Short random circuits define good quantum error correcting codes

Winton Brown
Département de Physique
Université de Sherbrooke, Canada
Email: winton.brown@usherbrooke.ca

Omar Fawzi
Institute for Theoretical Physics
ETH Zuerich, Switzerland
Email: ofawzi@phys.ethz.ch

Abstract—**We study the encoding complexity for quantum error correcting codes with large rate and distance. We prove that random Clifford circuits with $O(n \log^2 n)$ gates can be used to encode k qubits in n qubits with a distance d provided $\frac{k}{n} < 1 - \frac{d}{n} \log_2 3 - h(\frac{d}{n})$. In addition, we prove that such circuits typically have a depth of $O(\log^3 n)$.**

I. INTRODUCTION

Error-correcting codes are fundamental objects with many theoretical and practical applications. In the context of quantum information, quantum error correcting codes allow the preservation of quantum data in the presence of noise; see [12] for a reference. In addition to their application to reliable communication and computation, quantum error correcting codes have found applications in cryptography such as quantum key distribution [18] and secret sharing [7]. In this paper, a quantum error correcting code is a subspace of the Hilbert space associated with an n-qubit space. Such a code has two important parameters: the number of qubits k that can be encoded in this subspace and the distance d which quantifies the number of errors that can be corrected by the code. It is desirable to have both k and d as large as possible.

Our objective here is to understand how efficient the encoders of good quantum error correcting codes can be. This question has been studied for classical codes in several computation models, see e.g., [1], [11]. In this paper, we work in the circuit model with a gate set composed of all two-qubit gates. In this model it is simple to see that to obtain a linear distance, a linear number of gates are needed and the depth has to be at least $\Omega(\log n)$. On the other hand, it is known that a large family of quantum error correcting codes known as stabilizer codes, which include many good codes, can have an encoder using only $O(n^2)$ gates [6].

Specifically, the encoders we consider here are constructed by choosing a circuit at random with a given number of gates. Random quantum circuits have been well studied in the quantum information literature. Random quantum circuits of polynomial size are meant to be efficient implementations that inherit many useful properties of "uniformly" chosen unitary transformations, which are typically very inefficient. Most of the work has been in analyzing convergence properties of the random circuit model [10], [9], [17], [13], [4]. In some sense, we are here also interested in the convergence properties because our aim is to show that short random circuits define

codes that are as good as the codes defined by completely random Clifford unitaries.

A. Results

We prove that random quantum circuits with $O(n \log^2 n)$ gates can be used to encode k qubits in n qubits with a distance d provided $\frac{k}{n} < 1 - \frac{d}{n} \log_2 3 - h(\frac{d}{n})$. This is asymptotically the same as the distance of a code defined by a random unitary from the complete Clifford group, which is known to achieve the quantum Gilbert-Varshamov bound [5], [12]. But a typical Clifford unitary is only known to be computable using a circuit with $\Omega(n^2)$ gates.

We also study another complexity measure for circuits which is the depth. The depth is simply the number of time steps needed to evaluate the circuit, keeping in mind that gates acting on disjoint qubits can be executed simultaneously. By parallelizing the random quantum circuit mentioned in the previous paragraph, we prove the existence of codes achieving the same parameters with an encoding of depth $O(\log^3 n)$ and size $O(n \log^2 n)$. We remark that it was proved in [15] that the encoding and decoding operation of any stabilizer code can be implemented with quantum circuits of depth $O(\log n)$ using $O(n^2)$ qubits of ancilla, i.e., qubits in some fixed state that are restored to their original state at the end of the computation. In contrast, random quantum circuits do not use any ancilla qubits.

We say here a brief word on the proof. The first step of the proof is to relate the property of interest, which is the distance of the code, to the second moment operator of the random quantum circuit. This operator can then be studied as a Markov chain and the distance of the code translates to a property of the Markov chain. The convergence times of such Markov chains arising from the second order moments have been previously studied in [17], [13]. However, these convergence times are not sufficient to prove the result we are aiming for and can only give useful bounds when $\Omega(n^2)$ gates are applied. Instead, we analyze the Markov chain in a finer way without using the spectral gap and bound the probabilities of going from a state ℓ to state m within $O(n \log^2 n)$ steps as a function of ℓ and m.

II. PRELIMINARIES

A. Generalities

The state of a pure quantum system is represented by a unit vector in a Hilbert space. Quantum systems are denoted $A, B, C \ldots$ and are identified with their corresponding Hilbert spaces. The Hilbert spaces we consider here will be n-qubits spaces of the form $(\mathbb{C}^2)^{\otimes n}$. A density operator is a Hermitian positive semidefinite operator with unit trace. The density operator associated with a pure state is abbreviated by omitting the ket and bra $\psi \overset{\text{def}}{=} |\psi\rangle\langle\psi|$. For an introduction to quantum information, we refer the reader to [16], [19].

Throughout the paper, we use the Pauli basis to decompose operators. The 2×2 Pauli operators can be represented as follows:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For a string $\nu \in \{0,1,2,3\}^n$, we define $\sigma_\nu = \sigma_{\nu_1} \otimes \cdots \otimes \sigma_{\nu_n}$. The support $\mathrm{supp}(\nu)$ of ν is simply the subset $\{i \in [n] : \nu_i \neq 0\}$ and the weight $w(\nu) = |\mathrm{supp}(\nu)|$. Any operator acting on $(\mathbb{C}^2)^{\otimes n}$ can be represented as

$$T = \frac{1}{2^n} \sum_{\nu \in \{0,1,2,3\}} \mathrm{tr}[\sigma_\nu T] \sigma_\nu.$$

B. Quantum error correcting codes

As we are interested in the encoding complexity of quantum error correcting codes, we describe codes using the encoding operation. The encoding operation is a unitary transformation on an n-qubit space that we decompose as $A \otimes B$. It takes as input a k-qubit state $|\psi\rangle \in A$ (the state to be encoded) and the remaining input qubits are set to $|0\rangle^{\otimes n-k} \in B$. Such a code is called an $[n,k]$ quantum error correcting code. See Figure 1 for an illustration.
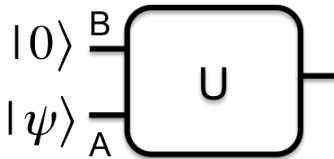

Fig. 1. Encoding the state $|\psi\rangle$ using the encoder U

For an encoding unitary U, the code space is defined as the vector space $\{U|\psi\rangle|0\rangle^{\otimes n-k} : |\psi\rangle \in (\mathbb{C}^2)^{\otimes k}\}$. By considering a basis $\{|x\rangle : x \in \{0,1\}^k\}$ of A, we obtain a basis $\{|\bar{x}\rangle = U|x\rangle \otimes |0\rangle^{\otimes n-k} : x \in \{0,1\}^{n-k}\}$ of the code space. A code has distance at least $d+1$ if we have for all $x, y \in \{0,1\}^k$ and all $\mu \in \{0,1,2,3\}^n$ with $1 \leq w(\mu) \leq d$

$$\langle\bar{x}|\sigma_\mu|\bar{y}\rangle = C_\mu \delta_{xy} \tag{1}$$

for some real numbers C_μ depending only on μ and not on x, y [2], [14]. Here, $\delta_{xy} = 1$ if $x = y$ and zero otherwise. A code with minimum distance $2e + 1$ can correct e errors.

We can describe a unitary transformation (and more generally any superoperator) by describing how it acts on the Pauli basis, i.e., $U\sigma_\nu U^\dagger$ for all $\nu \in \{0,1,2,3\}^n$. This is especially convenient when talking about stabilizer codes for which the encoding operation U belongs to the Clifford group. The Clifford group $\mathcal{C}_n$ is defined as the set of unitary transformation U under which the Pauli basis remains invariant up to phases. More precisely $\mathcal{C}_n = \{U : U\sigma_\nu U^\dagger \in \pm\{\sigma_\mu, \mu \in \{0,1,2,3\}^n\}\}$. Note that any unitary in $\mathcal{C}_n$ can be implemented using Hadamard gates, phase gates and CNOT gates. When the encoding unitary $U \in \mathcal{C}_n$, the minimum distance can be simply characterized as shown by the following proposition.

Proposition II.1. *A unitary $U \in \mathcal{C}_n$ defines a quantum error correcting code of distance at least $d+1$ if and only if d is the largest integer such that for all $\nu_A \in \{0,1,2,3\}^k - \{0\}$ and $\nu_B \in \{0,3\}^{n-k}$ and all $\mu \in \{0,1,2,3\}^n$ of weight $1 \leq w(\mu) \leq d$*

$$\mathrm{tr}[\sigma_\mu U \sigma_{\nu_A} \otimes \sigma_{\nu_B} U^\dagger] = 0. \tag{2}$$

Proof: We start by proving the "if" part. We have

$$\langle\bar{x}|\sigma_\mu|\bar{y}\rangle = \langle x|_A \otimes \langle 0|_B U^\dagger \sigma_\mu U |y\rangle_A \otimes |0\rangle_B$$
$$= \mathrm{tr}\left[\sigma_\mu U |y\rangle\langle x| \otimes |0\rangle\langle 0| U^\dagger\right] \tag{3}$$

But

$$|y\rangle\langle x| = \frac{\delta_{xy}}{2^k}\sigma_0 + \frac{1}{2^k} \sum_{\nu_A \in \{0,1,2,3\}^k, \nu_A \neq 0} \mathrm{tr}[\sigma_{\nu_A}|y\rangle\langle x|]\sigma_{\nu_A},$$

$$|0\rangle\langle 0|^{\otimes n-k} = \frac{1}{2^{n-k}} \sum_{\nu_B \in \{0,3\}^{n-k}} \sigma_{\nu_B}. \tag{4}$$

Plugging these expressions into (3), this shows that if condition (2) holds, then condition (1) holds with $C_\mu = \mathrm{tr}\left[\sigma_\mu U \frac{\sigma_0}{2^k} \otimes |0\rangle\langle 0| U^\dagger\right]$.

For the "only if" part, assume U satisfies the condition (1). Write

$$\sigma_{\nu_A} = \sum_{x,y \in \{0,1\}^k} \sigma_{\nu_A}(x,y)|x\rangle\langle y|.$$

Thus, if $1 \leq w(\mu) \leq d$,

$$\mathrm{tr}[\sigma_\mu U \sigma_{\nu_A} \otimes |0\rangle\langle 0| U^\dagger]$$
$$= \sum_{x,y \in \{0,1\}^k} \sigma_{\nu_A}(x,y) \mathrm{tr}\left[\sigma_\mu U |x\rangle\langle y| \otimes |0\rangle\langle 0| U^\dagger\right]$$
$$= \sum_{x,y \in \{0,1\}^k} \sigma_{\nu_A}(x,y) C_\mu \delta_{xy}$$
$$= 0,$$

because $\mathrm{tr}[\sigma_{\nu_A}] = \sum_x \sigma_{\nu_A}(x,x) = 0$. Moreover, recall (4) and note that U transforms Pauli operators to Pauli operators. As a result, we have that $\mathrm{tr}[\sigma_\mu U \sigma_{\nu_A} \otimes |0\rangle\langle 0| U^\dagger] = 0$ implies that for all $\nu_B \in \{0,3\}^{n-k}$, $\mathrm{tr}[\sigma_\mu U \sigma_{\nu_A} \otimes \sigma_{\nu_B} U^\dagger] = 0$. ∎

Consider a Pauli string $\nu_A \nu_B$ of weight for example 1. A two-qubit gate can increase the weight of this Pauli string by at most 1 and thus any code should have at least as many gates as its distance. Also as the weight of a Pauli string can be multiplied by at most two by a set of two-qubit gates acting on disjoint qubits, the depth of the encoding should be at least the logarithm of the distance.

C. Random quantum circuits

We consider the following simple model for a quantum circuit acting on n qubits. In a sequential random quantum circuit, a random two-qubit gate is applied to a randomly chosen pair of qubits in each time step. Here, the random two-qubit gate is going to be a random Clifford gate in $\mathcal{C}_2$ acting on two qubits.

A model of random circuits of a certain size defines a measure over unitary transformations on n qubits that we call p_{circ}. The second-order moment operator will play an important role in all our proofs. The second-order moment operator is a superoperator acting on two copies of the space of operators acting on the ambient Hilbert space, which is an n-qubit space in our setting. For a measure p over the unitary group, we can define the second moment operator M_p as

$$\mathrm{M}_p[X \otimes Y] = \mathop{\mathbf{E}}_{U \sim p} \left\{ U X U^\dagger \otimes U Y U^\dagger \right\}.$$

Even though we do not use the notion unitary designs here, it is worth pointing out that a distribution p over unitary transformations is called a two-design if $\mathrm{M}_p = \mathrm{M}_{\text{clifford}}$ where clifford is the uniform distribution over the Clifford group [8]. We denote by M_{circ} the moment operator for the distribution obtained by applying one step of the random circuit. It is possible to compute M_{circ} explicitly when a random Clifford gate is applied to a randomly chosen pair i, j of qubits, see e.g., [13, Section 3.2]. We have

$$\mathrm{M}_{\text{circ}} = \frac{1}{n(n-1)} \sum_{i \neq j} \mathrm{m}_{ij},$$

where m_{ij} only acts on qubits i and j and is defined by

$$\mathrm{m}_{ij}[\sigma_\mu \otimes \sigma_{\mu'}] = \begin{cases} 0 & \text{if } \mu \neq \mu' \\ \sigma_0 \otimes \sigma_0 & \text{if } \mu = \mu' = 0 \\ \frac{1}{15} \sum_{\nu \in \{0,1,2,3\}^2, \nu \neq 0} \sigma_\nu \otimes \sigma_\nu & \text{if } \mu = \mu' \neq 0 \end{cases}$$

for all $\mu, \mu' \in \{0,1,2,3\}^2$. We can thus represent the operator M_{circ} in the Pauli basis using the following $4^n \times 4^n$ matrix

$$Q(\mu, \nu) = \frac{1}{4^n} \mathrm{tr}\left[\sigma_\nu \otimes \sigma_\nu \, \mathrm{M}_{\text{circ}}[\sigma_\mu \otimes \sigma_\mu] \right].$$

In fact, it is simple to verify that $\sum_{\nu \in \{0,1,2,3\}^n} Q(\mu, \nu) = 1$ for all μ and so Q can be seen as a transition matrix for a Markov chain over the Pauli strings of length n.

Now for a random circuit with t independent random gates applied sequentially, the second moment operator is simply $\mathrm{M}_{\text{circ}}^t$ and the corresponding matrix in the Pauli basis is also the t-th power of Q. The properties we are interested in can be expressed as quadratic functions of the entries of unitary

transformation defined by the circuit and thus can be computed from the second moment operator. This means that these properties can be completely reduced to studying the evolution of the Markov chain defined by Q.

III. Encoding using random quantum circuits

A. Sequential circuit

The objective of this section is to prove the main result of the paper: a typical circuit with $t = O(n \log^2 n)$ gates defines an encoding into a quantum error correcting code with distance that is basically as good as for random Clifford unitaries. Let h be the binary entropy function defined by $h(x) = -x \log_2 x - (1-x) \log_2(1-x)$.

Theorem III.1 (Good codes with almost linear-size circuits). *For any $\delta > 0$, there exists a constant c such that a random quantum circuit with $cn \log^2 n$ gates defines an $[n, k]$ quantum error correcting code with distance at least $d + 1$ with probability at least*

$$1 - \frac{1}{n^8} - 2^{k - n(1 - h(d/n) - \log_2(3) d/n - 3\delta)}.$$

Proof: We prove this result by using Proposition II.1. Let U_t denote the random unitary computed by choosing t random gates. We can bound the probability that U_t fails to satisfy condition (2).

$$\mathbf{P}\left\{ \exists \nu_A, \nu_B, \mu : w(\mu) \in [1, d], \mathrm{tr}[\sigma_\mu U_t \sigma_{\nu_A} \otimes \sigma_{\nu_B} U_t^\dagger] \neq 0 \right\}$$
$$\leq \sum_{\nu_A, \nu_B} \sum_{\mu : w(\mu) \in [1, d]} \mathbf{P}\left\{ \mathrm{tr}[\sigma_\mu U_t \sigma_{\nu_A} \otimes \sigma_{\nu_B} U_t^\dagger] \neq 0 \right\}.$$

Note that because $U_t \in \mathcal{C}_n$, we have $\mathrm{tr}[\sigma_\mu U_t \sigma_{\nu_A} \otimes \sigma_{\nu_B} U_t^\dagger] = \pm 2^n$ when it is non-zero. This means that

$$\mathbf{P}\left\{ \mathrm{tr}[\sigma_\mu U_t \sigma_{\nu_A} \otimes \sigma_{\nu_B} U_t^\dagger] \neq 0 \right\}$$
$$= \frac{1}{2^n} \mathbf{E}\left\{ \left| \mathrm{tr}[\sigma_\mu U_t \sigma_{\nu_A} \otimes \sigma_{\nu_B} U_t^\dagger] \right| \right\}$$
$$= \frac{1}{2^{2n}} \mathbf{E}\left\{ \mathrm{tr}\left[\sigma_\mu^{\otimes 2} U_t^{\otimes 2} (\sigma_{\nu_A} \otimes \sigma_{\nu_B})^{\otimes 2} (U_t^\dagger)^{\otimes 2} \right] \right\}$$
$$= \frac{1}{4^n} \mathrm{tr}\left[\sigma_\mu^{\otimes 2} \, \mathrm{M}_{\text{circ}}^t \left[(\sigma_{\nu_A} \otimes \sigma_{\nu_B})^{\otimes 2} \right] \right]$$
$$= Q^t(\nu, \mu),$$

where $\nu = \nu_A \nu_B$ is the concatenation of ν_A and ν_B. As a result, the probability that condition (2) fails to hold can be bounded by

$$\sum_{\nu_A \in \{0,1,2,3\}^k, \nu_B \in \{0,3\}^{n-k}} \sum_{\mu : w(\mu) \in [1,d]} Q^t(\nu, \mu)$$
$$= \sum_{\ell=1}^{n} \sum_{\substack{\nu_A \in \{0,1,2,3\}^k, \nu_B \in \{0,3\}^{n-k} \\ w(\nu_A \nu_B) = \ell}} \sum_{m=1}^{d} \sum_{\mu : w(\mu) \in [1,d]} Q^t(\nu, \mu)$$
$$= \sum_{\ell=1}^{n} \sum_{p=0}^{\ell} \binom{k}{p} 3^p \binom{n-k}{\ell - p} \sum_{m=1}^{d} P^t(\ell, m), \quad (5)$$

where we defined the matrix $P(\ell, m) = \sum_{\mu : w(\mu) = m} Q(\nu, \mu)$ for any ν of weight ℓ. It is not hard to see that this expression is

independent of ν. P can be considered as the transition matrix of a Markov chain on $\{1, \ldots, n\}$ and in fact, the probabilities $P(\ell, m)$ can be computed exactly (see [13]):

$$P(\ell, m) = \begin{cases} 1 - \frac{2\ell(3n-2\ell-1)}{5n(n-1)} & \text{if } m = \ell \\ \frac{2\ell(\ell-1)}{5n(n-1)} & \text{if } m = \ell - 1 \\ \frac{6\ell(n-\ell)}{5n(n-1)} & \text{if } m = \ell + 1 \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

In order to evaluate the expression in (5), we analyze the behaviour of the Markov chain when it runs for $O(n \log^2 n)$ steps. One possible route to bounding this expression would be to compute the mixing time of the chain defined by P. The stationary distribution for this chain is quite simple and it is defined as

$$P_{\text{clifford}}(m) = \frac{\binom{n}{m}3^m}{4^n - 1}.$$

The problem with this approach is that it only gives a useful bound whenever $t = \Omega(n^2)$. In fact, this is what is done in [13], which proves that random Clifford circuits with $O(n^2)$ gates are approximate two-designs. To prove our result for circuits of almost linear size, we need to analyze the chain more carefully. In short, the problem with the mixing time is that it is about the worst case starting point. For example, starting at the state $\ell = 1$, it takes more time for the walk to mix, whereas if you start near the state $3n/4$, the distribution is already almost mixed. But an important point to realize is that the number of Pauli strings of low weight is small. So it is not necessary for the bound on $P^t(\ell, m)$ to be equally good for all ℓ. And in fact by analyzing the Markov chain precisely, one can prove the following almost optimal bounds.

Theorem III.2 ([3]). *Let P be the transition matrix of the Markov chain defined in (6). For any constants $\delta \in (0, 1/4), \eta \in (0, 1)$, there exists a constant c such that for $t \geq cn \log^2 n$ and all integers $1 \leq \ell \leq n$ and $1 \leq m \leq 3n/4$, we have for large enough n*

$$P^t(\ell, m) \leq 4^{\delta n} \cdot \frac{\binom{n}{m}3^m}{4^n - 1} + \frac{1}{(3-\eta)^\ell \binom{n}{\ell}} \frac{1}{n^{10}}. \quad (7)$$

Let us state some remarks about this theorem. If instead of a random circuit, we were to apply a completely random Clifford unitary on n qubits, we would have transition probabilities that are independent of ℓ:

$$P_{\text{clifford}}(\ell, m) = \frac{\binom{n}{m}3^m}{4^n - 1}.$$

Also the dependence in ℓ is close to optimal. Starting at state ℓ, there is a probability of roughly $\frac{1}{3^\ell \binom{n}{\ell}}$ to get back to the state 1. And in state 1, there is a probability of $2^{-O(\log^2 n)}$ of staying there for $t = O(n \log^2 n)$ steps.

In order to bound expression (5), we first evaluate $\sum_{p=0}^{\ell} \binom{k}{p}3^p \binom{n-k}{\ell-p}$. We bound this sum simply by finding the p for which it is maximum. In order to do so, note that the

ratio

$$\frac{\binom{k}{p+1}3^{p+1}\binom{n-k}{\ell-p-1}}{\binom{k}{p}3^p\binom{n-k}{\ell-p}} = 3\frac{(k-p)(\ell-p)}{(p+1)(n-k+p-\ell+1)}$$

is a decreasing function of p. Moreover, if we plug $p = \lambda \ell$ with $\lambda = \frac{3k}{n+2k}$ in this expression, we obtain

$$\frac{6k^2\ell - 9k\ell^2 + 3k\ell n}{4k^2 - 2k\ell + 6k^2\ell - 3k\ell^2 + 4kn - \ell n + 3k\ell n + n^2} \leq 1.$$

This means that the maximum occurs for some $p_{\max} \leq \lceil \lambda \ell \rceil$. As a result, we can bound the sum by

$$\sum_{p=0}^{\ell} \binom{k}{p}3^p \binom{n-k}{\ell-p} \leq (\ell+1) \cdot 3^{p_{\max}} \binom{k}{p_{\max}} \binom{n-k}{\ell-p_{\max}}$$

$$\leq (\ell+1) \cdot 3^{\lambda\ell+1} \sum_{p=0}^{\ell} \binom{k}{p} \binom{n-k}{\ell-p}$$

$$= (\ell+1) \cdot 3^{\lambda\ell+1} \binom{n}{\ell}.$$

Note that if $k > (1-\delta)n$, there is nothing to prove because the probability bound given by the theorem is negative. Assuming $k \leq (1-\delta)n$ and choosing η appropriately small to apply Theorem III.2, we obtain

$$\sum_{p=0}^{\ell} \binom{k}{p}3^p \binom{n-k}{\ell-p} \frac{1}{(3-\eta)^\ell \binom{n}{\ell}} \frac{1}{n^{10}} \leq \frac{1}{n^{10}}.$$

Also observe that

$$\sum_{\ell=1}^{n} \sum_{p=0}^{\ell} \binom{k}{p}3^p \binom{n-k}{\ell-p} \leq 2^{n+k} - 1.$$

Combining this with (7) and plugging this into (5), we obtain

$$\sum_{\ell=1}^{n} \sum_{p=0}^{\ell} \binom{k}{p}3^p \binom{n-k}{\ell-p} \sum_{m=1}^{d} P^t(\ell, m)$$

$$\leq \sum_{\ell=1}^{n} \sum_{m=1}^{d} (2^{n+k} - 1) \cdot 4^{\delta n} \cdot \frac{\binom{n}{m}3^m}{4^n - 1} + \frac{1}{n^{10}}$$

$$\leq \frac{1}{n^8} + n4^{\delta n}2^{k-n} \sum_{m=1}^{d} \binom{n}{m}3^m$$

$$\leq \frac{1}{n^8} + 2^{k-n(1-h(d/n)-\log_2(3)d/n-3\delta)} \quad (8)$$

for sufficiently large n. ∎

B. Parallelizing the circuit

In the previous section, the complexity measure for a circuit was the number of two-qubit gates applied. Another important complexity measure for circuits is the depth. The depth is related to the time complexity, or the number of time steps needed in order to execute the circuit. Note that two gates acting on disjoint qubits could in fact be executed simultaneously. For the problem of finding good error correcting codes, a natural question is how small can the depth of encoding circuits be. In this section, we show

that by parallelizing the random quantum circuits considered in the previous section, we obtain with high probability circuits with depth $O(\log^3 n)$. Using Theorem III.1, this proves that typical circuits of polylogarithmic depth define quantum error correcting codes that achieve a distance that is basically as good as the distance of a random stabilizer code.

To construct the parallelized circuit, one keeps adding gates to the current level until there is a gate that shares a qubit with a previously added gate in that level, in which case create a new level and continue. In the following proposition, we prove that by parallelizing a random circuit on n qubits having t gates we obtain with high probability a circuit of depth $O(\frac{t}{n} \log n)$.

Proposition III.3 ([3])**.** *Consider a random sequential circuit composed of t gates where t is a polynomial in n. Then parallelize the circuit as described above. Except with probability n^{-10}, the resulting circuit has depth at most $O\left(\frac{t}{n} \log n\right)$.*

Theorem III.4 (Good codes with low-depth circuits)**.** *For any constant $\delta > 0$ there exist $[n, k]$ stabilizer codes with encoding circuits of depth $O(\log^3 n)$ and size $O(n \log^2 n)$ with a distance of d provided $\frac{k}{n} \leq 1 - h(d/n) - \log_2(3)d/n - 4\delta$ and n is large enough.*

Proof: In the proof of Theorem III.1, we saw that with probability at most $1/3$, a random quantum circuit fails to define a circuit with distance as specified in the statement. Using Proposition III.3, the probability that a random circuit with $t = O(n \log^2 n)$ gates leads to a large depth when parallelized is also at most $1/3$. We conclude that there exists a circuit for which both of these conditions hold. ∎

IV. Conclusion

We have shown that good quantum error correcting codes can have encoding circuits with $O(n \log^2 n)$ gates and depth $O(\log^3 n)$. It is simple to show that $\Omega(n)$ gates are needed as well as a depth of $\Omega(\log n)$. It would be interesting to determine whether these simple lower bounds are achievable. It would also be interesting to study a random circuit model with a more restricted gate set, for example with the Hadamard, phase and CNOT gate. Can we obtain the same result for this gate set?

References

[1] L. Bazzi and S. Mitter, "Endcoding complexity versus minimum distance," *IEEE Trans. Inform. Theory*, vol. 51, no. 6, pp. 2103–2112, 2005.

[2] C. H. Bennett, D. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996, arXiv:quant-ph/9604024.

[3] W. Brown and O. Fawzi, "Decoupling with random quantum circuits," 2013, in preparation. see arXiv:1210.6644 for slightly weaker results.

[4] W. Brown and L. Viola, "Convergence rates for arbitrary statistical moments of random quantum circuits," *Phys. Rev. Lett.*, vol. 104, p. 250501, 2010.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405–408, 1997, arXiv:quant-ph/9605005.

[6] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A*, vol. 56, pp. 76–82, 1997, arXiv:quant-ph/9607030.

[7] R. Cleve, D. Gottesman, and H. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, 1999.

[8] C. Dankert, R. Cleve, J. Emerson, and E. Livine, "Exact and approximate unitary 2-designs and their application to fidelity estimation," *Phys. Rev. A*, vol. 80, no. 1, p. 12304, 2009, arXiv:quant-ph/0606161.

[9] J. Emerson, E. Livine, and S. Lloyd, "Convergence conditions for random quantum circuits," *Phys. Rev. A*, vol. 72, no. 6, p. 060302, 2005.

[10] J. Emerson, Y. Weinstein, M. Saraceno, S. Lloyd, and D. Cory, "Pseudo-random unitary operators for quantum information processing," *Science*, vol. 302, no. 5653, pp. 2098–2100, 2003.

[11] A. Gál, K. Hansen, M. Koucký, P. Pudlák, and E. Viola, "Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates," in *Proc. ACM STOC*, 2012, pp. 479–494.

[12] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, Caltech, 1997, arXiv:quant-ph/9705052.

[13] A. Harrow and R. Low, "Random quantum circuits are approximate 2-designs," *Comm. Math. Phys.*, vol. 291, pp. 257–302, 2009, arXiv:0802.1919v3.

[14] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, p. 900, 1997.

[15] C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes," *SIAM J. Comput.*, vol. 31, no. 3, pp. 799–815, 2002.

[16] M. Nielsen and I. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 2000.

[17] R. Oliveira, O. Dahlsten, and M. Plenio, "Generic entanglement can be generated efficiently," *Phys. Rev. Lett.*, vol. 98, no. 13, p. 130502, 2007.

[18] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000, arXiv:quant-ph/0003004.

[19] M. Wilde, *From Classical to Quantum Shannon Theory*, 2011, arXiv:1106.1445.