Fault tolerance of quantum low-density parity check codes with sublinear distance scaling

Alexey A. Kovalev and Leonid P. Pryadko

Phys. Rev. A **87**, 020304 — Published 28 February 2013

DOI: 10.1103/PhysRevA.87.020304

Fault-Tolerance of "Bad" Quantum Low-Density Parity Check Codes

Alexey A. Kovalev[1] and Leonid P. Pryadko[1]

[1] *Department of Physics & Astronomy, University of California, Riverside, California 92521, USA*

(Dated: February 1, 2013)

We study fault-tolerance of quantum low-density parity check (LDPC) codes such as generalized toric codes with finite rate suggested by Tillich and Zémor. We show that any family of quantum LDPC codes where each syndrome measurement involves a limited number of qubits, and each qubit is involved in a limited number of measurements (as well as any similarly-limited family of classical LDPC codes), where distance scales as a positive power α of the number of physical qubits (α less than one for "bad" codes), has a finite error probability threshold. We conclude that for sufficiently large quantum computers, quantum LDPC codes can offer an advantage over the toric codes.

PACS numbers: 03.67.Lx, 03.67.Pp, 64.60.ah

A practical implementation of a quantum computer will rely on quantum error correction (QEC) [1–3] due to the fragility of quantum states. There is a strong belief that surface (toric) codes [4, 5] can offer the fastest route to scalable quantum computer due to the error threshold around 1% and the locality of required gates [6–10]. Unfortunately, in the nearest future, the surface codes (in fact, any two-dimensional codes with local stabilizer generators[11]) can only lead to proof of the principle realizations as they encode a limited number of qubits (k), making any implementation of a useable quantum computer large (e.g., 2.2×10^8 physical qubits are required for a useful realization of Shor's algorithm [12]).

A large family of quantum low-density parity-check (LDPC) codes (a non-local generalization of toric codes) has been constructed by Tillich and Zémor[13]. These quantum hypergraph-product codes (QHPCs) contain families of Calderbank-Shor-Steane (CSS) codes [14] where the number of encoded qubits k scales linearly with the *blocklength* n, the number of physical qubits directly involved in the code. The finite asymptotic *rate* $R \equiv k/n$ substantially improves upon the toric codes where $R = 0$ (Fig. 1). This construction can also be modified to generalize the rotated toric codes[15] (e.g., checkerboard codes) with a finite-factor rate improvement[16]. Just as for the toric codes, the *distance* d (the minimal number of qubits in an error the code cannot detect) of QHPCs scales as a square root of the block length, $d \propto n^{1/2}$.

In general, removing the restriction of locality should considerably improve the code parameters. Non-local two-qubit gates are relatively inexpensive with floating gates [17], superconducting and trapped-ion qubits, as well as more exotic schemes with teleportation[18–23]. Thus, one can consider a much wider class of quantum LDPC codes[24, 25] for which, compared to general quantum codes, each quantum measurement involves fewer qubits, measurements can be done in parallel, and also the classical processing can be enormously simplified.

Furthermore, at sufficiently large blocklengths often necessary for achieving small computational error, a fault tolerant family of quantum LDPC codes with a finite asymptotic rate will require fewer physical qubits compared to a realization based on copies of toric code. Unfortunately, the parameters as well as the fault tolerance of general quantum LDPC codes are largely unexplored.

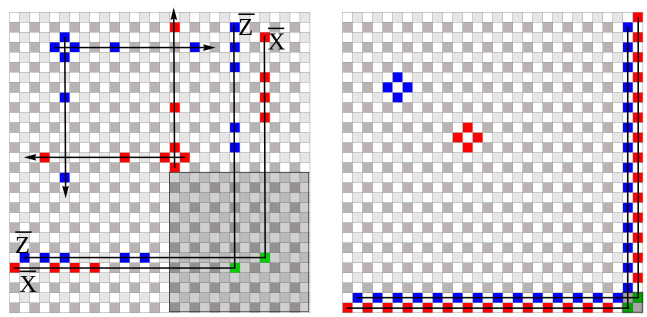

FIG. 1. (Color online) Left: Two stabilizer generators (arrows) and two pairs of anticommuting logical operators (lines) of a $[[450, 98, 5]]$ code in Eq. (1) formed by circulant matrices $\mathcal{H}_1 = \mathcal{H}_2$ with the first row $[1, 1, 0, 1, 0, 0, 0, 1, 0 \ldots 0]$ (red and blue, respectively, X and Z operators, green—overlap of Z and X operators, dark and light gray—dual sublattices of physical qubits). Other stabilizer generators are obtained by shifts over the same sublattice with periodic boundaries. Shaded regions: each gray square uniquely corresponds to a pair of logical operators, thus 98 encoded logical qubits. Right: same for the toric code $[[450, 2, 15]]$.

In this Rapid Communication, we discuss error-correction properties and fault-tolerance of families of finite-rate quantum (and where noted classical) LDPC codes whose relative distance $\delta \equiv d/n$ tends to zero in the limit of large blocklength. Even though we term such codes as "bad" (as good codes should have both the rate and the relative distance finite, see Ref. [26]) these are the best finite-rate quantum LDPC codes with explicitly known distance. For random uncorrelated (qu)bit errors (*e.g., quantum depolarizing channel*), we establish the existence and give a lower bound for the single (qu)bit error rate below which the decoding with probability one is possible, and analyze the scaling of successful decoding probability with the blocklength. This result is obtained by separating errors into small independent clusters on a graph, a construction analogous to the cluster theorem [27]. We also give related bounds for fault-tolerant operation in the presence of syndrome measurement errors. A similar analysis for errors when the erroneous (qu)bits are known (*erasure channel*) allows us to establish an upper limit for the achievable rate of a quantum LDPC code with power-law scaling of the distance with blocklength. These results are important since, unlike for regular QEC codes, there are very few general lower (existence) or upper bounds for quantum LDPC codes[28].

DEFINITIONS. A binary linear code $\mathcal{C}$ with parameters $[n, k, d]$ is a k-dimensional subspace of the vector space $\mathbb{F}_2^n$ of all binary strings of length n. Code distance d is the minimal weight (number of non-zero elements) of a non-zero string in the code. A linear code is uniquely specified by the binary parity check matrix H, namely $\mathcal{C} = \{\mathbf{c} \in \mathbb{F}_2^n | H\mathbf{c} = 0\}$, where operations are done mod 2.

A quantum $[[n, k, d]]$ (qubit) stabilizer code $\mathcal{Q}$ is a 2^k-dimensional subspace of the n-qubit Hilbert space $\mathbb{H}_2^{\otimes n}$, a common $+1$ eigenspace of all operators in an Abelian *stabilizer group* $\mathscr{S} \subset \mathscr{P}_n$, $-\mathbb{1} \notin \mathscr{S}$, where the n-qubit Pauli group $\mathscr{P}_n$ is generated by tensor products of the X and Z single-qubit Pauli operators. The stabilizer is typically specified in terms of its generators, $\mathscr{S} = \langle S_1, \ldots, S_{n-k} \rangle$; measuring the generators S_i produces the *syndrome* vector. The weight of a Pauli operator is the number of qubits it affects. The distance d of a quantum code is the minimum weight of an operator U which commutes with all operators from the stabilizer $\mathscr{S}$, but is not a part of the stabilizer, $U \notin \mathscr{S}$. A code of distance d can detect any error of weight up to $d - 1$, and correct up to $\lfloor d/2 \rfloor$.

A Pauli operator $U \equiv i^m X^{\mathbf{v}} Z^{\mathbf{u}}$, where $\mathbf{v}, \mathbf{u} \in \{0, 1\}^{\otimes n}$ and $X^{\mathbf{v}} = X_1^{v_1} X_2^{v_2} \ldots X_n^{v_n}$, $Z^{\mathbf{u}} = Z_1^{u_1} Z_2^{u_2} \ldots Z_n^{u_n}$, can be mapped, up to a phase, to a quaternary vector, $\mathbf{e} \equiv \mathbf{u} + \omega \mathbf{v}$, where $\omega^2 \equiv \overline{\omega} \equiv \omega + 1$. A product of two quantum operators corresponds to a sum (mod 2) of the corresponding vectors. Two Pauli operators commute if and only if the *trace inner product* $\mathbf{e}_1 * \mathbf{e}_2 \equiv \mathbf{e}_1 \cdot \overline{\mathbf{e}}_2 + \overline{\mathbf{e}}_1 \cdot \mathbf{e}_2$ of the corresponding vectors is zero, where $\overline{\mathbf{e}} \equiv \mathbf{u} + \overline{\omega} \mathbf{v}$.

With this map, generators of a stabilizer group are mapped to rows of a parity check matrix H of an *additive* (forming a group with respect to addition but not necessarily over the full set of $\mathbb{F}_4$ operations) code over $\mathbb{F}_4$, with the condition that the trace inner product of any two rows vanishes[29]. The vectors generated by rows of H correspond to stabilizer generators; these vectors form the *degeneracy group* and are omitted from the distance calculation. For a more narrow set of CSS codes the parity check matrix is a direct sum $H = G_x \oplus \omega G_z$, and the commutativity condition simplifies to $G_x G_z^T = 0$.

An LDPC code, quantum or classical, is a code with a sparce parity check matrix. For a *regular* (j, l) LDPC code, every column and every row of H have weights j and l respectively, while for a (j, l)-limited LDPC code these weigths are limited from above by j and l.

The QHPCs [13] (Fig. 1) are constructed from two binary matrices, $\mathcal{H}_1$ (dimensions $r_1 \times n_1$) and $\mathcal{H}_2$ (dimensions $r_2 \times n_2$), as a CSS code with the stabilizer [16]

$$G_x = (E_2 \otimes \mathcal{H}_1, \mathcal{H}_2 \otimes E_1), G_z = (\mathcal{H}_2^T \otimes \widetilde{E}_1, \widetilde{E}_2 \otimes \mathcal{H}_1^T). \tag{1}$$

Here each matrix is composed of two blocks constructed as Kronecker products (denoted with "$\otimes$"), and E_i and $\widetilde{E}_i$, $i = 1, 2$, are unit matrices of dimensions given by r_i and n_i, respectively. In the original construction[13], given the binary parity check matrix $\mathcal{H}_1 = \mathcal{H}_2^T$ of an (h, v)-limited classical LDPC code $[n_c, k_c, d_c]$, the QHPC (1) is a CSS code with the parameters $[[n = n_c^2 + (n_c - k_c)^2, k = k_c^2, d = d_c]]$, and column and row weights limited by $j \le \max(h, v)$, $\ell \le h + v$. An original classical LDPC code produces a quantum LDPC code, and the corresponding distance scales as $d \propto n^{1/2}$.

OUR KEY OBSERVATION is that for LDPC codes, quantum or classical, large-weight errors are mostly those composed of *disjoint* small-weight clusters that can be detected or corrected independently. Indeed, e.g., for a regular (j, ℓ) LDPC code, two random (qu)bits have non-zero values in the same row with probability z/n, where $z \equiv (\ell - 1)j$. Correcting any of such disjoint errors does not affect the syndrome for the others.

More generally, for a (j, ℓ)-limited LDPC code, we represent all (qu)bits as nodes of a graph $\mathcal{G}_1$ of degree at most z: two nodes are connected by an edge iff there is a row in the parity check matrix which has non-zero values at both positions. An error with support in a subset $\mathcal{E} \subseteq V(\mathcal{G}_1)$ of the vertices defines the subgraph $\mathcal{G}_1(\mathcal{E})$ induced by $\mathcal{E}$. Generally, we will not make a distinction between a set of vertices and the corresponding induced subgraph. In particular, a (connected) cluster in $\mathcal{E}$ corresponds to a connected subgraph of $\mathcal{G}_1(\mathcal{E})$. Different clusters affect disjoint sets of rows of the parity check matrix. This implies the following

Lemma 1. *For a distance-d LDPC code, any error whose support is a union of disconnected clusters on $\mathcal{G}_1$ of weights $w_i < d$, is detectable.*

In the case of an erasure channel (quantum or classical), we actually know which (qu)bits are affected. In known locations, a code of distance d can correct all errors of weight $d - 1$ or smaller. Therefore, correcting clusters one-by-one, we can guarantee success if all the clusters have weights $w_i < d$. It is then obvious that the problem of error correction for an erasure channel is related to the problem of site percolation on graphs[30].

For any (j, ℓ)-limited LDPC code, the vertices of the graph $\mathcal{G}_1$ have degrees at most $z \equiv (\ell - 1)j$. In what follows, we will need the cluster size distribution [the probability $n_s^{(p)}(x)$ that the point x is a member of a cluster of size s] below the percolation threshold. Although one expects exponential tail in the cluster size distribution, $n_s(p) \le \exp(-sg(p))$ for all $s \ge s_0$ and some $g(p) > 0$ and $s_0 > 0$, this can be violated for sufficiently heterogeneous graphs[31]. Restricting the range of p, we have

Lemma 2. *For any graph $\mathcal{G}$ with vertex degrees limited by z, the site- or bond-percolation cluster size distribution has exponential tail for $p < p_0 \equiv (z-1)^{-1}$.*

Proof. A size-s cluster containing x on $\mathcal{G}$, after cutting any loops, can be mapped to a size-s cluster on z-regular tree $\mathcal{T}_z$ (Bethe lattice), with x mapped to the root. Such a mapping can only increase the perimeter (size of the boundary, i.e., number of sites outside the cluster but neighboring with a site inside it). Any size-s cluster on $\mathcal{T}_z$ has the perimeter $t_z(s) \equiv s(z-2)+2$; for a cluster on $\mathcal{G}$ we have $t \le t_z(s)$. Let us now use the standard expression for the cluster size distribution, $n_s^{(p)}(x) = \sum_t a_{s,t}(x) p^s (1-p)^t$, where $a_{s,t}(x) \ge 0$ is the number of x-containing site-percolation clusters of size s and perimeter t. For $p \le p_0$,

$$(1-p)^t \le (1-p_0)^t \frac{(1-p)^{t_z(s)}}{(1-p_0)^{t_z(s)}}, \qquad (2)$$

which gives the exponential tail

$$n_s^{(p)}(x) \le n_s^{(p_0)}(x) \frac{(1-p)^2}{(1-p_0)^2} \alpha_z^s, \;\; \alpha_z \equiv \frac{p(1-p)^{z-2}}{p_0(1-p_0)^{z-2}}. \qquad (3)$$

since $\alpha_z(p) < 1$ for $p < p_0$ and $n_s^{(p_0)} \overset{\text{def}}{\le} 1$. □

Notice that the threshold for exponential tail coincides with the lower boundary of the (bond) percolation transition for degree-limited graphs[32], which is also the lower boundary for the site percolation transition[33]; both boundaries are achieved on z-regular tree $\mathcal{T}_z$.

We can now formulate the following

Theorem 1. *For an infinite family of (j,l)-limited LDPC codes, quantum or classical, where the distance d scales as a power law at large n, $d \ge An^\alpha$, with some $\alpha > 0$ and $A > 0$, asymptotically certain recovery is possible for (qu)bit erasure probabilities $p < p_e$, where $p_e \ge p_0 = (z-1)^{-1}$ and $z \equiv (\ell-1)j$. A non-zero threshold p_e also exists for such code families with the distance scaling logarithmically at large n, $d \ge A_0 \ln n$.*

Proof. The conditions match those of Lemmas 1 and 2. For $p < p_0$, we just need to ensure that the probability to find a cluster of size $s \ge d$ anywhere on $\mathcal{G}_1$ vanishes at large n, i.e., $n \sum_{s \ge d} n_s^{(p)}/s \to 0$. The sufficient condition on the distance is $d > \ln n / |\ln \alpha_z|$, which is always the case at large n with power-law distance, and gives $\alpha_z(p) \le e^{-A_0}$ with logarithmically increasing distance. The latter equation is satisfied for small enough p by continuity of $\alpha_z(p)$ since $\alpha_z(0) = 0$. □

Given the upper limit on the rate of stabilizer codes in Theorem 3.8 of Ref. 28, we also obtain the limit on the rate of quantum codes in Theorem 1:

Corollary 2. *Any family of (j,ℓ)-limited LDPC quantum codes with power-law scaling of the minimum distance with the block length n, has rate R limited by*

$$R < 1 - 2\left[z - 1 - (z-3)\left(\frac{z-2}{z-1}\right)^{\ell-1}\right]^{-1}. \qquad (4)$$

The situation gets a bit more complicated for the *depolarizing channel* (memoryless binary symmetric channel in the classical case), where the positions of the errors are unknown. A bound on single-(qu)bit error probability which guarantees almost certain error correction for large codes is given by

Theorem 3. *For an infinite family of (j,l)-limited LDPC codes, quantum or classical, where the distance d scales as a power law at large n, asymptotically certain recovery is possible for (qu)bit* depolarizing *probabilities $p < p_d \ge p_1$, where $4p_1(1-p_1) = p_0^2(1-p_0)^{2(z-2)} < [e(z-1)]^{-2}$, $p_1 < 1/2$, and e is the base of the natural logarithm. A threshold $p_d > 0$ also exists for code families with distance scaling logarithmically at large n.*

Proof. The clusters can be irrecoverably misidentified only if there exists a set of $s \ge d$ connected vertices on $\mathcal{G}_1$ with $m \ge \lceil s/2 \rceil$ errors. We will call such sets violating (s,m)-sets. To estimate the probability of encountering such a set, we notice that an (s,m) set with an additional error at the perimeter can be extended to become an $(s+1, m+1)$ set. Thus, one only needs to count connected sets of size $s \ge d$, with perimeter free of errors. For $s \ge d$, the probability $\tilde{n}_s^{(p)}(x)$ that one of violating (s,m) sets includes the point x, can be limited as $\tilde{n}_s^{(p)}(x) < f_s^{(p)}(x)$, where

$$f_s^{(p)}(x) \equiv \sum_t a_{st}(x) \sum_{m=\lceil s/2 \rceil}^{u} \binom{s}{m} p^m (1-p)^{s-m+t}. \qquad (5)$$

The sum over m can be limited by $2^s p^{s/2}(1-p)^{s/2+t}$, which gives a bound in terms of the regular cluster size distribution, $f_s^{(p)} \le [4(1-p)/p]^{s/2} n_s^{(p)}(x)$. Using Eq. (3), we have the condition $4(1-p)/p\alpha_z^2 < 1$ to have exponential tail for $\tilde{n}_s^{(p)}(x)$. This condition is satisfied for $p < p_1$. The rest of the proof follows that of Theorem 1. □

Note that this bound is rather loose as there are many sets which differ just by error-free regions. We believe a more accurate general bound should be a factor of e^2 larger, $p_1 = [2(z-1)]^{-2}$, as can be obtained by counting chains on a z-regular tree (to reduce multiple counts).

We also note that the threshold in Theorem 3 corresponds to maximum-likelihood (ML) decoding[34] and is *not* related to a particular decoder, as is commonly done for classical LDPC codes. For a practical approach in the quantum case, one can identify putative clusters by first adding all positions corresponding to a non-zero syndrome element, then at each step adding up to $\ell - 1$ positions from each of the non-zero-syndrome rows which include qubit(s) already in the cluster. A corrected cluster can be dropped [Theorem 3]; putative clusters which cannot be corrected individually need to be joined with one or more such cluster(s) nearby using a variant of the algorithm for toric codes[5, 8, 9]. Below the percolation threshold the actual clusters will typically have size of order $s \lesssim \ln n/|\ln \alpha_z|$, scaling logarithmically with n. Thus, for $p < p_1$, we expect that the number of classical operations for exhaustive search of the correct error configuration in each cluster will scale as a power of n.

So far our discussion has been limited to idealized performance of the code, which assumes that the syndrome is measured perfectly. With qubit measurement errors, LDPC codes suddenly appear at a disadvantage, as a single-qubit error accompanied by the errors of some of the stabilizer generators (up to j) which involve this qubit, could remain undetected. In other words, the effective distance to such combined errors cannot exceed the *minimum* column weight plus one. In order to prevent errors from spreading, either we have to keep the measurement error small, or we have to combine the information from different syndrome measurement cycles. To help with the bookkeeping, we constructed an auxiliary classical code combining different time slices. The code is based on the parity-check matrix of the original code, and the repetition codes (in the simplest case) for each measured syndrome[35]. This generalizes the auxiliary three-dimensional gauge model used in the decoding of the surface codes[5]. The corresponding graph $\mathcal{G}_1$ has up to $2j$ additional neighbors per qubit, which corresponds to possible syndrome measurement errors in the two neighboring layers. The percolation problem works similarly to that with perfect measurements. Overall, the analysis in Theorem 3 can be repeated with $z \to z' \equiv j(\ell+1)$, which in the case of isotropic error probability $p = p_{\rm meas}$ gives a finite lower bound $p \geq [2e(z'-1)]^{-2}$ for such *fault-tolerant* measurements.

Combining repeated syndrome measurements is only part of the story of fault-tolerant implementation of a code. We implicitly assumed that the hardware allows for parallel measurement of non-overlapping stabilizer generators, that this can be done in fixed time even though the corresponding qubits may not necessarily lie next to each other, and also that all gates are done fault-tolerantly [36], so that errors do not spread. With these assumptions, the full syndrome can be measured in approximately z steps, which would take bounded time independent of the size of the code. Fault-tolerant operation also implies some implemetation of logical operators, e.g., as suggested in Ref. 37.

Our results apply to QHPCs and related codes[13, 16]. As an example, we start with a *random* (h, v)-regular binary LDPC code ($h < v$, ensemble A in Ref. [38]) with $\mathcal{H}_1 = \mathcal{H}_2^T$. The rate of such a code is limited, $R_{\rm c} \equiv k_{\rm c}/n_{\rm c} \geq 1 - h/v$. With high probability at large $n_{\rm c}$, the code will have the relative distance in excess of $\delta_{\rm c} \equiv \delta_c(h, v)$ given in Ref. 38. Such $[n_c, k_c, d_c]$ codes produce QHPCs (1) which are $(v, v+h)$-limited LDPC codes $[z = v(v + h - 1)]$ with the asymptotic rates $R \geq (v - h)^2/(h^2 + v^2)$ and the distance scaling as $d/\sqrt{n} = \delta_c v/\sqrt{h^2 + v^2}$. For large n, all errors can be corrected with certainty for single-qubit error probabilities below p_1, see Theorem 3. For $h = 3$, $v = 4$, we obtain QHPCs $[[n, n/25, 0.09\sqrt{n}]]$ with numerically estimated threshold probabilities that are close (within a factor of two[39]) to the toric code thresholds of around 1% [5, 8, 9] and 19% [10], with and without the syndrome errors, respectively (e.g., these values are much higher than the lower bound in Theorem 3).

Suppose we need to maintain quantum information for $\mathcal{N}$ QEC cycles with a fault probability less than P_f. We can crudely estimate the minimal required blocklength from the equation $P_f = \mathcal{N}\mathcal{M} f_d^{(p)}(x) d/n$, where $f_d^{(p)}(x)$ is given by Eq. (5), $\mathcal{M}$ is the number of syndrome measurements per QEC cycle ($\mathcal{M} = 2$ for toric code and $\mathcal{M} = 2v(v+h-1)$ for QHPC). Taking $P_f/\mathcal{N} = 10^{-9}$, we need at least 30000 physical (1200 logical) qubits, fewer than in $k/2$ copies of the toric code for the same $P_f/\mathcal{N}$.

In conclusion, we established a sufficient condition for an LDPC code family with asymptotically vanishing relative distance to have a finite probability threshold to correct all errors with certainty, including the case of syndrome measurement errors, see Theorem 3. Existence of such a threshold is one of *necessary* conditions for achieving fault-tolerance in a quantum computer, and it should facilitate search for new efficient quantum codes with less stringent requirements on the number of physical qubits. In particular, we established the existence of such a threshold for the finite-rate quantum LDPC codes constructed in the framework of QHPCs[13, 16]. According to our estimates, QHPCs require lower (more stringent) error thresholds compared to toric codes, but they use fewer physical qubits at large code blocklengths.

The simplest versions of hypergraph-product codes correspond to the Wen-plaquette model[40] with topological order described by Z_2 symmetry. It is an open question whether some classification of hypergraph-product codes with respect to topological order can be done. Error correction threshold for the toric code can be related to the phase transition in the random bond Ising model[5]. It is not known whether such a connection can be established for general hypergraph-product codes.

We have also established the existence of a related threshold when the erroneous qubits are known, see Theorem 1, which resulted in an upper bound for the rate of quantum LDPC codes [see Eq. (4)].

We are grateful to I. Dumer and M. Grassl for multiple helpful discussions. This work was supported in part by the U.S. Army Research Office Grant No. W911NF-11-1-0027, and by the NSF Grant No. 1018935.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[2] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[3] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996).

[4] A. Y. Kitaev, Ann. Phys. **303**, 2 (2003).

[5] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).

[6] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).

[7] D. S. Wang, A. G. Fowler, and L. C. L. Hollenberg, Phys. Rev. A **83**, 020302 (2011).

[8] D. S. Wang, A. G. Fowler, and L. C. L. Hollenberg, Phys. Rev. A **83**, 020302 (2011).

[9] A. G. Fowler, A. C. Whiteside, and L. C. L. Hollenberg, Phys. Rev. Lett. **108**, 180501 (2012).

[10] H. Bombin, R. S. Andrist, M. Ohzeki, H. G. Katzgraber, and M. A. Martin-Delgado, Phys. Rev. X **2**, 021004 (2012).

[11] S. Bravyi, D. Poulin, and B. Terhal, Phys. Rev. Lett. **104**, 050503 (2010).

[12] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, ArXiv e-prints (2012), arXiv:1208.0928 [quant-ph].

[13] J.-P. Tillich and G. Zemor, in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on* (2009) pp. 799 –803.

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Infomation* (Cambridge Unive. Press, Cambridge, MA, 2000).

[15] A. A. Kovalev, I. Dumer, and L. P. Pryadko, Phys. Rev. A **84**, 062319 (2011).

[16] A. Kovalev and L. Pryadko, in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on* (2012) pp. 348 –352, [arXiv:1202.0928].

[17] L. Trifunovic, O. Dial, M. Trif, J. R. Wootton, R. Abebe, A. Yacoby, and D. Loss, Phys. Rev. X **2**, 011006 (2012).

[18] T. Yamamoto, Y. A. Pashkin, O. Astafiev, Y. Nakamura, and J. S. Tsai, Nature **425**, 941 (2003).

[19] R. McDermott, R. W. Simmonds, M. Steffen, K. B. Cooper, K. Cicak, K. D. Osborn, S. Oh, D. P. Pappas, and J. M. Martinis, Science **307**, 1299 (2005).

[20] J. Benhelm, G. Kirchmair, C. F. Roos, and R. Blatt, Nature Physics **4**, 463 (2008).

[21] A. Friedenauer, H. Schmitz, J. T. Glueckert, D. Porras, and T. Schaetz, Nature Physics (2008), 10.1038/nphys1032.

[22] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[23] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).

[24] M. S. Postol, "A proposed quantum low density parity check code," (2001), unpublished, arXiv:quant-ph/0108131v1.

[25] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, IEEE Transactions on Information Theory **59**, 2315 (2004).

[26] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[27] C. Domb and M. S. Green, eds., *Phase transitions and critical phenomena*, Vol. 3 (Academic, London, 1974).

[28] N. Delfosse and G. Zémor, "Upper bounds on the rate of low density stabilizer codes for the quantum erasure channel," (2012), arXiv:1205.7036v1.

[29] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Th. **44**, 1369 (1998).

[30] This relation has been noticed in Refs. [5, 28].

[31] A. Bandyopadhyay, J. Steif, and Á. Timár, Rev. Mat. Iberoamericana **26**, 529 (2010).

[32] Theorem 1.2 in R. van der Hofstad, in *New Perspectives on Stochastic Geometry*, edited by I. Molchanov and W. Kendall (Oxford University Press, 2010) Chap. 6, pp. 173–247, iSBN 978-0-19-923257-4.

[33] J. M. Hammersley, J. Math. Phys. **2**, 728 (1961).

[34] J. Feldman, M. Wainwright, and D. Karger, Information Theory, IEEE Transactions on **51**, 954 (2005).

[35] A. A. Kovalev and L. P. Pryadko, unpublished (2012).

[36] P. W. Shor, in *Proceedings of the 37th Annual Symposium on Fundamentals of Computer Science*, IEEE (IEEE Computer Society Press, Los Alamitos, 1996) pp. 56–65, quant-ph/9605011; D. P. DiVincenzo and P. W. Shor, Phys. Rev. Lett. **77**, 3260 (1996); D. Gottesman, Phys. Rev. A **57**, 127 (1998); A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997); Nature **399**, 124 (1999); E. Knill, **434**, 39 (2005).

[37] A. M. Steane and B. Ibinson, Phys. Rev. A **72**, 052335 (2005).

[38] S. Litsyn and V. Shevelev, Information Theory, IEEE Transactions on **48**, 887 (2002).

[39] A. A. Kovalev and L. P. Pryadko, unpublished.

[40] X.-G. Wen, Phys. Rev. Lett. **90**, 016803 (2003).