\rangle$.

For all $t \in [T/3]$, send M_t to Alice in round t.

Phase 2: *Receiving Alice's input.*

Listen for $2T/3$ rounds. Let $\tilde{M}_t = \tilde{\mathsf{F}}_t \otimes \tilde{\mathsf{C}}_t$ be the register received in round $t \in (T/3, T]$.

if $\exists t \in (T/3, T]$ such that $\tilde{\mathsf{F}}_t$ is in state $|0\rangle$ **then**

  For $t \in (T/3, T]$, measure $\tilde{\mathsf{C}}_t$ in the standard basis to get $\tilde{C}_t \in [q/2]$.

  Define $\left(\tilde{\sigma}, \tilde{J}\right) = \mathsf{D}^{\mathsf{A}}\left(\tilde{C}_{T/3+1}, \ldots, \tilde{C}_T\right)$.

  View $N_{\tilde{J}}$ as n halves of EPR pairs and $\tilde{\sigma}$ as the teleportation outcomes. Apply the corresponding Pauli correction and move the output to B_{out}.

else

  Apply the decoding map D^{Q} to $\tilde{C}_{T/3+1}, \ldots, \tilde{C}_T$ and denote the output register B_{out}.

Note from Line 47 that J is a subset of $[T/3]$ of size $\frac{n}{\log q}$. Using the standard upper bound on binomial coefficients that says that $\binom{n}{k} \leq \left(\frac{3n}{k}\right)^k$ for all $0 < k \leq n$, we get that the number of different subsets J is at most $\left(\frac{3 \log q}{R}\right)^{\frac{n}{\log q}} \leq \left(\frac{10}{R}\right)^n = \left(\frac{2000}{\epsilon}\right)^n$. Thus, such a set J can be represented using $n \cdot \log\left(\frac{2000}{\epsilon}\right) \leq 50n \cdot \log(1/\epsilon)$ bits. As the domain of C^{A} is large enough, Line 49 is well defined.

6.1 Analysis

We now show that the protocol defined above solves the message transfer task with resilience $\frac{2}{3} - \epsilon$. For this, fix an arbitrary reference register R, and assume that the protocol starts in the (pure) input state $|\psi\rangle_{A_{\mathsf{inp}}R}$. Fix any adversary $\mathsf{Adv} \subseteq [T]$ such that $|\mathsf{Adv}| \leq \left\lceil \left(\frac{2}{3} - \epsilon\right) \cdot T \right\rceil$. We divide the proof into two cases based on the size of $\mathsf{Adv} \cap [T/3]$. Note that Alice knows this set as this is exactly the set $\mathcal{E}$ computed in Line 45

When $|\mathcal{E}| \leq \frac{T}{3} \cdot (1 - \epsilon)$. In this case, the if statement in Line 46 evaluates to true and Alice executes Lines 47 to 50. In Line 47, by definition of J, we get that the reduced state on $\tilde{M}_J N_J$ is n independent EPR pairs, where the registers $\tilde{M}_J$ are held by Alice and the registers N_J are held by Bob (who does not know J). In Line 48, Alice teleports A_{inp} using her side of the EPR pairs to get a teleportation string $\sigma \in \{0,1\}^{2n}$.

Alice then executes Line 49, where she applies the encoding map C^{A} to encode the pair (σ, J). She sends the registers obtained by the encoding to Bob (after tensoring with $|0\rangle$) in Line 50. Some of these registers maybe erased by the adversary but the fact that $|\mathsf{Adv}| \leq \left\lceil \left(\frac{2}{3} - \epsilon\right) \cdot T \right\rceil$ implies that Bob receives at least ϵT of these registers. Let the indices for these registers be $S \subseteq (T/3, T]$. As Alice tensored her registers with the state $|0\rangle$, Bob will evaluate the if in Line 57 as true and execute Lines 58 to 60. While executing Line 59, we have by Lemma 3.2 that Bob sets $\left(\tilde{\sigma}, \tilde{J}\right) = (\sigma, J)$. This means that when he applies the Pauli correction corresponding to $\tilde{\sigma}$ on $N_{\tilde{J}}$ in Line 60, the reduced state on $B_{\mathsf{out}}R$ will be $|\psi\rangle_{B_{\mathsf{out}}R}$, as desired.

When $|\mathcal{E}| > \frac{T}{3} \cdot (1 - \epsilon)$. In this case, the if statement in Line 46 evaluates to false and Alice executes Line 52, where she applies the encoding map C^{Q} to A_{inp} and obtains output registers $\mathsf{C}_{T/3+1}, \ldots, \mathsf{C}_T$. These registers are (tensored with registers in $|1\rangle$ and) sent to Bob in Line 53 where some of these may be erased by the adversary. Note that $|\mathsf{Adv}| \leq \left\lceil \left(\frac{2}{3} - \epsilon\right) \cdot T \right\rceil$ implies that $|\mathsf{Adv} \cap (T/3, T]| \leq \left(\frac{1}{3} - \frac{\epsilon}{2}\right) \cdot T$. Thus, the number of registers erased by the adversary is at most $\left(\frac{1}{3} - \frac{\epsilon}{2}\right) \cdot T$.

Equivalently, Bob receives at least $\left(\frac{1}{3} + \frac{\epsilon}{2}\right) \cdot T$ of the registers sent by Alice. Let the indices for these registers be $S \subseteq (T/3, T]$. As Alice tensored her registers with the state $|1\rangle$, Bob will evaluate the if in Line 57 as false and execute Line 62. While executing Line 62, he has the registers C_S. By Lemma 3.3, we get that after Line 62, the reduced state on $B_{\mathsf{out}}R$ will be $|\psi\rangle_{B_{\mathsf{out}}R}$, as desired.

7 Optimally Resilient Quantum Interactive Coding

We now show an interactive coding scheme when both Alice and Bob can send qubits.

Theorem 7.1. *Let $\epsilon > 0$ be small enough that Π be a protocol of length T and alphabet q. The protocol Π' defined in Algorithms 5 and 6 has length $T' \leq \frac{40T \cdot \log q}{\epsilon}$ and alphabet 5 and*

is such that for every adversary Adv' *for* Π' *satisfying* $|\mathsf{Adv}'| \leq \left\lceil \left(\frac{1}{2} - \epsilon\right) T' \right\rceil$*, the protocol* Π' *simulates* Π *in the presence of* Adv'*.*

To prove Theorem 7.1, we consider the protocol described in Algorithms 5 and 6. Let $\epsilon > 0$ be a (small enough) parameter and let Π be a noiseless protocol of length T. We assume without loss of generality that T is even, the protocol Π has a binary alphabet and is alternating starting from Bob[15] and for convenience, pad the protocol by having the parties send $|0\rangle$ alternately after the protocol finishes. We describe a protocol Π' of length $T' = \frac{20T}{\epsilon}$, classicality parameter $\tau = 0$, and using an alphabet of size $q = 5$. Our protocol is described in Algorithms 5 and 6.

7.1 Analysis

We now analyze the protocols in Algorithms 5 and 6 and show that they satisfy Theorem 7.1. For this, we fix an arbitrary Adv' for Π' satisfying $|\mathsf{Adv}'| \leq \left\lceil \left(\frac{1}{2} - \epsilon\right) T' \right\rceil$, fix any inputs of Alice and Bob and any reference register R, and show that the output state produced by an execution of Π' in the presence of Adv' is identical to the output state produced by a noiseless execution of Π.

Note that in addition to Adv' and the parties' inputs, the values of the variables in our protocol also depend on the measurement outcomes. Throughout the proof, we will condition on a sequence of arbitrary outcomes for these measurement and show that Theorem 7.1 holds even under this conditioning. Together with the adversary, fixing the outcomes in these measurements means that the values of all variables throughout the execution of our protocol is fixed.

Notation. We start by defining some notation. For a variable *var* in Algorithms 5 and 6 and an iteration $t' \in [T'/2]$, we let $var_{t'}^{\mathsf{A}}$ denote Alice's value of the variable *var* at the end of iteration t' of the loop in Line 65. We omit the subscript t' when $t' = T'/2$ and use $t' = 0$ to denote Alice's value before the loop starts. The notation $var_{t'}^{\mathsf{B}}$ is defined analogously.

The analysis is roughly divided into two parts. First, we analyze the properties of Algorithms 5 and 6 that hold regardless of the number of erasures. These highlight the structure of Algorithms 5 and 6. Then, we use the fact that $|\mathsf{Adv}'| \leq \left\lceil \left(\frac{1}{2} - \epsilon\right) T' \right\rceil$ to finish the proof.

7.2 The Structure of Algorithms 5 and 6

Note from Lines 63 and 94 that Alice and Bob initialize $\mathsf{A\text{-}cnt}$ to 1 and $\mathsf{B\text{-}cnt}$ to 0. Moreover, Alice only ever changes $\mathsf{A\text{-}cnt}$ in Lines 88 and 92 where she may increment it by 2. In addition, at most one of Lines 88 and 92 can be executed in any iteration. This means that her value for $\mathsf{A\text{-}cnt}$ is always odd, only increases, and increases by at most 2 in any iteration. Analogous statements hold from Lines 110 and 114 for Bob's value of $\mathsf{B\text{-}cnt}$. Formally,

[15] That is, Alice transmits qubits to Bob in even rounds and Bob transmits qubits to Alice in odd rounds.

Algorithm 5 Alice's side of the protocol. She starts with registers $A = (A_{\mathsf{inp}}, A_{\mathsf{anc}}, A_{\mathsf{out}})$, message registers $M_2, M_4, \ldots, M_T$ and instruments as in Equation (1).

Set counters $\mathsf{A\text{-}cnt} \leftarrow 1, \mathsf{B\text{-}cnt} \leftarrow 0$, bits $\sigma_0, \sigma_1, \tilde{\sigma}_0, \tilde{\sigma}_1 \leftarrow 0$, and set $\mathsf{LastOk} \leftarrow \mathtt{True}$.
Prepare a register Q in state $|0\rangle$.
for $t' \in [T'/2]$ **do**
    if $\mathsf{A\text{-}cnt} \equiv 0 \pmod 3$ **then**
        Prepare a register F_1 in the state $|0\rangle$.
        if $\mathsf{A\text{-}cnt} \equiv 3 \pmod{30}$ **then**
            If LastOk, prepare registers $|Q\mathsf{F}_2\rangle$ in state $|\Phi^+\rangle$. Else, prepare F_2 in state $|\mathsf{E}\rangle$.
        else
            Prepare a register F_2 in the state $|\sigma_{\mathbb{1}(\mathsf{A\text{-}cnt} \bmod 30 = 27)}\rangle$.
    else
        Prepare registers $\mathsf{F}_1\mathsf{F}_2$ in the state $|1\rangle\,|(\mathsf{A\text{-}cnt} \bmod 3) - 1\rangle$.
    Send registers $M'_{2t'-1} = \mathsf{F}_1\mathsf{F}_2$ to Bob.
    Listen to Bob to get register $\tilde{M}'_{2t'} = \tilde{\mathsf{F}}_1\tilde{\mathsf{F}}_2$.
    Set $\mathsf{LastOk} \leftarrow \mathtt{True}$ if and only if $\tilde{M}'_{2t'}$ is not erased.
    if LastOk **then**
        Measure $\tilde{\mathsf{F}}_1$ in the standard basis and obtain outcome f_1.
        if $f_1 = 0$ **then**
            Set $\mathsf{LastE} \leftarrow \mathtt{True}$ if and only if $\tilde{\mathsf{F}}_2$ is in state $|\mathsf{E}\rangle$.
            Set $\mathsf{B\text{-}cnt}$ so that $|\mathsf{A\text{-}cnt} - \mathsf{B\text{-}cnt}| \leq 1$ and $\mathsf{B\text{-}cnt} \equiv 0 \pmod 3$.
            if $\mathsf{B\text{-}cnt} \equiv 18 \pmod{30}$ **and not** LastE **then**
                Discard Q and relabel $\tilde{\mathsf{F}}_2$ as Q. Use Alice's instrument in Π for round $\lceil \frac{\mathsf{B\text{-}cnt}}{15} \rceil$ and the outcomes so far to get its outcome and message $M_{\lceil \frac{\mathsf{B\text{-}cnt}}{15} \rceil}$. Do Bell measurements on Q and $M_{\lceil \frac{\mathsf{B\text{-}cnt}}{15} \rceil}$ to get teleportation bits σ_0, σ_1.
            else if $\mathsf{B\text{-}cnt} \equiv 6 \pmod{30}$ **and** $\mathsf{B\text{-}cnt} > \mathsf{A\text{-}cnt}$ **then**
                Measure F_2 in the standard basis to obtain outcome $\tilde{\sigma}_0$.
            else if $\mathsf{B\text{-}cnt} \equiv 12 \pmod{30}$ **and** $\mathsf{B\text{-}cnt} > \mathsf{A\text{-}cnt}$ **then**
                Measure F_2 in the standard basis to obtain outcome $\tilde{\sigma}_1$. Apply the Pauli correction corresponding to $(\tilde{\sigma}_0, \tilde{\sigma}_1)$ on Q and move the output to $\tilde{M}_{\lceil \frac{\mathsf{B\text{-}cnt}}{15} \rceil}$.
            If not LastE and $\mathsf{B\text{-}cnt} > \mathsf{A\text{-}cnt}$, set $\mathsf{A\text{-}cnt} \leftarrow \mathsf{A\text{-}cnt} + 2$.
        else
            Measure $\tilde{\mathsf{F}}_2$ in the standard basis and obtain outcome f_2.
            Set $\mathsf{B\text{-}cnt}$ so that $|\mathsf{A\text{-}cnt} - \mathsf{B\text{-}cnt}| \leq 1$ and $\mathsf{B\text{-}cnt} \equiv f_2 + 1 \pmod 3$.
            If $\mathsf{B\text{-}cnt} > \mathsf{A\text{-}cnt}$, set $\mathsf{A\text{-}cnt} \leftarrow \mathsf{A\text{-}cnt} + 2$.
Use Alice's output instrument in Π for the outcomes so far to compute the output.

Algorithm 6 Bob's side of the protocol. He starts with registers $B = (B_{\mathsf{inp}}, B_{\mathsf{anc}}, B_{\mathsf{out}})$, message registers $M_1, M_3, \ldots, M_{T-1}$, and instruments as in Equation (1).

Set counters $\mathsf{A\text{-}cnt} \leftarrow 1, \mathsf{B\text{-}cnt} \leftarrow 0$, bits $\sigma_0, \sigma_1, \tilde{\sigma}_0, \tilde{\sigma}_1 \leftarrow 0$, and set $\mathsf{LastOk} \leftarrow \texttt{True}$.
Prepare a register Q in state $|0\rangle$.
for $t' \in [T'/2]$ **do**
    Listen to Alice to get register $\tilde{M}'_{2t'-1} = \tilde{\mathsf{F}}_1\tilde{\mathsf{F}}_2$.
    Set $\mathsf{LastOk} \leftarrow \texttt{True}$ if and only if $\tilde{M}'_{2t'-1}$ is not erased.
    if LastOk **then**
        Measure $\tilde{\mathsf{F}}_1$ in the standard basis and obtain outcome f_1.
        if $f_1 = 0$ **then**
            Set $\mathsf{LastE} \leftarrow \texttt{True}$ if and only if $\tilde{\mathsf{F}}_2$ is in state $|\mathsf{E}\rangle$.
            Set $\mathsf{A\text{-}cnt}$ so that $|\mathsf{A\text{-}cnt} - \mathsf{B\text{-}cnt}| \leq 1$ and $\mathsf{A\text{-}cnt} \equiv 0 \pmod 3$.
            if $\mathsf{A\text{-}cnt} \equiv 3 \pmod{30}$ **and not** LastE **then**
                Discard Q and relabel $\tilde{\mathsf{F}}_2$ as Q. Use Bob's instrument in Π for round $\lceil \frac{\mathsf{A\text{-}cnt}}{15} \rceil$ and the outcomes so far to get its outcome and message $M_{\lceil \frac{\mathsf{A\text{-}cnt}}{15} \rceil}$. Do Bell measurements on Q and $M_{\lceil \frac{\mathsf{A\text{-}cnt}}{15} \rceil}$ to get teleportation bits σ_0, σ_1.
            else if $\mathsf{A\text{-}cnt} \equiv 21 \pmod{30}$ **and** $\mathsf{A\text{-}cnt} > \mathsf{B\text{-}cnt}$ **then**
                Measure F_2 in the standard basis to obtain outcome $\tilde{\sigma}_0$.
            else if $\mathsf{A\text{-}cnt} \equiv 27 \pmod{30}$ **and** $\mathsf{A\text{-}cnt} > \mathsf{B\text{-}cnt}$ **then**
                Measure F_2 in the standard basis to obtain outcome $\tilde{\sigma}_1$. Apply the Pauli correction corresponding to $(\tilde{\sigma}_0, \tilde{\sigma}_1)$ on Q and move the output to $\tilde{M}_{\lceil \frac{\mathsf{A\text{-}cnt}}{15} \rceil}$.
            If not LastE and $\mathsf{A\text{-}cnt} > \mathsf{B\text{-}cnt}$, set $\mathsf{B\text{-}cnt} \leftarrow \mathsf{B\text{-}cnt} + 2$.
        else
            Measure $\tilde{\mathsf{F}}_2$ in the standard basis and obtain outcome f_2.
            Set $\mathsf{A\text{-}cnt}$ so that $|\mathsf{A\text{-}cnt} - \mathsf{B\text{-}cnt}| \leq 1$ and $\mathsf{A\text{-}cnt} \equiv f_2 + 1 \pmod 3$.
            If $\mathsf{A\text{-}cnt} > \mathsf{B\text{-}cnt}$, set $\mathsf{B\text{-}cnt} \leftarrow \mathsf{B\text{-}cnt} + 2$.
    if $\mathsf{B\text{-}cnt} \equiv 0 \pmod 3$ **then**
        Prepare a register F_1 in the state $|0\rangle$.
        if $\mathsf{B\text{-}cnt} \equiv 18 \pmod{30}$ **then**
            If LastOk, prepare registers $|\mathsf{F}_2 Q\rangle$ in state $|\Phi^+\rangle$. Else, prepare F_2 in state $|\mathsf{E}\rangle$.
        else
            Prepare a register F_2 in the state $|\sigma_{\mathbb{1}(\mathsf{B\text{-}cnt} \bmod 30 = 12)}\rangle$.
    else
        Prepare registers $\mathsf{F}_1\mathsf{F}_2$ in the state $|1\rangle\,|(\mathsf{B\text{-}cnt} \bmod 3) - 1\rangle$.
    Send registers $M'_{2t'} = \mathsf{F}_1\mathsf{F}_2$ to Alice.
Use Bob's output instrument in Π for the outcomes so far to compute the output.

Proposition 7.2. *We have* $\mathsf{A\text{-}cnt}_0^{\mathsf{A}} = 1$ *and for all* $t' \in [T'/2]$*, we have* $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{A}} \in \left\{\mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}}, \mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}} + 2\right\}$*. Similarly, we have* $\mathsf{B\text{-}cnt}_0^{\mathsf{B}} = 0$ *and for all* $t' \in [T'/2]$*, we have* $\mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}} \in \left\{\mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}}, \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}} + 2\right\}$*. It follows that for all* $t' \in [0, T'/2]$*, we have* $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{A}} + 1 \equiv \mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}} \equiv 0 \pmod 2$.

Lemma 7.3. *The following hold for all* $t' \in [0, T'/2]$*:*

1. *We have:*

$$\left|\mathsf{A\text{-}cnt}_{t'}^{\mathsf{A}} - \mathsf{B\text{-}cnt}_{t'}^{\mathsf{A}}\right| = 1,$$
$$\left|\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}} - \mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}}\right| = 1,$$
$$\left|\mathsf{A\text{-}cnt}_{t'}^{\mathsf{A}} - \mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}}\right| = 1.$$

2. *If* $t' > 0$*, we have:*

$$\left|\mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}} - \mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}}\right| = 1.$$

3. *If* $\mathsf{LastOk}_{t'}^{\mathsf{A}} = \texttt{True}$*, we have* $\mathsf{B\text{-}cnt}_{t'}^{\mathsf{A}} = \mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}}$.

4. *If* $t' > 0$ *and* $\mathsf{LastOk}_{t'}^{\mathsf{B}} = \texttt{True}$*, we have* $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}} = \mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}}$.

Proof. Proof by induction on t'. The base case $t' = 0$ is by Lines 63 and 94. We show the result for $t' > 0$ assuming it holds for $t' - 1$.

We first show Item 4. Assume that $\mathsf{LastOk}_{t'}^{\mathsf{B}} = \texttt{True}$. From Line 98, this means that Bob received Alice's message correctly in iteration t' and the if statement in Line 99 evaluates to true. Thus, he measures the register F_1 sent by Alice in iteration t' in Line 100 to get outcome $f_{1,t'}^{\mathsf{B}}$. Notice from Lines 67 and 73 that this register is a classical register. Thus, we have from Line 66 that $f_{1,t'}^{\mathsf{B}} = 0$ if and only if $\mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}} \equiv 0 \pmod 3$. Using this, we divide the proof in two cases:

- **When** $f_{1,t'}^{\mathsf{B}} = 0$ **and** $\mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}} \equiv 0 \pmod 3$**:** In this case, Bob sets $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}}$ in Line 103 to be the unique value cnt satisfying $\left|\mathsf{cnt} - \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}}\right| \leq 1$ and $\mathsf{cnt} \equiv 0 \pmod 3$. As the induction hypothesis implies that $\mathsf{cnt} = \mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}}$ is one such value, we have $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}} = \mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}}$, as desired.

- **When** $f_{1,t'}^{\mathsf{B}} = 1$ **and** $\mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}} \not\equiv 0 \pmod 3$**:** In this case, note from Line 73 that the register F_2 sent by Alice in iteration t' is also classical. Thus, we have from Lines 73 and 112 that $f_{2,t'}^{\mathsf{B}} = \left(\mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}} \bmod 3\right) - 1$. As Bob sets $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}}$ in Line 113 to be the unique value cnt satisfying $\left|\mathsf{cnt} - \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}}\right| \leq 1$ and $\mathsf{cnt} \equiv f_{2,t'}^{\mathsf{B}} + 1 \pmod 3$ and as the induction hypothesis implies that $\mathsf{cnt} = \mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}}$ is one such value, we have $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}} = \mathsf{A\text{-}cnt}_{t'-1}^{\mathsf{A}}$, as desired.

Next, we show Item 2. We have from Proposition 7.2 that $\mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}} \in \left\{\mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}}, \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}} + 2\right\}$. If $\mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}} = \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}}$, the result follows from the induction hypothesis, so we assume that $\mathsf{B\text{-}cnt}_{t'}^{\mathsf{B}} = \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}} + 2$. This means that Bob incremented in one of Lines 110 and 114 in iteration t' implying that $\mathsf{LastOk}_{t'}^{\mathsf{B}} = \texttt{True}$ and $\mathsf{A\text{-}cnt}_{t'}^{\mathsf{B}} > \mathsf{B\text{-}cnt}_{t'-1}^{\mathsf{B}}$. Combining with Item 4, we

get that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} > \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}$. The induction hypothesis implies that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}+1$ and the result follows.

We now show Item 3. The proof is similar to the proof of Item 4 above. Assume that $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{True}$. From Line 76, this means that Alice received Bob's message correctly in iteration t' and the if statement in Line 77 evaluates to true. Thus, she measures the register F_1 sent by Bob in iteration t' in Line 78 to get outcome $f^{\mathsf{A}}_{1,t'}$. Notice from Lines 116 and 122 that this register is a classical register. Thus, we have from Line 115 that $f^{\mathsf{A}}_{1,t'} = 0$ if and only if $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} \equiv 0 \pmod 3$. Using this, we divide the proof in two cases:

- **When $f^{\mathsf{A}}_{1,t'} = 0$ and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} \equiv 0 \pmod 3$:** In this case, Alice sets $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'}$ in Line 81 to be the unique value cnt satisfying $\left|\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} - \mathsf{cnt}\right| \leq 1$ and $\mathsf{cnt} \equiv 0 \pmod 3$. By Item 2, we have that $\mathsf{cnt} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$ is one such value, implying that $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$, as desired.

- **When $f^{\mathsf{A}}_{1,t'} = 1$ and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} \not\equiv 0 \pmod 3$:** In this case, note from Line 122 that the register F_2 sent by Bob in iteration t' is also classical. Thus, we have from Lines 90 and 122 that $f^{\mathsf{A}}_{2,t'} = \left(\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} \bmod 3\right) - 1$. As Alice sets $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'}$ in Line 91 to be the unique value cnt satisfying $\left|\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} - \mathsf{cnt}\right| \leq 1$ and $\mathsf{cnt} \equiv f^{\mathsf{A}}_{2,t'} + 1 \pmod 3$ and as Item 2 implies that $\mathsf{cnt} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$ is one such value, we have $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$, as desired.

We now prove Item 1, starting with the third equation. By the induction hypothesis, we have that $\left|\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} - \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}\right| = 1$. Using Proposition 7.2, the result follows unless the larger of these two is incremented by 2 and the smaller one stays unchanged. Assume first that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}$ is larger and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}$. In this case, we have that Alice incremented in one of Lines 88 and 92 in iteration t' which can only happen if $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'} > \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}$ and $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{True}$. These combined with Item 3 contradict that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}$ is larger, and we are done. In the other case when $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}$ is unchanged, we are done by Item 2.

For the first equation, note that if $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{False}$, the if in Line 76 evaluates to false and Alice does not update either counter in iteration t'. The result follows by the induction hypothesis. On the other hand, if $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{True}$, the result follows from the third equation and Item 3. Finally, for the second equation, note that if $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$, the if in Line 98 evaluates to false and Bob does not update either counter in iteration t'. The result follows by the induction hypothesis. On the other hand, if $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{True}$, the result follows from Items 2 and 4. □

Lemma 7.4. *Let $t' \in [T'/2]$.*

1. *If Alice executes Line 83 in iteration t', then Bob executes Line 118 in iteration t' and $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{True}$.*

2. *If Bob executes Line 105 in iteration t', then Alice executes Line 69 in iteration t' and $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{True}$.*

Proof. The proof for both Items 1 and 2 is similar. Let $t' \in [T'/2]$ be such that Alice executes Line 83 in iteration t'. Then, the if statements in Lines 77 and 82 must have evaluated to true in iteration t'. This means that $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{True}$ and $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'} \equiv 18 \pmod{30}$ and $\mathsf{LastE}^{\mathsf{A}}_{t'} = \texttt{False}$. From $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{True}$, we get that Bob's message to Alice was not erased in iteration t' and using Item 3 of Lemma 7.3, also get that $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} \equiv 18 \pmod{30}$. This means that Bob executes Line 118 in iteration t' proving the first part of the result. For the second part, if $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$, we have from Lines 80 and 118 that $\mathsf{LastE}^{\mathsf{A}}_{t'} = \texttt{True}$, a contradiction.

For Item 2, let $t' \in [T'/2]$ be such that Bob executes Line 105 in iteration t'. Then, the if statements in Lines 99 and 104 must have evaluated to true in iteration t'. This means that $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{True}$ and $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t'} \equiv 3 \pmod{30}$ and $\mathsf{LastE}^{\mathsf{B}}_{t'} = \texttt{False}$. From $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{True}$, we get that Alice's message to Bob was not erased in iteration t' and using Item 4 of Lemma 7.3, also get that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} \equiv 3 \pmod{30}$. This means that Alice executes Line 69 in iteration t' proving the first part of the result. For the second part, if $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False}$, we have from Lines 69 and 102 that $\mathsf{LastE}^{\mathsf{B}}_{t'} = \texttt{True}$, a contradiction. □

Lemma 7.5. *Let $t \geq 0$ and $t' \in [0, T'/2]$.*

1. *If t is odd and $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} = 15t$, then by the end of iteration t', Alice and Bob have successfully simulated[16] t rounds of Π.*

2. *If t is even and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} = 15t$, then by the end of iteration t', Alice and Bob have successfully simulated t rounds of Π.*

Proof. Note that the parties modify the registers of the original protocol Π only in Lines 83, 87, 105 and 109. We call the lines the "relevant" lines in this proof. Also, note that without loss of generality, for any $t \geq 0$, we can consider the smallest t' satisfying the condition. Indeed, for all larger t', we have from Item 1 of Lemma 7.3 that the parties do not execute the relevant lines and if the lemma holds for the smaller t', it will also hold for the larger t'.

The rest of the proof by induction on t. The base case $t = 0$ implies $t' = 0$ and is trivial. We show the result for $t > 0$ assuming it holds for $t - 1$. As the proof for the other case is analogous, assume that t is even. Let t'_0 be such that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'_0} = 15(t-1)$. By Item 1 of Lemma 7.3, we have that $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'_0} \in \{15t - 16, 15t - 14\}$. Similarly, Item 1 of Lemma 7.3 combined with the fact that $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} = 15t$ means that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} \in \{15t - 1, 15t + 1\}$. Using Proposition 7.2, we get that there exist iterations $t'_1 < t'_2 < t'_3 \in (t'_0, t')$ such that:

$$\begin{aligned} \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'_1-1} &= 15t - 13, & \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'_1} &= 15t - 11, \\ \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'_2-1} &= 15t - 10, & \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'_2} &= 15t - 8, \\ \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'_3-1} &= 15t - 4, & \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'_3} &= 15t - 2. \end{aligned} \tag{3}$$

[16] That is, the state of Alice's and Bob's local registers A, B and the message registers exchanged is identical to their state after t rounds of a noiseless execution of Π.

We first claim that the parties do not execute the relevant lines in iterations $t'' \in [t'_0, t'_1)$. Indeed, for all such t'', we have that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t''} \in \{15t-15, 15t-13\}$. Using Item 1 of Lemma 7.3, we get that the only relevant line Bob can execute is Line 83 and that too only if $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t''-1} = 15t-13$. However, if Alice executes Line 83 in iteration t'', we have from Line 82 that $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t''} \equiv 18 \pmod{30}$ and $\mathsf{LastE}^{\mathsf{A}}_{t''} = \texttt{False}$. As $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t''} \in \{15t-15, 15t-13\}$, we get that Alice also executes Line 88 in iteration t'' and increments $\mathsf{A\text{-}cnt}$, contradicting the fact that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t''} \in \{15t-15, 15t-13\}$.

Due to this claim and the induction hypothesis, we get that before iteration t'_1, the Alice and Bob have successfully simulated $t-1$ rounds of Π. In iteration t'_1, we have from Equation (3) that Alice increments in one of Lines 88 and 92 in iteration t'_1. However, she cannot increment in Line 92 as that would mean $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'_1} = 15t-12$ which is impossible from Line 91. Thus, she increments in Line 88. Using this and Line 81, conclude that $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'_1} = 15t-12$ implying that Alice executes Line 83 in iteration t'_1. From Item 1 of Lemma 7.5, conclude that then Bob executes Line 118 in iteration t'_1 and $\mathsf{LastOk}^{\mathsf{B}}_{t'_1} = \texttt{True}$. Using this, observe that the bits $\sigma^{\mathsf{A}}_{0,t'_1}, \sigma^{\mathsf{A}}_{1,t'_1}$ Alice obtains by teleportation in Line 83 would give Bob the right message if he uses the corresponding Pauli correction on $Q^{\mathsf{B}}_{t'_1}$. In the rest of this proof, we show that this is indeed the case.

For this, we first claim that there does not exist $t'' \in (t'_1, t']$ such that Bob executes Line 118 in iteration t'' and $\mathsf{LastOk}^{\mathsf{B}}_{t''} = \texttt{True}$. We prove this by contradiction. If there exists such a t'', we have from Line 117 and Item 4 of Lemma 7.3 that $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-12$ and $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t''} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t''-1}$. As $t'' \in (t'_1, t']$ and we have Item 1 of Lemma 7.3, this means that $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-11$. As $\mathsf{LastOk}^{\mathsf{B}}_{t''} = \texttt{True}$, we have that Bob executed one of the Lines 103 and 113 to set this value. In fact, as $15t-11 \not\equiv 0 \pmod 3$, he must have executed Line 113 in iteration t''. However, this means that he must have incremented in Line 114 a contradiction.

Note that this claim together with Item 1 of Lemma 7.4 also implies that there does not exist $t'' \in (t'_1, t']$ such that Alice executes Line 83 in iteration t''. As Line 83 is the only line where Alice changes the variables σ_0 and σ_1, we get that the teleportation bits $\sigma^{\mathsf{A}}_{0,t'_1}, \sigma^{\mathsf{A}}_{1,t'_1}$ obtained by Alice above stay unchanged till the end of iteration t'.

Next, we claim that there does not exist $t'' \in (t'_1, t']$ such that Bob executes Line 105 in iteration t''. Indeed for this to happen, we have from Line 104 that $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t''} \equiv 3 \pmod{30}$. This is impossible given that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} \in \{15t-1, 15t+1\}$ and Equation (3).

Finally, we claim that for all $t'' \in (t'_1, t']$ Bob executes Lines 107 and 109 in iteration t'' if and only if he increments in Line 110 and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-8$ and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-2$ respectively. For this, assume first that Bob increments in Line 110 and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-8$. By Line 103 and Item 1 of Lemma 7.3, this means that $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-9$. Using the if statement in Line 110, conclude that Bob also executes Line 107, as desired. A similar argument show that if Bob increments in Line 110 and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t''} = 15t-2$, he also executes Line 109. For the converse, it suffices to show that if Bob executes one of the Lines 107 and 109 in iteration t'', then $\mathsf{LastE}^{\mathsf{B}}_{t''} = \texttt{False}$. This is because if not, we have from Line 102 that Bob received the second register in state $|\mathsf{E}\rangle$ in iteration t''. This is only possible if Alice executes Line 69

in iteration t'' which from Line 68 means that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t''-1} \equiv 3 \pmod{30}$. However, if Bob executes one of the Lines 107 and 109 in iteration t'', then we have $\mathsf{LastOk}^{\mathsf{B}}_{t''} = \texttt{True}$ and $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t''} \bmod 30 \in \{21, 27\}$. This contradicts Item 4 of Lemma 7.3.

From this last claim and Equation (3) conclude that for all $t'' \in (t'_1, t']$ Bob executes Lines 107 and 109 in iteration t'' if and only if $t'' = t'_2$ and $t'' = t'_3$ respectively. Also, combining the three claims above gives that when Bob executes the Pauli correction in Line 109 in iteration t'_3, he does so on the register $Q^{\mathsf{B}}_{t'_1}$. Thus, if we show that $\left(\tilde{\sigma}^{\mathsf{B}}_{0,t'_3}, \tilde{\sigma}^{\mathsf{B}}_{1,t'_3}\right) = \left(\sigma^{\mathsf{A}}_{0,t'_1}, \sigma^{\mathsf{A}}_{1,t'_1}\right)$, we will get that the received message register computed by Bob in iteration t'_3 is correct. To this end, note that Bob only changes $(\tilde{\sigma}_0, \tilde{\sigma}_1)$ in Lines 107 and 109. Thus, it suffices to show that we have $\tilde{\sigma}^{\mathsf{B}}_{0,t'_2} = \sigma^{\mathsf{A}}_{0,t'_1}$ and $\tilde{\sigma}^{\mathsf{B}}_{1,t'_3} = \sigma^{\mathsf{A}}_{1,t'_1}$. As we showed that the teleportation bits obtained by Alice above stay unchanged till the end of iteration t', it suffices to show that $\tilde{\sigma}^{\mathsf{B}}_{0,t'_2} = \sigma^{\mathsf{A}}_{0,t'_2-1}$ and $\tilde{\sigma}^{\mathsf{B}}_{1,t'_3} = \sigma^{\mathsf{A}}_{1,t'_3-1}$. We prove the former as the proof of the latter is analogous. Note from the fact that Bob executes Line 107 in iteration t'_2 implies that $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t'_2} \equiv 21 \pmod{30}$ and $\mathsf{LastOk}^{\mathsf{B}}_{t'_2} = \texttt{True}$. From Item 4 of Lemma 7.3, this means that $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'_2-1} \equiv 21 \pmod{30}$. From Line 71, we have the result.

Finally, to finish the proof, it suffices to that Alice and Bob do not execute any relevant lines in iterations $t'' \in (t'_3, t']$. For Lines 83, 87 and 105 this is because of Equation (3) and for Line 109, this is because of the last claim above. □

7.3 Finishing the Proof

Recall that we assume that T is even. Lemma 7.5 shows that if $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{T'/2} \geq 15T$, the the parties have successfully simulated the protocol. In this section, we show that $\mathsf{B\text{-}cnt}^{\mathsf{B}}$ is indeed large enough at the end of the protocol. For this, we show the Lemma 7.7 below that uses our upper bound on $|\mathsf{Adv}'|$. Observe that this lemma combined with Lemma 7.5 finishes our proof of correctness of Algorithms 5 and 6.

Lemma 7.6. *Let $t' \in [T'/2]$.*

1. *If $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \mathsf{LastE}^{\mathsf{A}}_{t'} = \texttt{True}$, we have $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$ and $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}$.*
2. *If $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \mathsf{LastE}^{\mathsf{B}}_{t'} = \texttt{True}$, we have $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False}$ and $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-2}$.*

Proof. We prove each part separately.

1. If $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \mathsf{LastE}^{\mathsf{A}}_{t'} = \texttt{True}$, then we have from Line 80 that Alice measures the second register she receives in iteration t' and gets $|\mathsf{E}\rangle$. From Line 118, this is possible only if $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$. This means that Bob does not execute Lines 110 and 114 in iteration t' and we have $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}$.

2. If $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \mathsf{LastE}^{\mathsf{B}}_{t'} = \texttt{True}$, then we have from Line 102 that Bob measures the second register he receives in iteration t' and gets $|\mathsf{E}\rangle$. From Line 69, this is possible only if $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False}$. This means that Alice does not execute Lines 88 and 92 in iteration $t'-1$ and we have $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-2}$.

□

Lemma 7.7. *We have* $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{T'/2} \geq 15T$.

Proof. We call an iteration $t' \in [T'/2]$ a pause iteration if it holds that $\max\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}\right) = \max\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}\right)$. Deduce from Proposition 7.2 and Item 1 of Lemma 7.3 that for any pause iteration t', it holds that $\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}\right) = \left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}\right)$. We say a pause iteration is an Alice-pause iteration if $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} > \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$ and a Bob-pause iteration if $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} < \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$.

We claim that any Bob-pause iteration t' must satisfy either $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{False}$ or $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$. To see why, assume that $\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{True}$ for a Bob-pause iteration t'. Item 3 of Lemma 7.3 implies that $\mathsf{B\text{-}cnt}^{\mathsf{A}}_{t'} > \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'}$. From Lines 88 and 92, this is possible only if $\mathsf{LastE}^{\mathsf{A}}_{t'} = \texttt{True}$. From Item 1 of Lemma 7.6, this means that $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$, as desired. From this claim, we can bound the number of Bob-pause iterations by:

$$\sum_{\text{Bob-pause } t'} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{False}\right) + \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}\right). \tag{4}$$

Next, we claim that any Alice-pause iteration must satisfy that either $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}$ or both $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False}$ and $t'-1$ is not a Bob-pause iteration. To see why, assume that $\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{True}$ for an Alice-pause iteration t'. Item 4 of Lemma 7.3 implies that $\mathsf{A\text{-}cnt}^{\mathsf{B}}_{t'} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'} > \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}$. From Lines 110 and 114, this is possible only if $\mathsf{LastE}^{\mathsf{B}}_{t'} = \texttt{True}$. From Item 2 of Lemma 7.6, this means that $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False}$ and $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1} = \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-2}$. Using Proposition 7.2, the latter gives $\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-2} > \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'} \geq \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-2}$. If $t'-1$ were a Bob-pause iteration, we would have $\mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-2} = \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1} > \mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}$, a contradiction. Thus, we have $\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False}$ and that $t'-1$ is not a Bob-pause iteration, as desired. From this claim, we can bound the number of Alice-pause iterations by:

$$\sum_{\text{Alice-pause } t'} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}\right) + \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False} \wedge t'-1 \text{ is not Bob-pause}\right). \tag{5}$$

Adding Equations (4) and (5) we get that the total number of pause iteration is upper bounded by:

$$\sum_{\text{pause } t'} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}\right) + \sum_{\text{Bob-pause } t'} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{False}\right) + \sum_{\text{Alice-pause } t'} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False} \wedge t'-1 \text{ is not Bob-pause}\right).$$

This is upper bounded by:

$$\sum_{t' \in [T'/2]} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}\right) + \sum_{\text{Bob-pause } t'} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{False}\right)$$

$$+ \sum_{t' \in [T'/2]} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'-1} = \texttt{False} \wedge t'-1 \text{ is not Bob-pause}\right).$$

Using Alice's intialization in Line 63, we get the upper bound:

$$\sum_{t' \in [T'/2]} \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{B}}_{t'} = \texttt{False}\right) + \mathbb{1}\left(\mathsf{LastOk}^{\mathsf{A}}_{t'} = \texttt{False}\right).$$

Note that this is just the number of rounds erased by the adversary. Thus, we get that the number of pause iterations is at most $|\mathsf{Adv}'| \leq \left\lceil \left(\frac{1}{2} - \epsilon\right) T' \right\rceil$. Thus, at least $\epsilon T' - 1$ iterations are not pause iterations and satisfy $\max\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'}\right) \neq \max\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{t'-1}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{t'-1}\right)$. Due to Proposition 7.2 and the fact that $T' = \frac{20T}{\epsilon}$, we get that $\max\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{T'/2}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{T'/2}\right) \geq 15T$. Again using Proposition 7.2, we get that $\min\left(\mathsf{A\text{-}cnt}^{\mathsf{A}}_{T'/2}, \mathsf{B\text{-}cnt}^{\mathsf{B}}_{T'/2}\right) \geq 15T$, and the lemma follows. □

References

[BBC+93] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993. 12

[BDSS06] Charles H. Bennett, Igor Devetak, Peter W. Shor, and John A. Smolin. Inequalities and separations among assisted capacities of quantum channels. *Physical Review Letters*, 96:150502, 2006. 5

[BEK+25] Mark Braverman, Klim Efremenko, Gillat Kol, Raghuvansh R. Saxena, and Zhijun Zhang. Round-vs-resilience tradeoffs for binary feedback channels. In Raghu Meka, editor, *Innovations in Theoretical Computer Science Conference (ITCS)*, pages 22:1–22:23, 2025. 4

[Ber64] Elwyn R. Berlekamp. *Block Coding with Noiseless Feedback*. PhD thesis, Massachusetts Institute of Technology, 1964. 4

[BGG22] Thiago Bergamaschi, Louis Golowich, and Sam Gunn. Approaching the quantum singleton bound with approximate error correction. *arXiv preprint arXiv:2212.09935*, 2022. 12

[BN05] Garry Bowen and Rajagopal Nagarajan. On feedback and the classical capacity of a noisy quantum channel. *IEEE Transactions on Information Theory*, 51(1):320–324, 2005. 2, 5

[BNT+19] Gilles Brassard, Ashwin Nayak, Alain Tapp, Dave Touchette, and Falk Unger. Noisy interactive quantum communication. *SIAM Journal on Computing*, 48(4):1147–1195, 2019. 4, 11

[Bow04] Garry Bowen. Quantum feedback channels. *IEEE Transactions on Information Theory*, 50(10):2429–2434, 2004. 2, 5

[Bow05] Garry Bowen. Feedback in quantum communication. *International Journal of Quantum Information*, 3(1):123–127, 2005. 2, 5

[CG97] Richard Cleve and Daniel Gottesman. Efficient computations of encodings for quantum error correction. *Physical Review A*, 1997. 12

[Die82] DGBJ Dieks. Communication by epr devices. *Physics Letters A*, 1982. 12

[DQSW19] Dawei Ding, Yihui Quek, Peter W. Shor, and Mark M. Wilde. Entropy bound for the classical capacity of a quantum channel assisted by classical feedback. In *IEEE International Symposium on Information Theory*, pages 2399–2403, 2019. 2, 5

[DSW16] Runyao Duan, Simone Severini, and Andreas Winter. On zero-error communication via quantum channels in the presence of noiseless feedback. *IEEE Transactions on Information Theory*, 62(9):5260–5277, 2016. 5

[DW18] Dawei Ding and Mark M. Wilde. Strong converse for the feedback-assisted classical capacity of entanglement-breaking channels. *Problems of Information Transmission*, 54(1):1–19, 2018. 5

[EKSZ22] Klim Efremenko, Gillat Kol, Raghuvansh R. Saxena, and Zhijun Zhang. Binary codes with resilience beyond one-quarter via interaction. In *Symposium on Foundations of Computer Science (FOCS)*, pages 1–12, 2022. 1, 4

[GGZ23] Meghal Gupta, Venkatesan Guruswami, and Rachel Yun Zhang. Binary error-correcting codes with minimal noiseless feedback. In *Symposium on Theory of Computing (STOC)*, pages 1475–1487, 2023. 4

[GI05] Venkatesan Guruswami and Piotr Indyk. Linear-time encodable/decodable codes with near-optimal rate. *IEEE Transactions on Information Theory*, 2005. 11

[GKZ22] Meghal Gupta, Yael Tauman Kalai, and Rachel Yun Zhang. Interactive error correcting codes over binary erasure channels resilient to greater one-half adversarial corruption. In *Symposium on Theory of Computing (STOC)*, pages 609–622, 2022. 1, 4

[Got97] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997. 12

[GZ22] Meghal Gupta and Rachel Yun Zhang. Positive rate binary interactive error correcting codes resilient to greater than one-half adversarial erasures, 2022. 1, 4

[GZ23] Meghal Gupta and Rachel Yun Zhang. A new upper bound on the maximal error resilience of interactive error-correcting codes, 2023. 1, 4

[HB97] Mark Hillery and V Bužek. Quantum copying: Fundamental inequalities. *Physical Review A*, 1997. 2

[HKV15] Bernhard Haeupler, Pritish Kamath, and Ameya Velingker. Communication with partial noiseless feedback. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, APPROX/RANDOM 2015, pages 881–897, 2015. 4

[KO26] Kao-Yueh Kuo and Yingkai Ouyang. Degenerate quantum erasure decoding. *npj Quantum Information*, 2026. 12

[KW99] Michael Keyl and Reinhard F Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 1999. 2

[Leu08] Alan W. Leung. Quantum entanglement capacity with classical feedback. *Physical Review A*, 77:012322, 2008. 2, 5

[LLS09] Debbie Leung, Joungkeun Lim, and Peter W. Shor. Capacity of quantum erasure channel assisted by backward classical communication. *Physical Review Letters*, 103:240505, 2009. 2, 5

[Sch92] Leonard J. Schulman. Communication on noisy channels: A coding theorem for computation. In *Symposium on Foundations of Computer Science (FOCS)*, pages 724–733, 1992. 4

[Sch93] Leonard J. Schulman. Deterministic coding for interactive communication. In *Symposium on Theory of Computing (STOC)*, pages 747–756, 1993. 4

[Sch96] Leonard J. Schulman. Coding for interactive communication. *IEEE Transactions on Information Theory*, 42(6):1745–1756, 1996. 4

[Sha56] Claude E. Shannon. The zero error capacity of a noisy channel. *IRE Transactions on Information Theory*, 2(3):8–19, 1956. 4

[Ske04] Andrew Skeen. Classical feedback for quantum channels, 2004. 2, 5

[Win06] Andreas Winter. Identification via quantum channels in the presence of prior correlation and feedback. In *General Theory of Information Transfer and Combinatorics*, volume 4123 of *Lecture Notes in Computer Science*, pages 486–504. Springer, 2006. 5

[WQC17] Gang Wang, Yanyuan Qin, and Chengjuan Chang. Communication with partial noisy feedback. In *IEEE Symposium on Computers and Communications*, pages 602–607, 2017. 4

[WZ82] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982. 12, 13

[Zig76] K. Sh. Zigangirov. On the number of correctable errors for transmission over a binary symmetrical channel with feedback. *Problems of Information Transmission*, 12(2):85–97, 1976. 4

A Proof of Theorem 3.1

Proof by backward induction on τ. We first consider the base case $\tau = T$. Let $\left(\mathcal{I}^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}\right)_{K^{\mathsf{A}}_{\leq T}\in\mathcal{K}^{\mathsf{A}}_{\leq T}}$ be the instruments used by Alice to compute the output. As the outcomes of these instruments are discarded in the execution, they may be assumed to be CPTP maps without loss of generality. By the Stinespring dilation theorem, we get that there exists a register E^{A} and unitaries $\left(U^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}\right)_{K^{\mathsf{A}}_{\leq T}\in\mathcal{K}^{\mathsf{A}}_{\leq T}}$ such that for all $K^{\mathsf{A}}_{\leq T} \in \mathcal{K}^{\mathsf{A}}_{\leq T}$ and all density matrices $\rho_{A\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})}}$, it holds that:

$$\mathcal{I}^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}\left(\rho_{A\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})}}\right) = \mathsf{tr}_{E^{\mathsf{A}}}\left(U^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}\left(\rho_{A\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})}}\otimes|0\rangle\langle 0|_{E^{\mathsf{A}}}\right)U^{\mathsf{A},\dagger}_{T+1,K^{\mathsf{A}}_{\leq T}}\right).$$

We define E^{B} and unitaries $\left(U^{\mathsf{B}}_{T+1,K^{\mathsf{B}}_{\leq T}}\right)_{K^{\mathsf{B}}_{\leq T}\in\mathcal{K}^{\mathsf{B}}_{\leq T}}$ analogously. Define the protocol Π' to be the same as Π except that the registers E^{A} and E^{B} are added[17] to registers A and B respectively, and for all $K^{\mathsf{A}}_{\leq T} \in \mathcal{K}^{\mathsf{A}}_{\leq T}$, the instrument $\mathcal{I}^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}$ is replaced by the instrument $\mathcal{I}'^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}$ that consists of (only) the unitary operator $U^{\mathsf{A}}_{T+1,K^{\mathsf{A}}_{\leq T}}$ (and likewise for Bob's instruments). To show the protocols Π and Π' are equivalent, consider an arbitrary reference register R and an arbitrary adversary Adv. By construction, Π and Π' behave identically in the T rounds of communication except that Π' has additional registers E^{A} and E^{B}. Thus, for any outcomes $K^{\mathsf{A}}_{\leq T}$ and $K^{\mathsf{B}}_{\leq T}$ of the parties' instruments, if conditioned on these outcomes, the joint state of Alice and Bob and the reference register after T rounds of communication in Π is represented by the density matrix ρ, their corresponding state in Π' is $\rho\otimes|0\rangle\langle 0|_{E^{\mathsf{A}}E^{\mathsf{B}}}$.

Recall that $O = A_{\mathsf{out}}B_{\mathsf{out}}$ denotes the output registers of the parties. To finish the proof, recall that the parties in Π compute the output state as (letting $t = T+1$):

$$\mathsf{tr}_{\overline{OR}}\left(\left(\mathcal{I}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}\otimes\mathcal{I}^{\mathsf{B}}_{t,K^{\mathsf{B}}_{<t}}\otimes\mathsf{I}_R\right)(\rho)\right)$$

[17] Note that all other instruments used by the parties need to be adjusted to allow for the extra registers but we will ignore this technicality.

$$= \mathsf{tr}_{\overline{OR}E^{\mathsf{A}}E^{\mathsf{B}}}\Big(\Big(U^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}} \otimes U^{\mathsf{B}}_{t,K^{\mathsf{B}}_{<t}} \otimes \mathsf{I}_R\Big)(\rho \otimes |0\rangle\langle 0|_{E^{\mathsf{A}}E^{\mathsf{B}}})\Big(U^{\mathsf{A},\dagger}_{t,K^{\mathsf{A}}_{<t}} \otimes U^{\mathsf{B},\dagger}_{t,K^{\mathsf{B}}_{<t}} \otimes \mathsf{I}_R\Big)\Big)$$
$$= \mathsf{tr}_{\overline{OR}E^{\mathsf{A}}E^{\mathsf{B}}}\Big(\Big(\mathcal{I}'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}} \otimes \mathcal{I}'^{\mathsf{B}}_{t,K^{\mathsf{B}}_{<t}} \otimes \mathsf{I}_R\Big)(\rho \otimes |0\rangle\langle 0|_{E^{\mathsf{A}}E^{\mathsf{B}}})\Big).$$

This is exactly the output state of Π', and we are done. We now deal with the case $\tau < T$ assuming the result holds for $\tau + 1$. By the induction hypothesis, we get that there is an equivalent protocol Π'' with the same classicality prefix such that the theorem holds for all $t \in (\tau+1, T+1]$. Abusing notation slightly, we henceforth denote this protocol by Π. Let $t = \tau + 1$ and assume without loss of generality that $\mathsf{p}(t) = \mathsf{A}$. For $t' \in \{0\} \cup [T]$, we let $A_{t'} = AM_{\mathsf{p}^{-1}(\mathsf{A})_{>t'}}\tilde{M}_{\mathsf{p}^{-1}(\mathsf{B})_{\leq t'}}$ and $B_{t'} = BM_{\mathsf{p}^{-1}(\mathsf{B})_{>t'}}\tilde{M}_{\mathsf{p}^{-1}(\mathsf{A})_{\leq t'}}$ be the registers held by Alice and Bob respectively after t' rounds.

Recall that for all outcomes $K^{\mathsf{A}}_{<t} \in \mathcal{K}^{\mathsf{A}}_{<t}$, Alice has an instrument $\mathcal{I}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$. Let $\mathcal{I}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}} = \left\{\mathcal{I}^{\mathsf{A},K^{\mathsf{A}}_t}_{t,K^{\mathsf{A}}_{<t}}\right\}_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t}$ be the collection of completely positive trace-non-increasing maps (whose sum is trace preserving) for these instruments. Define the CPTP map $\mathcal{J}$ on the registers A_τ such that for all density matrices ρ_{A_τ}, we have:

$$\mathcal{J}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}(\rho_{A_\tau}) = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} \mathcal{I}^{\mathsf{A},K^{\mathsf{A}}_t}_{t,K^{\mathsf{A}}_{<t}}(\rho_{A_\tau}) \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'}\,, \tag{6}$$

for an auxiliary register E'. By the Stinespring dilation theorem, there exist registers E and a unitary $U'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$ such that for all density matrices ρ_{A_τ}, we have:

$$\mathcal{J}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}(\rho_{A_\tau}) = \mathsf{tr}_E\Big(U'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}(\rho_{A_\tau} \otimes |0\rangle\langle 0|_{EE'})U'^{\mathsf{A},\dagger}_{t,K^{\mathsf{A}}_{<t}}\Big), \tag{7}$$

We define the protocol Π' to be the same as the protocol Π except that (1) The registers E and E' are added to the register A. (2) For all $K^{\mathsf{A}}_{<t} \in \mathcal{K}^{\mathsf{A}}_{<t}$, the instrument $\mathcal{I}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$ is replaced by the instrument $\mathcal{I}'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$ that only consists of the unitary operator $U'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$. (3) For all $t' \in (t, T+1]$, the unitary[18] $U^{\mathsf{A}}_{t',K^{\mathsf{A}}_{\leq t}}$ used by Alice in round t' is replaced by the unitary $U'^{\mathsf{A}}_{t',K^{\mathsf{A}}_{<t}} = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} U^{\mathsf{A}}_{t',K^{\mathsf{A}}_{\leq t}} \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'} \otimes \mathsf{I}_E$. Also, note from $\mathsf{p}(t) = \mathsf{A}$ that Bob's instrument in round t was the identity instrument. Thus, it suffices to show that the protocols Π and Π' are equivalent. We do this next.

For all $t' \in \{0\} \cup [T]$, let $A'_{t'} = A_{t'}EE'$ be the registers held by Alice in Π' after t' rounds. Fix an arbitrary reference register R, an arbitrary adversary Adv. Also, fix any outcomes $K^{\mathsf{A}}_{<t} \in \mathcal{K}^{\mathsf{A}}_{<t}$ and $K^{\mathsf{B}}_{<t} \in \mathcal{K}^{\mathsf{B}}_{<t}$ observed by Alice and Bob before in the first $t-1$ rounds. By construction, Π and Π' behave identically in the first $\tau = t-1$ rounds of communication except that Π' has additional registers EE'. Thus, conditioned on these outcomes, the joint state of Alice and Bob and the reference register after τ rounds of communication in Π is represented by the density matrix ρ on the registers $A_\tau B_\tau R$, their corresponding state in Π' is $\rho \otimes |0\rangle\langle 0|_{EE'}$.

[18] Recall that the instruments used in these rounds consist of a single unitary and have a fixed outcome.

In round t in Π', Alice applies the instrument $\mathcal{I}'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$ and her state becomes:

$$\rho'_{A'_\tau B_\tau R} = \Big(U'^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}} \otimes \mathsf{I}_{B_\tau R}\Big)(\rho \otimes |0\rangle\langle 0|_{EE'})\Big(U'^{\mathsf{A},\dagger}_{t,K^{\mathsf{A}}_{<t}} \otimes \mathsf{I}_{B_\tau R}\Big)$$

Similarly, in the protocol Π, Alice applies the instrument $\mathcal{I}^{\mathsf{A}}_{t,K^{\mathsf{A}}_{<t}}$ and, for all $K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t$, gets outcome K^{A}_t with probability $p_\rho\big(K^{\mathsf{A}}_t \mid K^{\mathsf{A}}_{<t}\big) = \mathsf{tr}\Big(\mathcal{I}^{\mathsf{A},K^{\mathsf{A}}_t}_{t,K^{\mathsf{A}}_{<t}}(\mathsf{tr}_{B_\tau R}(\rho))\Big)$, and conditioned on this outcome, her state becomes:

$$\rho^{K^{\mathsf{A}}_t}_{A_\tau B_\tau R} = \frac{1}{p_\rho\big(K^{\mathsf{A}}_t \mid K^{\mathsf{A}}_{<t}\big)} \cdot \Big(\mathcal{I}^{\mathsf{A},K^{\mathsf{A}}_t}_{t,K^{\mathsf{A}}_{<t}} \otimes \mathsf{I}_{B_\tau R}\Big)(\rho).$$

From Equations (6) and (7), we get:

$$\mathsf{tr}_E\big(\rho'_{A'_\tau B_\tau R}\big) = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} p_\rho\big(K^{\mathsf{A}}_t \mid K^{\mathsf{A}}_{<t}\big) \cdot \Big(\rho^{K^{\mathsf{A}}_t}_{A_\tau B_\tau R} \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'}\Big). \tag{8}$$

Claim A.1. *Let $A' = AEE'$ and suppose there are density matrices $\rho'_{A'BR}$ and $\Big(\rho^{K^{\mathsf{A}}_t}_{ABR}\Big)_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t}$ and constants $\Big(\lambda_{K^{\mathsf{A}}_t}\Big)_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t}$ satisfying:*

$$\mathsf{tr}_E(\rho'_{A'BR}) = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} \lambda_{K^{\mathsf{A}}_t} \cdot \Big(\rho^{K^{\mathsf{A}}_t}_{ABR} \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'}\Big).$$

1. *For any unitaries $\Big(U_{K^{\mathsf{A}}_t}\Big)_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t}$ on the register A, if $U' = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} U_{K^{\mathsf{A}}_t} \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'} \otimes \mathsf{I}_E$, it holds that:*

$$\mathsf{tr}_E\big((U' \otimes \mathsf{I}_{BR})\rho'_{A'BR}\big(U'^\dagger \otimes \mathsf{I}_{BR}\big)\big) = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} \lambda_{K^{\mathsf{A}}_t} \cdot \Big(U_{K^{\mathsf{A}}_t} \otimes \mathsf{I}_{BR}\Big)\rho^{K^{\mathsf{A}}_t}_{ABR}\Big(U^\dagger_{K^{\mathsf{A}}_t} \otimes \mathsf{I}_{BR}\Big) \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'}.$$

2. *For any unitary U on the register B, it holds that:*

$$\mathsf{tr}_E\big((U \otimes \mathsf{I}_{A'R})\rho'_{A'BR}\big(U^\dagger \otimes \mathsf{I}_{A'R}\big)\big) = \sum_{K^{\mathsf{A}}_t \in \mathcal{K}^{\mathsf{A}}_t} \lambda_{K^{\mathsf{A}}_t} \cdot (U \otimes \mathsf{I}_{AR})\rho^{K^{\mathsf{A}}_t}_{ABR}\big(U^\dagger \otimes \mathsf{I}_{AR}\big) \otimes |K^{\mathsf{A}}_t\rangle\langle K^{\mathsf{A}}_t|_{E'}.$$

3. *It holds that:*

$$\mathsf{tr}_E\Big(\mathsf{tr}_{M_{t'}}(\rho'_{A'BR}) \otimes |\bot\rangle\langle\bot|_{\tilde{M}_{t'}}\Big)$$

$$= \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} \lambda_{K_t^{\mathsf{A}}} \cdot \left(\mathsf{tr}_{M_{t'}} \left(\rho_{ABR}^{K_t^{\mathsf{A}}} \right) \otimes |\perp\rangle\langle\perp|_{\tilde{M}_{t'}} \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} \right).$$

Proof. We prove the parts separately.

1. We have:

$$\begin{aligned}
&\mathsf{tr}_E\big((U' \otimes \mathsf{I}_{BR})\rho'_{A'BR}(U'^{\dagger} \otimes \mathsf{I}_{BR})\big) \\
&= \left(\sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} U_{K_t^{\mathsf{A}}} \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} \otimes \mathsf{I}_{BR} \right) \mathsf{tr}_E(\rho'_{A'BR}) \left(\sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} U^{\dagger}_{K_t^{\mathsf{A}}} \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} \otimes \mathsf{I}_{BR} \right) \\
&= \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} \lambda_{K_t^{\mathsf{A}}} \cdot \left(U_{K_t^{\mathsf{A}}} \otimes \mathsf{I}_{BR} \right) \rho_{ABR}^{K_t^{\mathsf{A}}} \left(U^{\dagger}_{K_t^{\mathsf{A}}} \otimes \mathsf{I}_{BR} \right) \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} .
\end{aligned}$$

2. We have:

$$\begin{aligned}
&\mathsf{tr}_E\big((U \otimes \mathsf{I}_{A'R})\rho'_{A'BR}(U^{\dagger} \otimes \mathsf{I}_{A'R})\big) \\
&\quad = (U \otimes \mathsf{I}_{AE'R})\, \mathsf{tr}_E(\rho'_{A'BR}) \big(U^{\dagger} \otimes \mathsf{I}_{AE'R}\big) \\
&\quad = \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} \lambda_{K_t^{\mathsf{A}}} \cdot (U \otimes \mathsf{I}_{AE'R}) \left(\rho_{ABR}^{K_t^{\mathsf{A}}} \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} \right) \big(U^{\dagger} \otimes \mathsf{I}_{AE'R}\big) \\
&\quad = \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} \lambda_{K_t^{\mathsf{A}}} \cdot (U \otimes \mathsf{I}_{AR}) \rho_{ABR}^{K_t^{\mathsf{A}}} \big(U^{\dagger} \otimes \mathsf{I}_{AR}\big) \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} .
\end{aligned}$$

3. We have:

$$\begin{aligned}
&\mathsf{tr}_E\Big(\mathsf{tr}_{M_{t'}}(\rho'_{A'BR}) \otimes |\perp\rangle\langle\perp|_{\tilde{M}_{t'}} \Big) \\
&\quad = \mathsf{tr}_{EM_{t'}}(\rho'_{A'BR}) \otimes |\perp\rangle\langle\perp|_{\tilde{M}_{t'}} \\
&\quad = \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} \lambda_{K_t^{\mathsf{A}}} \cdot \left(\mathsf{tr}_{M_{t'}} \left(\rho_{ABR}^{K_t^{\mathsf{A}}} \right) \otimes |\perp\rangle\langle\perp|_{\tilde{M}_{t'}} \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} \right).
\end{aligned}$$

□

From Equation (8) and Claim A.1, we get that regardless of the erasures introduced by the channel, and the unitaries applied by Alice and Bob, if $\rho'_{A'_T B_T R}$ is the joint state at the end of Π', conditioned on the outcomes $K^{\mathsf{A}}_{<t}$ and $K^{\mathsf{B}}_{<t}$, and, for all $K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}$, let $\rho^{K_t^{\mathsf{A}}}_{A_T B_T R}$ is the joint state at the end of Π, additionally conditioned on the outcomes K_t^{A}, then we have:

$$\mathsf{tr}_E\left(\rho'_{A'_T B_T R}\right) = \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} p_\rho\big(K_t^{\mathsf{A}} \mid K^{\mathsf{A}}_{<t}\big) \cdot \left(\rho^{K_t^{\mathsf{A}}}_{A_T B_T R} \otimes |K_t^{\mathsf{A}}\rangle\langle K_t^{\mathsf{A}}|_{E'} \right).$$

This means:

$$\mathsf{tr}_{\overline{OR}EE'}\left(\rho'_{A'_T B_T R}\right) = \sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} p_\rho\left(K_t^{\mathsf{A}} \mid K_{<t}^{\mathsf{A}}\right) \cdot \mathsf{tr}_{\overline{OR}}\left(\rho^{K_t^{\mathsf{A}}}_{A_T B_T R}\right)$$
$$= \mathsf{tr}_{\overline{OR}}\left(\sum_{K_t^{\mathsf{A}} \in \mathcal{K}_t^{\mathsf{A}}} p_\rho\left(K_t^{\mathsf{A}} \mid K_{<t}^{\mathsf{A}}\right) \cdot \rho^{K_t^{\mathsf{A}}}_{A_T B_T R}\right).$$

In other words, the output states of the protocols are the same, as desired.

B Two-Way Code with Free Noiseless Classical Feedback

This section is devoted to proving Theorem B.1, where free and noiseless feedback is available.

Theorem B.1. *For all $\epsilon > 0$, there exists a two-way code with free noiseless classical feedback and resilience $(1-\epsilon)$ over an alphabet of size $q = O_\epsilon(1)$, constant rate $\Omega_\epsilon(1)$, and runs in polynomial time.*

Let A_{inp} and B_{out} be n-qubit registers[19] for input and output respectively, and $1-\epsilon$ the target erasure resilience. Set $L = 200n/\epsilon$ and $R = 10/\epsilon$. Let K_{C} be the constant claimed by Lemma 3.2 for rate $\epsilon/100$ and relative distance $1-\epsilon/10$.

The protocol consists of R iterations. In each iteration, Alice first sends L qudits over an alphabet of size $K = 2K_{\mathsf{C}}$. Then, Bob replies with L bits indicating whether each qudit is received. The overall length of the protocol is thus $T = LR = O_\epsilon(n)$.

Let C be a one-way classical erasure code with $2n$-bit inputs and L-symbol codewords over an alphabet of size K_{C}, that has resilience $1-\epsilon/10$. Its existence is guaranteed by Lemma 3.2 as $\epsilon/100 \cdot L \geq 2n$. Let D be the decoding function corresponding to C.

The Alice's and Bob's sides of the protocol are given in Algorithms 7 and 8 respectively. Capital letters W, X, Y, Z are reserved for quantum registers. All other variables are classical. If some variable var appears in both sides of the protocol, we may use superscripts A, B to avoid confusion when necessary. That is, we write $\mathsf{var}^{(\mathsf{A})}$ for Alice's copy and $\mathsf{var}^{(\mathsf{B})}$ for Bob's copy. If the same variable var is used across multiple iterations, we write $\mathsf{var}^{(r)}$ to denote its value at the end of the r-th (outer) iteration. The superscripts are omitted when they are clear from context.

B.1 Analysis

Now we prove Theorem B.1. Fix an arbitrary n-qubit input and any adversary with at most $(1-\epsilon)\cdot T$ erasures. The protocol is well-defined as Alice uses an alphabet of size at most $2K_{\mathsf{C}} = K$ in Lines 129 and 133. We can also prove the following technical claim similar to Lemma 5.3. The argument is almost identical and omitted here.

[19] Without loss of generality, we assume the input and the output are binary, as in Section 5.

Algorithm 7 Alice's side of the protocol with input register A_{inp}.

Initialize $\mathsf{tp} \leftarrow 0$ and $A \leftarrow \perp^L$.
for $r \in [R]$ **do**
  if $\mathsf{tp} = 1$ **then**
    for $\ell \in [L]$ **do**
      Send $|\mathsf{tp}\rangle \otimes |A_\ell\rangle$ (as one qudit) to Bob.
  else
    for $\ell \in [L]$ **do**
      Initialize a fresh EPR pair $(Z^{(\mathsf{A})}_{L\cdot(r-1)+\ell}, Z^{(\mathsf{B})}_{L\cdot(r-1)+\ell})$.
      Send $|\mathsf{tp}\rangle \otimes Z^{(\mathsf{B})}_{L\cdot(r-1)+\ell}$ (as one qudit) to Bob.
  Receive an L-bit string $b^{(r)}$ from Bob.
  if $\mathsf{tp} = 0$ **and** $b^{(\le r)}$ has at least n bits "1" **then**
    Set $\mathsf{tp} \leftarrow 1$.
    Teleport A_{inp} using EPR halves $Z^{(\mathsf{A})}$ indexed by the first n bits "1" in $b^{(\le r)}$, resulting in $2n$ teleportation bits a.
    Encode $A \leftarrow \mathsf{C}(a)$.

Algorithm 8 Bob's side of the protocol with output register B_{out}.

Initialize $\mathsf{end} \leftarrow 0$ and $Z^{(\mathsf{B})} \leftarrow |\perp\rangle^{\otimes LR}$.
for $r \in [R]$ **do**
  Initialize $b^{(r)} \leftarrow 0^L$ and $A^{(r)} \leftarrow \perp^L$.
  for $\ell \in [L]$ **do**
    Receive $|\mathsf{tp}\rangle \otimes W$ (as one qudit) from Alice.
    if $\mathsf{end} = 0$ **and** $|\mathsf{tp}\rangle \otimes W \neq |\perp\rangle$ **then**
      Set $b^{(r)}_\ell \leftarrow 1$.
      if $\mathsf{tp} = 1$ **then**
        Set $A^{(r)}_\ell \leftarrow s$ where $W = |s\rangle$.
        if $A^{(r)}$ has at least $\epsilon/10 \cdot L$ non-erasure symbols **then**
          Decode $a \leftarrow \mathsf{D}(A^{(r)})$.
          Recover B_{out} from EPR halves $Z^{(\mathsf{B})}$ indexed by the first n bits "1" in $b^{(\le r)}$, corrected by $2n$ teleportation bits a.
          Set $\mathsf{end} \leftarrow 1$.
      else
        Relabel W as $Z^{(\mathsf{B})}_{L\cdot(r-1)+\ell}$.
  Send the L-bit string $b^{(r)}$ to Alice.

Lemma B.2. *For $r \in [R]$, it holds that*

1. $$\mathsf{tp}^{(\mathsf{A},r-1)} \leq \mathsf{tp}^{(\mathsf{A},r)}.$$

2. $$\mathsf{end}^{(r-1)} \leq \mathsf{end}^{(r)}.$$

Let $r_0 \in [R]$ be the unique iteration in which Alice executes Line 136 and $r_1 \in [R]$ be the unique iteration in which Bob executes Line 151. Lemma B.3 shows that r_0, r_1 are well-defined.

Lemma B.3. *It holds that*

$$1 \leq r_0 < r_1 \leq R.$$

Proof. Since Bob's communication to Alice is noiseless, they always hold the same $b^{(\leq r)}$ in any iteration r. Suppose for the sake of contradiction that Alice never executes Line 136. Then, $\mathsf{tp}^{\mathsf{B}} = \mathsf{tp}^{\mathsf{A}} = 0$ throughout. Due to the "if" condition in Line 135, Bob must have received less than n EPR halves in total, implying at least $T - n > (1-\epsilon) \cdot T$ erasures, a contradiction. Thus, r_0 is well-defined and its uniqueness follows from Item 1 in Lemma B.2.

Observe that Bob executes Line 151 only if Alice has already executed Line 136 in a previous iteration, because of the "if" condition in Line 146, hence $r_1 > r_0$. Now suppose for the sake of contradiction that Bob never executes Line 151. By Line 148, this happens only if more than $(1-\epsilon/10) \cdot L$ erasures have occurred in every iteration from $r_0 + 1$ onwards. However, the total number of erasures would be

$$\begin{aligned} & L \cdot (r_0 - 1) - n + (1-\epsilon/10) \cdot L \cdot (R - r_0) \\ & \quad \geq L \cdot (r_0 - 2) + (1-\epsilon/10) \cdot L \cdot (R - r_0) && (\text{as } n \leq L) \\ & \quad \geq (1-\epsilon/10) \cdot L \cdot (R-2) \\ & \quad > (1-\epsilon) \cdot T, \end{aligned}$$

a contradiction. Consequently, r_1 is well-defined and its uniqueness follows from Item 2 in Lemma B.2. □

Finally, we are ready to prove Theorem B.1.

Proof of Theorem B.1. By Lemma B.3, Alice executes Line 136 in the r_0-th iteration. She then teleports A_{inp} and encodes the teleportation bits a. In the r_1-th iteration, Bob executes Line 151 only after he decodes the teleportation bits and completes teleportation. The decoding $\mathsf{D}(\cdot)$ is always possible as the code $\mathsf{C}(\cdot)$ has erasure resilience $\epsilon/10$. Also note that Alice and Bob agree on the subset of EPR halves used for teleportation. This is because they hold the same $b^{(\leq r)}$ throughout as the backward channel is noiseless. Thus, B_{out} must be in the same state as input. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il