[9] A. Klapper and M. Goresky, , R. Anderson, Ed., "2-adic shift registers," in *Fast Software Encryption, Lecture Notes in Computer Science*. New York: Springer, 1994, vol. 809, pp. 174–178.

[10] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Crypt.*, vol. 10, pp. 111–147, 1997.

[11] N. Koblitz*, p-Adic Numbers, p-Adic Analysis, and Zeta Functions, Graduate Texts in Mathematics*. New York: Springer, 1984, vol. 58.

[12] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "First-order optimal approximation of binary sequences," in *Sequences and Their Applications-SETA'01*, T. Helleseth, P. V. Kumar, and K. Yang, Eds. London, U.K.: Springer, 2002, pp. 242–256.

[13] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2758–2764, Oct. 2002.

[14] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k-error linear complexity," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 694–698, Mar. 2000.

[15] T. Kaida, S. Uehara, and K. Imamura, "An algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n, p a prime," *Inf. Comput.*, vol. 151, pp. 134–147, 1999.

[16] T. Kaida, S. Uehara, and K. Imamura, "A new algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n," in *Sequences and Their Applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer, 1999, pp. 284–296.

[17] T. Kaida, S. Uehara, and K. Imamura, "On the profile of the k-error linear complexity and the zero sum property for sequences over $GF(p^m)$ with period p^n," in *Sequences and Their Applications-SETA'01*, T. Helleseth, P. V. Kumar, and K. Yang, Eds. London, U.K.: Springer, 2002, pp. 218–227.

[18] R. Lidl and H. Niederreiter*, Finite Fields*. Reading, MA: Addison-Wesley, 1983, (now distributed by Cambridge Univ. Press).

[19] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[20] W. Meidl, "Extended Games-Chan algorithm for the 2-adic complexity of FCSR-sequences," *Theoret. Comput. Sci.*, vol. 290, pp. 2045–2051, 2003.

[21] W. Meidl and H. Niederreiter, "On the expected value of the linear complexity and the k-error linear complexity of periodic sequences," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2817–2825, Nov. 2002.

[22] W. Meidl and H. Niederreiter, "Counting functions and expected values for the k-error linear complexity," *Finite Fields Appl.*, vol. 8, pp. 142–154, 2002.

[23] W. Meidl and H. Niederreiter, "Linear complexity, k-error linear complexity, and the discrete Fourier transform," *J. Complex.*, vol. 18, pp. 87–103, 2002.

[24] H. Niederreiter, "Periodic sequences with large k-error linear complexity," *IEEE Trans. Info. Theory*, vol. 49, no. 2, pp. 501–505, Feb. 2003.

[25] H. Niederreiter and H. Paschinger, "Counting functions and expected values in the stability theory of stream ciphers," in *Sequ. Their Applicat.*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer, 1999, pp. 318–329.

[26] W. Qi and H. Xu, "Partial period distribution of FCSR sequences," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 761–765, Mar. 2003.

[27] R. A. Rueppel*, Analysis and Design of Stream Cipher*. Berlin, Germany: Springer-Verlag, 1986.

[28] C. Seo, S. Lee, Y. Sung, K. Han, and S. Kim, "A lower bound on the linear span of an FCSR," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 691–693, Mar. 2000.

[29] M. Stamp and C. F. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1398–1401, Jul. 1993.

[30] D. Ye and Z. Dai, "Linear complexities of sequences obtained from periodic sequences over F_q by two-symbol substitution," (in Chinese) *J. Graduate School, Academia Sinica*, vol. 17, no. 2, pp. 7–9, Dec. 2000.

Communicating Over Adversarial Quantum Channels Using Quantum List Codes

Debbie Leung and Graeme Smith*, Member, IEEE*

***Abstract*—In this correspondence, we study quantum communication in the presence of adversarial noise. In this setting, communicating with perfect fidelity requires a quantum code of bounded minimum distance, for which the best known rates are given by the quantum Gilbert–Varshamov (QGV) bound. Asking only for arbitrarily high fidelity and letting the sender and reciever use a secret key of length logarithmic in the number of qubits sent, we find a dramatic improvement over the QGV rates. In fact, our protocols allow high fidelity transmission at noise levels for which perfect fidelity is impossible. To achieve such rates, we introduce fully quantum list codes, which may be of independent interest.**

***Index Terms*—Adversarial channels, approximate quantum codes, quantum error correction, quantum list codes.**

I. Introduction

Effectively dealing with noise is a major challenge faced by all proposals for the coherent manipulation of quantum information. Besides communication, sending a quantum state over a noisy channel models noisy storage, and as such, characterizing communication rates for quantum channels is a central question in the study of both quantum information and computation.

Various asymptotic capacities of quantum channels have been studied [1]–[11]. However, this work has been almost exclusively concerned with discrete memoryless channels (DMCs), wherein a sender and receiver use many independent and identical copies of a channel. In this scenario, one studies the asymptotic communication rate possible using an operation of the form $\mathcal{N}^{\otimes n}$, where $\mathcal{N}$ is the channel under consideration and the rate is $R = k/n$ where k is the number of high fidelity logical qubits sent. Relatively little is known outside of the DMC scenario, with notable exceptions found in [12]–[16].

In this paper, we study an adversarial quantum channel (AQC), which is perhaps as different from a DMC as one can imagine. When sending n qubits over an AQC, instead of errors on different qubits occuring independently, an adversary who knows what protocol is being used tries to foil the communication by maliciously choosing a superposition of errors, subject only to a restriction on the number of qubits each error affects. We call this channel $\mathcal{N}_{p,n}^{\mathrm{adv}}$, where p is the fraction of qubits the adversary is allowed to corrupt. $\mathcal{N}_{p,n}^{\mathrm{adv}}$ is the natural quantum generalization of the classical adversarial channel that was considered in [17], [18] and whose roots go back to [19].

Manuscript received June 14, 2006; revised July 6, 2007. D. Leung acknowledges travel funds from the CIAR to visit IBM, and funding from the Tolman Foundation, CIAR, NSERC, CRC, CFI, and OIT. The work of G. Smith was supported by the U.S. NSF Grant PHY-0456720 and Canada's NSERC. This work was supported by the U.S. NSF Grant EIA-0086038. The material in this correspondence was presented at the Ninth Workshop on Quantum Information Processing, Paris, France, January 2006.

D. Leung was with Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125 USA. She is now with the Institute for Quantum Computing, University of Waterloo, ON N2L 3G1, Canada (e-mail: wcleung@iqc.ca).

G. Smith was with the Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125 USA. He is now with the IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA (e-mail: graemesm@us.ibm.com).

Communicated by A. Winter, Associate Editor for Quantum Theory.

Digital Object Identifier 10.1109/TIT.2007.913433

If the receiver must reconstruct the logical state exactly, communicating over $\mathcal{N}_{p,n}^{\mathrm{adv}}$ requires a quantum error-correcting code (QECC) of distance $2\lceil np\rceil + 1$. The quantum Gilbert–Varshamov bound guarantees the existence of such a code with a rate of at least $1-H(2p)-2p\log 3$ [20], where logarithms are taken base 2 here and throughout. Communication beyond this rate is possible only if QECCs beating the Gilbert–Varshamov bound exist, which is a question that has been quite difficult to resolve. Furthermore, Rains has shown [21], [22] that no quantum code can have distance greater than $n(3-\sqrt{3})/4 \approx 0.317n$, so that it is impossible to send even a single qubit for $p \geq (3-\sqrt{3})/8 \approx 0.158$.

However, if we ask only for a high fidelity reconstruction, and allow the sender and receiver to share a secret key of size $O(\log n)$ it is possible to communicate at rates much higher than the Gilbert–Varshamov and Rains bounds suggest. Below, we present a coding strategy for this scenario with a rate of $1-H(p)-p\log 3$, which is significantly larger than the Gilbert–Varshamov rate for all values of p and remains nonzero up to $p \approx 0.189$. Our rate equals the best communication rate via the depolarizing channel (in the DMCs scenario) of error probability p using only nondegenerate codes.

There are three ingredients in achieving such rates with negligible length secret keys. The first is a predetermined quantum list code that is known to the adversary. This alone allows high-rate but low-fidelity transmission. To improve the fidelity, a random subcode is further chosen according to a secret key unknown to the adversary. Finally, the subcode is derandomized using small-biased sets.

Before explaining the construction of our code, we first discuss some intuition on why the code works and how resources are being reduced. Informally, a quantum list code is an error correcting code with the relaxed reconstruction requirement that the decoded state be equal to the original state acted on by a superposition of a small number of errors. We call the number of errors the "list length." This relaxation allows a considerable increase in rate over QECCs, and by a random coding argument we show there are list codes with constant-length lists and rates approaching $1-H(p)-p\log 3$ that tolerate pn errors. To distinguish between the errors in the list and communicate with high fidelity, the sender and receiver select a large subcode of the list code using a secret key. In particular, this can be chosen pseudorandomly by using $O(\log n)$ bits of secret key.

We can interpret our code as a set of (parity) check conditions that yield syndrome information. Most of these conditions are used in list-decoding and can be known to the adversary, and the rest of the conditions are pseudorandom and with high probability are capable of completely distinguishing the errors on the list. Note that there are simpler constructions using randomness unknown to the adversary, and we now make a comparison. The first construction is simply a random (nondegenerate) quantum error correcting code achieving the same rate but requiring $O(n^2)$ bits of secret key [1]. Second, one could use a secret permutation of the n qubits in the AQC turning the adversarial channel to something very similar to n depolarizing DMC's of error p in the DMC's setting [24], [15]. The best known rate is similar to ours (but slightly better for large p) but the cost will be $O(n\log n)$ bits of key, which, unfortunately, still gives a divergent key rate. Third, the standard derandomizing technique of key recycling cannot be used in a straightforward way in the current, adversarial, context. Thus, our hybrid construction involving a known list-code and a pseudorandom subcode demonstrates what type of randomness is unnecessary, and can be seen as a method to derandomize other key-inefficient protocols, achieving the same task with a much shorter key.

For the rest of the paper, we summarize related works, review background material, present the details of our construction, after which we discuss various applications and open problems.

Related work

Approximate error correction was studied in [25] to reduce the block length (and thus improving the rate) for a more specific error model. Success criterion and algebraic sufficient conditions were given. Reference [26] provided an information theoretic approximate error correction criterion. The approximation in these works stems from a *relaxed decoding* procedure. Much closer to our work is [27] (in the context of quantum secret sharing) that used a randomized code to maximize the distance with high probability but the rate is low (of lesser concern in that context). Our construction was inspired by that in [17] in the classical setting. Further comparisons between our work and these earlier results and insights obtained will be discussed in Section V.

After the initial presentation of this result [28], we learned of two independent studies of list codes, both in settings quite different from our own. Reference [29] studied decoding of *classical list codes* with quantum algorithms, and [30] studied list codes for sending *classical* messages via iid quantum channels.

II. Background and Definitions

Our sender, receiver, and adversary will be named Alice, Bob, and Eve, respectively. The encoding of a k-qubit state $|\psi\rangle$ into a QECC will be written as $|\bar{\psi}\rangle$. We call the Pauli group acting on n qubits $\mathcal{G}_n$ and write its elements in the form $P = i^t X^{\mathbf{u}} Z^{\mathbf{v}}$, where $t \in \{0,1,2,3\}, \mathbf{u}, \mathbf{v}$ are binary vectors of length $n, X^{\mathbf{u}}$ $(Z^{\mathbf{v}})$ denotes $X^{u_1} \otimes \cdots \otimes X^{u_n}$ $(Z^{v_1} \otimes \cdots \otimes Z^{v_n})$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The (anti)commutation relation between $P_1, P_2 \in \mathcal{G}_n$ is determined by $P_1 P_2 = (-1)^{\omega(P_1,P_2)} P_2 P_1$ with $\omega(P_1,P_2) = \mathbf{u}_1 \cdot \mathbf{v}_2 + \mathbf{u}_2 \cdot \mathbf{v}_1$, where the dot products and sum are computed in arithmetic modulo two. We let $\langle P_l \rangle$ denote the subgroup of $\mathcal{G}_n$ generated by a set of Pauli elements $\{P_l\}$.

A state $|\psi\rangle$ is said to be stabilized by a Pauli matrix P when $P|\psi\rangle = |\psi\rangle$. An $[n,k]$ stabilizer code is a 2^k-dimensional space of n-qubit states simultaneously stabilized by all elements of a size 2^{n-k} Abelian subgroup of $\mathcal{G}_n$. The abelian subgroup is typically called S and is referred to as the code's stabilizer, and has $n-k$ generators denoted by $\{S_i\}_{i=1}^{n-k}$. For any $E \in \mathcal{G}_n$ we refer to the $(n-k)$-bit string $\omega(E, S_i)$ as the syndrome of E [20], [31]. The weight of a Pauli matrix P, which we denote by $\mathrm{wt}(P)$, is the number of qubits on which P acts nontrivially, and we call a stabilizer code an $[n,k,d]$ code if it can detect all errors outside of S of weight less than the distance d, which is equivalent to being able to correct all errors of weight less than $\lfloor (d-1)/2 \rfloor$. For any positive real number r, let $\mathcal{E}^r$ be the set of Pauli matrices of weight no more than $\lfloor r \rfloor$. Let $N(S)$ be the set of all unitaries leaving S invariant under conjugation. ($N(S)$ is the center and also the normalizer of S in $\mathcal{G}_n$, thus the symbol N.) Note that two errors E_i and E_j have the same syndrome if and only if $E_i^{\dagger} E_j \in N(S)$. Thus S defines an $[n,k,d]$ code exactly when every pair of errors $E_i, E_j \in \mathcal{E}^{(d-1)/2}$ satisfies $E_i^{\dagger} E_j \notin N(S) - S$. Intuitively, it means that the syndrome can be used to identify all errors of concern up to a multiplicative factor that is in S and has no effect on the codespace.

We state a property of the Pauli group that will be useful later. For any subgroup G of $\mathcal{G}_n$, for any set s of i *independent* elements in G, and a specific (ordered) list of i (anti)commutation relations with elements of s, exactly $|G|/2^{-i}$ elements of G will satisfy those relations.

Definition 1: The n-qubit adversarial quantum channel with error rate p, which we call $\mathcal{N}_{p,n}^{\mathrm{adv}}$, acts on a state of n qubits, ρ, and is of the

[1] It is folklore, somewhat implicit in the hashing protocol of [23]. It is also implied by our current construction.

form

$$\begin{aligned}\mathcal{N}^{\mathrm{adv}}_{p,n}(\rho) &= \sum_i A_i \rho A_i^\dagger \quad \text{with } A_i \\ &= \sum_{E \in \mathcal{E}^{pn}} \alpha^i_E E \end{aligned} \tag{1}$$

subject to the requirement that $\sum_i A_i^\dagger A_i = I$ and where $\mathcal{E}^{np} = \{E \in \mathcal{G}_n | wt(E) \leq pn\}$ is as defined before. The particular choice of the $\{A_i\}$'s is made by Eve only after Alice and Bob have decided on a communication strategy.

Notice that to communicate effectively over $\mathcal{N}^{\mathrm{adv}}_{p,n}$ one must find a strategy that works with high fidelity for *all* channels described by (1). To do this, we will use quantum list codes, which are defined below.

Definition 2: We say that an $[n,k]$ stabilizer code, $\mathcal{C}$, is an $[n,k,t,L]$-list code if there is a decoding operation, $\mathcal{D}$, such that for every $E_i \in \mathcal{E}^t$ and $|\bar{\psi} \in \mathcal{C}$, the decoded k-qubit state, along with the syndrome s, is given by $\mathcal{D}(E_i|\bar{\psi}\rangle\langle\bar{\psi}|E_i^\dagger) = \sum_s \sum_j A_j^s |\psi\rangle\langle\psi| A_j^{s\dagger} \otimes |s\rangle\langle s|$ where $\sum_{sj} A_j^{s\dagger} A_j^s = I$, and each A_j^s is a linear combination of the 2^L elements of $\langle P_l^s \rangle_{l=1}^L$, where $\{P_l^s\}_{l=1}^L$ is a list of logical errors on the codespace and $\langle P_l^s \rangle_{l=1}^L$ is the group they generate.

Note that in the above definition, the set $\{P_l^s\}_{l=1}^L$ generating the error list depends on the syndrome s.

III. Quantum List Codes

We now show that, asymptotically, there exist $[n,k,t,L]$-list codes with favorable parameters. We proceed by considering random stabilizer codes, arguing along the lines of [23] and [20]. In particular, we will show that if we choose a random stabilizer code with rate as below, in the limit of large n the probability of it failing to be L-list decodable is less than 1.

Theorem 3: $[n, \lfloor Rn \rfloor, \lfloor pn \rfloor, L]$-list codes exist for sufficiently large n and for

$$R < 1 - \left(1 + \frac{1}{L}\right)(H(p) + p\log 3). \tag{2}$$

Proof: Let $N_E = |\mathcal{E}^{pn}|$ and $\mathcal{E}^{pn} = \{E_i\}_{i=1}^{N_E}$. Since two errors E_i and E_j have the same syndrome iff $E_i^\dagger E_j \in N(S)$, a code will fail to be L-list decodable only if there are $L+1$ *independent* errors $E_0, \ldots, E_L$ outside of S having the same syndrome. Mathematically, this means $E_i^\dagger E_j \in N(S)$ for $0 \leq i,j \leq L$ (or equivalently, $E_0^\dagger E_j \in N(S)$ for $1 \leq j \leq L$). The proof consists of two steps: (1) bounding the probability (over the code) for a fixed list of L independent Pauli matrices to be in $N(S)$, and (2) taking the union bound over all such possible lists to show that list-decoding will fail with probability (over the code) *strictly* less than 1. Thus, the desired list code must exist.

Step (1) is essentially a counting argument. How many ways can we choose $n-k$ stabilizer generators $S_1, S_2, \ldots S_{n-k}$? Here we omit overall factors of $\pm 1, i$, but we count different generating sets (for the same code) and different orderings.[2] There are two constraints for the generating set, commutivity and independence. S_1 can be chosen from any of the $2^{2n}-1$ nontrivial Pauli matrices. Recall the property of $\mathcal{G}_n$ stated in the previous section. S_2 can be chosen from the 2^{2n-1} Pauli matrices commuting with S_1 but must be chosen from outside of the multiplicative group generated by S_1, thus there are $2^{2n-1}-2$ choices. Similarly, each S_i is chosen from the $2^{2n-(i-1)}$ Pauli matrices commuting with $S_1, \ldots, S_{i-1}$ but not from the multiplicative group generated by them, so there are $2^{2n-(i-1)} - 2^{i-1}$ choices. Thus, there are $\Pi_{a=0}^{n-k-1}(2^{2n-a}-2^a)$ distinct generating sets.

Now, for an arbitrary and fixed list $E_0, \ldots, E_L$ of independent errors, how many choices of stabilizer generators will give a code with $\{E_0^\dagger E_j\} \in N(S) \forall j{=}1, \ldots, L$? This counting is similar to the above, but now $S_1, S_2 \ldots S_{n-k}$ are constrained to commute with $\{E_0^\dagger E_j\}$, in addition to the two original constraints. In other words, S_1 can be chosen from the $2^{2n-L}-1$ nontrivial Pauli operators commuting with the $E_0^\dagger E_j$, and S_2 has $2^{2n-L+1}-2$ choices, and so on. Thus, there are $\Pi_{a=0}^{n-k-1}(2^{2n-L-a}-2^a)$ sets of stabilizer generators that commute with all of $E_0^\dagger E_j$.

Putting together with the two stabilizer counts, one unconstrained and the other with the same syndrome for $\{E_j\}_{j=0,\ldots,L}$, the latter has probability

$$\frac{\Pi_{a=0}^{n-k-1}(2^{2n-L-a}-2^a)}{\Pi_{a=0}^{n-k-1}(2^{2n-a}-2^a)} \leq 2^{-L(n-k)}. \tag{3}$$

For step (2), we apply the union bound for the choice of the $L+1$ E_j's. The probability that a random $[n,k]$ code is not L-list decodable is less than $\binom{N_E}{L+1} 2^{-L(n-k)}$, which is no more than $N_E^{L+1} 2^{-L(n-k)}$. The latter is less than 1 if $k < n - (1+\frac{1}{L})\log N_E$. But $N_E = |\mathcal{E}^{pn}| = \sum_{r=0}^{\lfloor np \rfloor} 3^r \binom{n}{r}$. For any $\delta > 0, \exists n_\delta$ s.t. whenever $n \geq n_\delta, \log N_E \leq n(H(p)+p\log 3+\delta/3)$ so choosing $k = n[1-(1+\frac{1}{L})(H(p)+p\log 3)-2\delta/3]$ finishes the proof. □

IV. Coding Strategy

Theorem 3 tells us that for any $R < 1-H(p)-p\log 3$, there exist $[n, Rn, pn, L]$-list codes for large enough n and L. For example, we can choose the various parameters as $\delta = 1-H(p)-p\log 3 - R, L \geq \frac{3}{\delta}(H(p)+\log 3)$, and $n \geq n_\delta$ in Theorem 3). Note that L does not grow with n.

We now fix such a list-code, $\mathcal{C}^{n,L}$. This *always* returns a syndrome s, a corresponding list of errors $Q_f^s \in \langle P_l^s \rangle$, and a list-decoded state of the form $\sum_i B_i^s |\psi\rangle\langle\psi| B_i^{s\dagger} = \mathcal{N}^s(|\psi\rangle\langle\psi|)$, where $|\psi\rangle$ is the sender's intended logical state, $\sum_i B_i^{s\dagger} B_i^s = I$, and each B_i^s is in the span of Q_f^s. Note that list-decoding removes all superposition between errors with different syndromes. Also, no approximation has been made so far.

Now we add a few more stabilizer generators to $\mathcal{C}^{n,L}$ so that with high probability (over the choice of the extra generators) the receiver can decode $|\psi\rangle$ unambiguously. These generators are determined by a secret key shared by the sender and receiver, making them unknown to the adversary.

It will follow from the proof of Theorem 4 below that adding $(1/\log(4/3))(2L + \log(1/\eta))$ random generators to the code $\mathcal{C}^{n,L}$ would allow us to distinguish among the $\{Q_f^s\}_{j=1}^{2^L}$ possible errors, with probability at least $1-\eta$. This would require $2n(2L+\log(1/\eta))/\log(4/3)$ bits of shared key.

A much smaller key can be used if small-biased sets are used to choose these extra stabilizers pseudorandomly [32], [33]. A subset of $\{0,1\}^m$, denoted A, is said to be an η-biased set of *length m* if for each $e \in \{0,1\}^m$, roughly half of the elements of A have odd/even parity with e, or mathematically, $|\Pr_{a\in A}(e\cdot a = 0) - \Pr_{a \in A}(e \cdot a = 1)| \leq \eta$. There are efficient constructions of η-biased sets of length m with only $O(\frac{m^2}{\eta})$ elements [32], [33].

Let G_0 be the set of stabilizer generators of $\mathcal{C}^{n,L}$. We add K extra stabilizer generators $T_1, \ldots, T_K$. When j of these have been added, denote the code by $\mathcal{C}_j^{n,L}$, with $k-j$ encoded qubits and generator set

[2] Our analysis revolves around random stabilizer generators rather than random codes. As an aside, the resulting code is also randomly distributed. Also, any stabilizer of size 2^{n-k} has $\prod_{b=0}^{n-k-1}(2^{n-k-b}-1)$ different generating sets, so we have also found the total number of stabilizers codes of this size.

G_j. (Each $\mathcal{C}_j^{n,L}$ is a subcode of $\mathcal{C}_{j-1}^{n,L}$.) The next generator T_{j+1} has to commute with all of G_j but not be generated by it, thus, it is an encoded operation on the code $\mathcal{C}_j^{n,L}$. Without loss of generality, it is an encoded Pauli operation on the encoded $k-j$ qubits, and can be chosen according to a random element of an η-biased set A_{j+1} of length $2(k-j)$. The following theorem shows that using this procedure to add $K = O(L \log 1/\eta)$ stabilizers allows the receiver to reconstruct the encoded state with high probability. Using the efficient constructions of η-biased sets of length $m \leq 2n$ with only $O(\frac{n^2}{\eta})$ elements, our construction requires $O((2L + \log(1/\eta)) \log(n^2/\eta))$ bits of key.

Theorem 4: Let $\mathcal{C}^{n,L}$ be an $[n, Rn, pn, L]$-list code of rate R and let $\mathcal{C}_K^{n,L}$ be the code obtained from $\mathcal{C}^{n,L}$ by progressively adding $K = (1/\log(4/3))(2L + \log(1/\eta))$ stabilizers determined by η-biased sets $A_1, \ldots, A_K$ (of decreasing length) as described above. By using a secret key of fewer than $O(K(\log(\frac{n^2}{\eta})))$ bits to select $\mathcal{C}_K^{n,L}$, $nR - K = n(R - o(n))$ qubits can be sent over $\mathcal{N}_{p,n}^{\mathrm{adv}}$ with fidelity at least $1 - \eta$ for all $\eta < 1/2$.

Proof: The $[n, Rn, pn, L]$-list code reduces the adversary's power to choosing some $\mathcal{N}^s$ (with operation elements in the span of $\{Q_f^s\}_{f=1}^{2L} = \langle P_l^s \rangle$) and a distribution of s. So, if for each s, the probability (over the choice of $T_1, \ldots, T_K$) is less than ϵ to fail to distinguish between the $\{Q_f^s\}_{f=1}^{2L}$, the fidelity of the decoded state with the original will be at least $1 - \epsilon$. More specifically, fix an arbitrary s. It is shown in [34] that $\mathcal{N}^s$ has a χ-representation $\mathcal{N}^s(\rho) = \sum_{f,f'} \chi_{f,f'} Q_f^s \rho (Q_{f'}^s)^\dagger$ and let

$$F_s = \left\{ k | \exists_{f,f'} \omega\left(T_l^k, Q_f^s\right) = \omega\left(T_l^k, Q_{f'}^s\right) \right\} \tag{4}$$

be the set of key values for which the additional stabilizer generators fail to determine the list element. Then, letting $|\psi_k\rangle$ be the encoded logical state and $\mathcal{D}_k^s$ be the decoding operation given list s and key k, our decoded state is

$$\begin{aligned} \frac{1}{K} \sum_{k=1}^{K} & \mathcal{D}_k^s(\mathcal{N}^s(|\psi_k\rangle\langle\psi_k|)) \\ &= \frac{1}{K} \sum_{k \notin F_s} \mathcal{D}_k^s(\mathcal{N}^s(|\psi_k\rangle\langle\psi_k|)) \\ &\quad + \frac{1}{K} \sum_{k \in F_s} \mathcal{D}_k^s(\mathcal{N}^s(|\psi_k\rangle\langle\psi_k|)) \\ &= (1 - \Pr(F_s))|\psi\rangle\langle\psi| + \Pr(F_s)\phi_s \end{aligned} \tag{5}$$

where $\phi_s = \frac{1}{K \Pr(F_s)} \sum_{k \in F_s} \mathcal{D}_k^s(\mathcal{N}^s(|\psi_k\rangle\langle\psi_k|))$ is the state conditional on the key failing to distinguish the list elements properly. We will now show that $\Pr(F_s)$ can be made less than ϵ for all lists of length 2^L by choosing K as in the theorem. This results in a decoding fidelity of at least $1 - \epsilon$.

Now fix f, f' and define the events M_j as $\{\omega(Q_f^s, T_j) = \omega(Q_{f'}^s, T_j)\}$. Then, the probability, over the choices of $T_{1,\ldots,K}$, that they assign the same syndrome to Q_f^s and $Q_{f'}^s$ is $\Pr(\cap_{j=1}^K M_j) = \prod_{j=1}^K \Pr(M_j | M_{j-1} \ldots M_1)$. Since each T_j is chosen using an η-biased string of encoded operations of the code $\mathcal{C}_{j-1}^{n,L}$, we have $\Pr(M_j | M_{j-1} \ldots M_1) \leq \frac{1+\eta}{2}$, which immediately implies that $\Pr(\cap_{j=1}^K M_j) \leq (\frac{1+\eta}{2})^K$. By a union bound over the choice of f, f', the probability of *any* pair having the same commutation relations for all j is less than $2^{2L}(\frac{1+\eta}{2})^K$.

By choosing $\eta \leq 1/2, K = (1/\log(4/3))(2L + \log(1/\eta))$ we make this failure probability less than ϵ so that with probability at least $1 - \epsilon, Q_f^s$ can be unambiguously identified and the state reconstructed. □

Note that ϵ can be made to vanish exponentially with n without incurring extra n-dependence on the key size.

In Theorem 4, the extra generators can distinguish the worst case $\mathcal{N}^s$ and no union bound over s is needed. Furthermore, the additional stabilizers do *not* depend on s. It means that the final construction is a single quantum error correcting code depending only on a small key. It also means that it is not necessary to first perform list-decoding before selecting the extra stabilizers. The combined decoding operation is independent of s but concludes the error based on the joint inputs of s and the extra syndrome bits (one possible way of which is to first output a list based on s).

V. Discussion

We have introduced the adversarial quantum channel and shown that using a logarithmic length secret key one can communicate over this channel with a rate of $1 - H(p) - p \log 3$. This is far higher than would be naively expected from existing QECC's, and quite close to the best known rates for independent depolarizing channels of error probability p. Our construction involves quantum list codes, which we defined and showed to exist with favorable parameters. Classical list decoding has recently played an important role in several complexity theoretic results (for a review, see [35]), and we expect quantum list codes will be similarly useful in the context of quantum complexity theory.

The scenario considered in this paper and the spirit of our protocols are closely related to those of [27]. Comparing their result with ours points to interesting open questions. Reference [27] constructed *approximate* quantum error correcting codes of length n capable of correcting up to $(n-1)/2$ errors with high probability (compared to at most $n/4$ correctable errors for an exact code). Thus, the fraction of errors that can be tolerated in [27] approaches $1/2$ as n gets large, which is much higher than in our scheme. Furthermore, unlike our scheme, no secret key is required. Instead, randomizing parameters are sent as part of the message via carefully constructed secret sharing schemes. However, the alphabet size of the codes in [27] grows as a function of both the blocklength and the code's accuracy which severely limits the transmission rate. Also, when their large dimensional channel is viewed as a block of qubit channels, the adversary considered in [27] is much more restricted than ours, being limited to the corruption of *contiguous blocks* of qubits.

Altogether, there is a general open question on the tradeoff between distance, rate, and key required for a code. More specifically, it is an interesting question whether there are *qubit* approximate QECCs which achieve the rates of our codes without using a secret key, or, less ambitiously, one with constant size. We have also left unanswered the capacity of $\mathcal{N}_{p,n}^{\mathrm{adv}}$ assisted by a negligible length secret key. It seems plausible that the capacity is equal to that of the depolarizing channel with error rate p, which would be in analogy with the classical result of [17]. While the capacity of for the depolarizing channel is an open question, one may find codes for $\mathcal{N}_{p,n}^{\mathrm{adv}}$ with rates matching the best known for the depolarizing channel. It will also be interesting to consider other side resources such as a negligible amount of entanglement. Finally, unlike DMC's, it is unclear for adversarial channels whether the capacity can be improved with a small number of uses of noiseless quantum channels.

As a side remark, our scheme uses the secret key as a randomizing parameter that is inaccessible to the adversary. Since the adversary must corrupt the transmitted state before it is received by Bob, if Bob is allowed to send a "receipt" of the quantum states to Alice, she can simply disclose the random code afterwards and no key is required. In other words, one bit of back communication along with logarithmic forward classical communication (all authenticated) can replace the key requirement.

As another side remark, as the channel can be used to create entanglement, the key used in the communication can be replenished by sending a negligible number of EPR pairs (without affecting the communication rate). Thus the key requirement is only catalytic.

Our result also finds application to a related problem—entanglement distillation with bounded weight errors. In this problem, a state is already distributed between Alice and Bob, so the adversary has already acted and randomizing parameters can be sent in public without a receipt. In [36], it was shown that n noisy EPR pairs with errors of weight up to pn could be purified to $n(1-H(p)-p\log 3)$ perfect EPR pairs by a two-way distillation procedure. Our construction lets us distill high fidelity EPR pairs at the same rate with only forward classical communication. In fact, it was suggested in [36] that quantum list codes could be used to reduce the computational complexity of their protocols—almost exactly the approach taken here, though in our case with an eye toward reducing the communication required. The question of efficent encoding and decoding via list codes has not yet been resolved.

It may also be interesting to consider how restricting the computational power of our adversary affects the channel's capacity, which is another topic we leave to future work. The investigation of other restrictions (such as causality of the adversarial channel) is also natural in certain situations and may lead to additional insights.

Acknowledgment

The authors are grateful to Roberto Oliveira, John Smolin, Daniel Gottesman, and especially Aram Harrow for helpful discussions, as well as to the IBM T. J. Watson Research Center, where the bulk of this work was completed.

References

[1] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, 2005.

[2] I. Devetak, A. W. Harrow, and A. Winter, "A family of quantum protocols," *Phys. Rev. Lett.*, vol. 93, p. 230505, 2004.

[3] I. Devetak and P. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Comm. Math. Phys.*, vol. 256, no. 2, pp. 287–303, 2005.

[4] P. W. Shor, "The quantum channel capacity and coherent information," MSRI Workshop on Quantum Computation, ser. Lecture Notes, , 2002 [Online]. Available: http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/

[5] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2481–2485, 1999.

[6] A. Winter, ""Extrinsic" and "intrinsic" data in quantum measurements: Asymptotic convex decomposition of positive operator valued measures," *Commun. Math. Phys.*, vol. 244, pp. 157–185, 2004.

[7] H. Barnum, E. Knill, and M. A. Nielsen, "On quantum fidelities and channel capacities," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1317–1329, 2000.

[8] B. Schumacher and M. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.

[9] A. Holevo, "The capacity of quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, pp. 269–273, 1998, arXiv:quant-ph/9611023.

[10] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, pp. 1613–1622, 1997.

[11] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2637–2655, 2002.

[12] G. Bowen, I. Devetak, and S. Mancini, "Bounds on classical information capacities for a class of quantum memory channels," *Phys. Rev. A.*, vol. 71, p. 034310, 2005, arXiv quant-ph/0312216.

[13] D. Kretschmann and R. F. Werner, "Quantum channels with memory," *Phys. Rev. A*, vol. 72, p. 062323, 2005.

[14] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1753–1768, 2003.

[15] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Swiss Federal Institute of Technology, Lausanne, Switzerland, 2005.

[16] G. Bowen and N. Datta, Beyond i.i.d. in Quantum Information Theory.

[17] M. Langberg, "Private codes or succinct random codes that are (almost) perfect," *Proc. FOCS*, pp. 325–334, 2004.

[18] V. Guruswami, "List decoding with side information," in *Proc. IEEE Conf. Comput. Complex.*, 2003, pp. 300–309.

[19] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, pp. 147–160, 1950.

[20] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," Ph.D. dissertattion, California Institute of Technology, Pasadena, CA.

[21] E. Rains, "Quantum shadow enumerators," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2361–2366, 1999.

[22] E. Rains, "New asymptotic bounds for self-dual codes and lattices," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1261–1274, 2003.

[23] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A.*, vol. 54, pp. 3824–3851, 1996.

[24] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000.

[25] D. Leung, M. Nielsen, I. Chuang, and Y. Yamamoto, "Approximate quantum error correction can lead to better codes," *Phys. Rev. A*, vol. 56, pp. 2567–2573, 1997.

[26] B. Schumacher and M. D. Westmoreland, "Approximate quantum error correction," *Quantum Inf. Process.*, vol. 1, 2002.

[27] C. Crepeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," *Adv. Crypt.—EUROCRYPT*, 2005.

[28] G. Smith, Communicating Over Adversarial Quantum Channels. Paris, France, [Online]. Available: http://www.lri.fr/qip06/slides/smith.pdf, 2006

[29] A. Kawachi and T. Yamakami, Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding, arxiv preprint: quant-ph/0602088.

[30] M. Hayashi, Channel Capacities of Classical and Quantum List Decoding, arxiv preprint: quant-ph/0603031.

[31] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge, 2004.

[32] J. Naor and M. Naor, "Small-bias probability spaces: Efficient constructions and applications," in *Proc. ACM Symp. Theory Comput.*, 1990, pp. 213–223.

[33] N. Alon, O. Goldreich, J. Hastad, and R. Peralta, "Simple constructions of almost k-wise independent random variables," in *Proc. IEEE Symp. Found. Comput. Sci.*, 1990, pp. 544–553.

[34] M. Nielsen and I. Chuang, Prescription for Experimental Determination of the Dynamics of a Quantum Black Box, arxiv preprint: quant-ph/9610001.

[35] M. Sudan, "List decoding: Algorithms and applications," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer, 2000, vol. 1872, p. 25.

[36] A. Ambainis and D. Gottesman, "The minimum distance problem for two-way entanglement purification," *IEEE Trans. Inf. Theory*, vol. 52, pp. 748–753, 2006.