A Good Family of Quantum Low-Density Parity-Check Codes

Reina Riemann and Peter Shor

***Abstract*—We present a good family of quantum low-density parity-check error-correcting codes. This family is derived from regular Platonic surfaces. We present a logarithmic lower bound on their shortest noncontractible cycle and therefore on the distance of the family of codes. We show the asymptotical low-density of their matrices, and show their asymptotical nonzero rate. We simulate their good decoding performance. This family answers a conjecture proposed by MacKay about the existence of families of quantum low-density parity-check (LDPC) codes with nonzero rate, growing minimum distance and a practical decoder.**

Index Terms—Low-density parity-check codes, message passing decoding, quantum codes.

I. Introduction

From a theoretical perspective a good family of error-correcting codes corrects errors in proportion to the block length of the codes and has a practical decoder [7]. For example classical low-density parity-check codes (LDPC), first introduced by Gallager [5], approach the Gilbert-Varshamov bound and have a practical decoder. LDCP codes have reemerged as one of the most influential coding schemes. Their sparse local parity-check dependencies imply low decoding complexity when using local iterative message-passing decoding algorithms. Classical LDPC and LDPC-like codes decoded with message-passing decoders are used in practice such as in internet and mobile media broadcast, optical networking and other applications.

The development of quantum information theory paves the way to the development of quantum computers extending the notion of classical channels and error-correcting codes [3]. The existence of good quantum error-correcting codes was shown non-constructively by Calderbank and Shor [4]. In 2003, MacKay [8] introduced some promising individual examples of quantum LDPC codes. MacKay's codes are dual-containing stabilizer codes whose matrix representation is sparse. Several theoretical questions were raised by this work including a conjecture about the existence of good families of sparse-graph quantum error-correcting codes with nonzero rate, growing minimum distance and a practical decoder. We answer this conjecture by presenting one such family here.

We present a family of good sparse quantum error-correcting codes with asymptotic logarithmic distance.We show their asymptotical sparsity, non-zero rate, and their decoding performance with belief propagation. These codes are derived from sparse graphs, induced by tessellations of topological surfaces, and are therefore a type of low-density parity-check (LDPC) code. Note that while most known LDPC codes are derived from regular graphs, there are known classical LDPC codes derived from irregular graphs [9].

The low-density parity-check families of quantum codes that we present are generalizations of Kitaev's codes [6] to surfaces of genus g that encode $2g$ qubits, as explained in section III. Kitaev's topological codes are a class of stabilizer codes derived from lattices on surfaces of single genus, or tori, with asymptotical zero rate.

In section II we give definitions, background and notation used in this paper. In section III we review stabilizer quantum error-correcting codes, topological quantum error-correcting codes and their generalization to tessellations on 2-manifolds. In section IV we describe the family of Platonic graphs and surfaces. We present a quantum code derived from π_7 and a good family of Platonic quantum low-density parity-check codes. We derive the asymptotical low-density of their matrices and their rate. In section V we provide a logarithmic lower bound on their distance. In section VI we present decoding simulations using belief propagation. In section VII we provide our insights and conclusions.

II. Definitions

In this section we introduce the topological graph-theoretical definitions used in the quantum error-correcting codes families of codes that we present in this paper. Let $G = (V, E)$ be a graph, where V is a set of vertices, and E, a set of edges.

Definition 1. If a graph G can be drawn on a $2-dimensional$ $manifold$ or surface M without edge crossing, then it is said to be $embedded$ on this manifold.

The family of quantum error-correcting codes that we present is derived from embeddings of graphs on 2-dimensional surfaces.

Definition 2. An embedding of a graph is a $tessellation$ of a surface.

Reina Riemann. Computer Science and Artificial Intelligence Laboratory. Massachusetts Institute of Technology. Cambridge, MA 02139, USA. e-mail: riemann@mit.edu

Peter Shor. Department of Mathematics. Massachusetts Institute of Technology. Cambridge, MA 02139, USA. e-mail: shor@math.mit.edu

Definition 3. The $genus$ of a graph G is the smallest genus of a $2-dimensional$ manifold M in which the graph can be embedded.

The genus of the surfaces on which these graphs are embedded is related to the number of qubits that can be encoded as explained in the next section, topological quantum error-correcting codes.

Definition 4. A $planar$ graph is a graph that can be embedded in a surface of genus 0, that is the plane.

Definition 5. The $girth$ of a graph is the length of its shortest cycle.

Definition 6. The $shortest\ noncontractible\ cycle$ of a graph of genus g is the length of the shortest cycle or closed path that is not a face of the induced tessellation. A face is one of the open discs derived from the difference between the two dimensional manifold M and the embedded graph.

Furthermore the shortest noncontractible cycle of a graph is related to the number of errors that the code can correct as we explain in the next section.

III. Topological Quantum Error-correcting Codes

Topological codes are a class of stabilizer codes associated with tessellations of manifolds. Stabilizer codes can be described in terms of group theory or of binary vector spaces. In terms of group theory a codeword is the $+1$ eigenstate of the group generated by a stabilizer set.

In terms of binary vector spaces, a stabilizer code is described by a pair of binary matrices whose rows represent generators, and whose columns represent different qubits. One matrix is associated with

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and the other matrix with

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Simultaneous entries in both matrices are associated with

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Multiplication of generators is equivalent to vector addition mod 2. Elements of the stabilizer group have to commute with each other, otherwise they stabilize the trivial space.

Using MacKay's notation [8], let $a_i|b_i$ denote a binary vector, where a_i is in row i of the matrix of a stabilizer parity check matrix associated with X errors and b_i is in the matrix associated with Z errors. Let $a_j|b_j$ be another such vector, then the condition that two stabilizer generators commute is equivalent to the following product:

$$a_i \centerdot b_j \quad + a_j \centerdot b_i \equiv \quad 0 \; mod \; 2$$

The binary vector view of stabilizer codes emphasizes connections between classical and quantum error correcting codes.

Kitaev's toric codes are defined by an $L \times L$ lattice on the torus. The encoding qubits are associated with edges of this lattice. The related stabilizer quantum error-correcting code check operators are associated with faces and vertices as follows:

$$\begin{aligned} Z^{face} &= \prod_{e \in face} Z_e \\ X^{vertex} &= \prod_{e \in vertex} X_e \end{aligned}$$

The vertex and face operators commute because they either act on disjoint qubits or on an even number of qubits in common. Let e be the number of edges, v the number of vertices and f the number of faces of a given grid. By Euler's equation, these toric codes encode 2 qubits. Since the number of logical qubits remains constant as the number of encoding qubits increases, their asymptotic rate is zero.

In order to generalize toric codes to higher genus surfaces, we study tessellations of an orientable 2-manifold of genus g. Furthermore a noncontractible cycle in the tessellation or dual tessellation commutes with the stabilizer group of the code because it is a cycle. Nevertheless it is not contained in the stabilizer group. Therefore the distance of the code is the length of the shortest non-contractible cycle in the tessellation.

We decode the family of topological codes using belief propagation by simulating the 4-ary symmetric channel as two independent binary symmetric channels in the belief propagation section. Therefore we calculate the independent asymptotical rate of X^{vertex} and Z^{facce} in the next section.

The rate for the Z^{face} is

$$\frac{e-(f-1)}{e}$$

The rate for the X^{vertex} is

$$\frac{e-(v-1)}{e}$$

And the topological rate for the respective code is

$$\frac{e-(f-1)-(v-1)}{e}$$

IV. Platonic Quantum Low-Density Parity-Check Codes

A. Platonic Graph And Surfaces

$Platonic\ Graphs\ \pi_n$ are generalizations of the Platonic solids [2]. They are characterized by regular tessellations of Riemann surfaces or 2-manifolds, which are called $Platonic\ Surfaces\ S_n$.

Definition 7. $Platonic\,Graphs\,\pi_n$ are determined by vertices and edges. A vertex of π_n is defined by a pair of integers $\binom{a}{b}$ such that $\binom{a}{b} \sim \binom{-a}{-b}$. The pair is taken projectively, that is, $gcd(a,b) = 1$. An edge joins two vertices, $\binom{a}{b}$ and $\binom{c}{d}$ iff $det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \pm 1\ mod\ n$.

Furthermore any two vertices have two paths of length two note that the $Platonic\,Graphs$ have the two-step property [2], that is, any two vertices have exactly two paths of length two, associating π_n to a unique triangulated topological 2-manifold. Also note that n does not have to be a prime number. When $n \geqslant 6$, we obtain a tessellation of a surface of $genus \geqslant 1$.

The first few Platonic graphs are the tetrahedron π_3, the octahedron π_4, and the icosahedron π_5. The Dual Platonic graphs, π'_n, have a vertex for each triangular face in π_n, and an edge between two vertices iff the respective π_n faces are adjacent. The first few dual Platonic Graphs are the tetrahedron π'_3 (self-dual), the cube π'_4, and the dodecahedron π'_5.

Remark 8. For p odd prime, the graph π_p has $\frac{p^2-1}{2}$ vertices. Let v_p be the number of vertices of π_p, then there are $\frac{v_p.p}{2}$ edges e_p, and $\frac{v_p.p}{3}$ faces f_p. For π'_n, there are $v'_p = f_p$, $e'_p = e_p$, and $f'_p = v_p$.

B. Platonic Quantum Low-Density Parity-Check Codes

In this section we give a specific example of a quantum LDPC code derived from π_7, and an infinite family of good LDPC codes derived from Platonic Surfaces. We calculate their asymptotic rate, analyze their sparsity and provide a lower bound on their distance, the length of its shortest non-contractible cycle

Example:

The Platonic quantum code derived from π_7 has $\frac{p^2-1}{2} = 24$ vertices v_p, $\frac{v_p.p}{3} = 56$ faces, and $\frac{v_p.p}{2} = 84$ edges, and that it follows that $g = 3$ is the genus of the surface. It has quantum rate 1/14. For π'_7, there are 56 vertices, 24 faces, and 84 edges, and its shortest non-contractible cycle is of length 8.

C. Family of Platonic Quantum Low-Density Parity-Check Codes

In general we derive a family of quantum LDPC codes from the dual Platonic graphs π'_p, analyze their rate and the next section we provide a bound on their distance of the length of the shortest non-contractible cycle.

D. Asymptotic nonzero classical rate for the platonic family of quantum error-correcting codes

Remark 9. The Z^{face} check operator of a dual Platonic quantum LDPC error-correcting code has rate approaching 1 for p odd prime.

$$\begin{aligned} lim_{p\to\infty} \quad & \frac{e'_p-(f'_p-1)}{e'_p} & = \\ lim_{p\to\infty} \quad & \frac{\frac{p^3-p}{4}-\left(\frac{p^2-1}{2}-1\right)}{\frac{p^3-p}{4}} & = \\ & 1 \end{aligned}$$

Remark 10. The X^{vertex} check operator of a dual Platonic quantum LDPC error-correcting code has rate approaching $\frac{1}{3}$, for p odd prime.

$$\begin{aligned} lim_{p\to\infty} \quad & \frac{e'_p-(v'_p-1)}{e'_p} & = \\ lim_{p\to\infty} \quad & \frac{\frac{p^3-p}{4}-\left(\frac{p^3-p}{6}-1\right)}{\frac{p^3-p}{4}} & = \\ & \frac{1}{3} \end{aligned}$$

Remark 11. The average combined rate of the X^{vertex} and Z^{face} operators approaches $\frac{2}{3}$, for p odd prime.

$$\begin{aligned} lim_{p\to\infty} \quad & \frac{2e'_p-(f'_p+v'_p-2)}{2e'} & = \\ lim_{p\to\infty} \quad & 1-\frac{f'_p+v'_p+-2}{2e'_p} & = \\ lim_{p\to\infty} \quad & 1-\frac{1}{p}-\frac{1}{3}+\frac{1}{p^3-p} & = \\ & \frac{2}{3} \end{aligned}$$

E. Asymptotic nonzero quantum rate for the platonic family of quantum error-correcting codes

Remark 12. The quantum rate of the platonic family of quantum error-correcting codes approaches $\frac{1}{3}$, for p odd prime.

$$\begin{aligned} lim_{p\to\infty} \quad & \frac{e'_p-(f'_p-1)-(v'_p-1)}{e'} & = \\ lim_{p\to\infty} \quad & 1-\frac{f'_p+v'_p+2}{e'_p} & = \\ lim_{p\to\infty} \quad & 1-\frac{\frac{p^2-1}{2}+\frac{p^3-p}{6}+2}{\frac{p^3-p}{4}} & = \\ & \frac{1}{3} \end{aligned}$$

F. *Sparsity Analysis for the Platonic quantum LDPC error-correcting codes*

Remark 13. Let w_f be the weight of the Z^{face} check operators of a dual Platonic quantum LDPC error-correcting code, and let e_p be the corresponding number of encoding qubits for prime p, then $\frac{w_f}{e_p}$ converges to a $c.p^{-2}$.

$$\begin{aligned} lim_{p\to\infty} \quad & \frac{p}{e_p} &= \\ lim_{p\to\infty} \quad & \frac{p}{\frac{v_p \cdot p}{2}} &= \\ lim_{p\to\infty} \quad & \frac{p}{\frac{p^2-1}{4}p} &= \\ & c.p^{-2} & \end{aligned}$$

Remark 14. Let $w_v = 3$ be the weight of the Z^{vertex} check operators of a dual Platonic quantum LDPC error-correcting code, and let e_p be the corresponding number of encoding qubits for prime p, then $\frac{w_v}{e_p}$ converges to zero.

$$\begin{aligned} lim_{p\to\infty} \quad & \frac{3}{e_p} &= \\ & 0 & \end{aligned}$$

V. Shortest non-contractible cycle bound for the dual Platonic surfaces $snc(\pi_p^{'})$

We show that the shortest non-contractible cycle of the family of dual platonic graphs π_p' grows logarithmically in the size of their genus. In order to improve the distance of π_p we obtain subfamilies of Platonic codes by subtessellating them up to $log(p)$ levels of recursion. See decoding simulation section.

We derive the π_p' bound by regarding these graphs as quotient of T_3, the infinite cubic tree [1]. Vertices in T_3 are labeled with unordered triplets of irreducible rational numbers, $\left(\binom{a}{b}\binom{c}{d}\binom{e}{f}\right)$. This labeling is known as a $Farey\ Tree$. See figure 1 .

Definition 15. We define the following binary tree B. The root of B is $\left(\binom{0}{1}\binom{1}{2}\binom{1}{1}\right)$. For a vertex $\left(\binom{a}{b}\binom{c}{d}\binom{e}{f}\right)$ in B, its left child is $\left(\binom{a}{b}\binom{a+c}{b+d}\binom{c}{d}\right)$ and its right child is $\left(\binom{c}{d}\binom{c+e}{d+f}\binom{e}{f}\right)$.

Definition 16. T_3 is defined recursively by generalizing the labels of the following rooted binary tree B. B_0 is B and B_n is obtained from B by adding n to the pairs, i.e. $\binom{a}{b}$ is relabeled as $\binom{(a+n)}{b}$. T_3 is obtained by adjoining the root of a copy B_n to $\left(\binom{1}{0}\binom{n}{1}\binom{n+1}{1}\right)$.

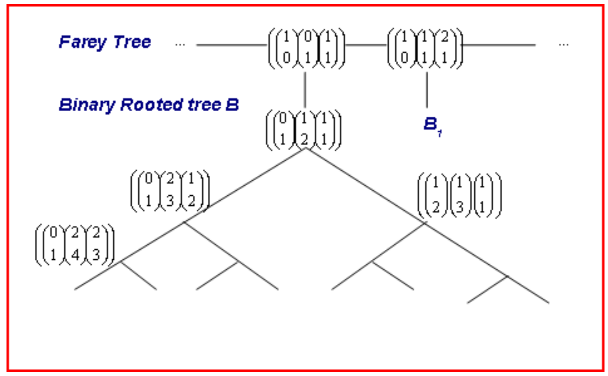


Figure 1. Farey Tree

In the girth of a family of 3-regular graphs, the triplets $T(p)$, by mapping each pair $\binom{a}{b}$ to $a.b^{-1}mod$ p. If b = 0, then $a.b^{-1}mod$ p is mapped to ∞. We obtain the dual Platonic graphs π' from T_3 under the equivalence $\binom{a}{b} \sim \binom{-a}{-b} mod\ \ p$. Using T_3, we show that the shortest non-contractible cycle in the graph, for large p prime, is bounded by $p^2 \le Fibonacci(snc(\pi_p') + 2)$. We provide lemmas about the rooted binary tree B and prove a lemma about a needed symmetry of the tree before proving the distance theorem.

Lemma 17. *For any vertex* $\left(\binom{a}{b}\binom{c}{d}\binom{e}{f}\right)$ *in* B*,*

$$b \cdot c - a \cdot d \quad = \quad d \cdot e - c \cdot f = 1.$$

Corollary 18. *For each pair* $\binom{a}{b}$,

$$gcd(a,b) \quad = \quad 1.$$

Lemma 19. *The largest* b *in a pair* $\binom{a}{b}$ *at level* r*, is* $Fibonacci(r+2)$.

In addition we further observe that there is a symmetry of the tree B that preserves the level of the vertices and induces a reflection on the tree. The symmetry is given by $\binom{b-a}{b}$ on each pair. In the following lemma we use x, as short for $\binom{a}{b}$, and $(1-x)$ as short for $\binom{b-a}{b}$.

Lemma 20. *Let* $((x)\,(y)\,(z))$ *be a vertex* v*, then the involution* i *that takes* v *to* $((1-z)\,(1-y)\,(1-x))$ *is a reflection of the tree* B.

Proof. We prove this lemma by induction. Note that the root of B, $\left(\binom{0}{1}\binom{1}{2}\binom{1}{1}\right)$, is a fixed point of the symmetry. Assume that the symmetry holds for all vertices in B at levels less than n. Let $v = \left(\binom{a}{b}\binom{c}{d}\binom{e}{f}\right)$, be a vertex at level $n-1$. Denote the involution on v, as $i(v) = \left(\binom{f-e}{f}\binom{d-c}{d}\binom{b-a}{b}\right)$. Denote the left descendant of v as v_{left}, and the right descendant as v_{right}. Then,

$$v_{left} \quad = \quad \left(\binom{a}{b}\binom{a+c}{b+d}\binom{c}{d}\right)$$

and

$$v_{right} \quad = \quad \left(\binom{c}{d}\binom{c+e}{b+f}\binom{e}{f}\right)$$

Under the involution, the results are:

$$i(v_{left}) \quad = \quad \left(\binom{d-c}{d}\binom{b+d-c-a}{b+d}\binom{b-a}{b}\right)$$

and

$$i(v_{right}) \quad = \quad \left(\binom{f-e}{f}\binom{b+f-c-e}{b+f}\binom{d-c}{d}\right)$$

which implies that $i(v_{left}) = (i(v))_{right}$, and $i(v_{right}) = (i(v))_{left}$.

Theorem 21. *For large p prime, $p^2 \leq$Fibonacci ($snc(\pi_p^{'})$+2).*

Proof. Because π_p' is vertex transitive, we consider only the cycles from $\left(\binom{1}{0}\binom{0}{1}\binom{1}{1}\right)$. A set of three pairs $\left(\binom{a}{b}\binom{c}{d}\binom{e}{f}\right)$ corresponds to a vertex in π_p' and a face in π_p. Each individual pair corresponds to a vertex in π_p. The order of the pairs within a set does not matter. Therefore, there are six ways in which a vertex in T_3 can reduce to $\left(\binom{1}{0}\binom{0}{1}\binom{1}{1}\right)$, that is all 6 permutations of 3 pairs. In addition, the reflection proved in lemma 20 allows us to consider only 4 cases. Note that under this symmetry, the following cases are equivalent $\left(\binom{0}{1}\binom{1}{1}\binom{1}{0}\right) \sim \left(\binom{1}{0}\binom{0}{1}\binom{1}{1}\right)$, and $\left(\binom{1}{1}\binom{0}{1}\binom{1}{0}\right) \sim \left(\binom{1}{0}\binom{1}{1}\binom{0}{1}\right)$.

Case $\left(\binom{0}{1}\binom{1}{0}\binom{1}{1}\right)$

$$\begin{pmatrix} a \cdot p + e \cdot p + 1 \\ f \cdot p + b \cdot p + 1 + g \end{pmatrix}$$

In order for this pair to reduce to $\binom{1}{0}$, we have that $g = -1$. By applying lemma 17, we get a contradiction.

Case $\left(\binom{1}{0}\binom{1}{1}\binom{0}{1}\right)$

We get a similar reduction to the previous case

Case $\left(\binom{1}{0}\binom{0}{1}\binom{1}{1}\right)$

A vertex that reduces to $\left(\binom{1}{0}\binom{0}{1}\binom{1}{1}\right)$ must be of the form:

$$\left(\begin{pmatrix} a \cdot p \mp 1 \\ b \cdot p \end{pmatrix}\begin{pmatrix} a \cdot p + e \cdot p \\ b \cdot p + f \cdot p \mp 1 \end{pmatrix}\begin{pmatrix} e \cdot p \mp 1 \\ f \cdot p \mp 1 \end{pmatrix}\right)$$

For simplicity let $c = a+e$ and $d = b+f$. Then by applying lemma 17 to the first two pairs, we get:

$$b \cdot c \cdot p^2 - (a \cdot p \pm 1) \cdot (dp \mp 1) = 1$$

which implies that

$$\mp d = (a \cdot d - b \cdot c) \cdot p \mp a$$

Let $a \cdot d - b \cdot c = g$. Then a vertex that reduces to $\left(\binom{1}{0}\binom{0}{1}\binom{1}{1}\right)$ has the following form:

$$\left(\begin{pmatrix} a \cdot p \pm 1 \\ b \cdot p \end{pmatrix}\begin{pmatrix} c \cdot p \\ g \cdot p^2 \mp a \cdot p \mp 1 \end{pmatrix}\begin{pmatrix} e \cdot p \mp 1 \\ f \cdot p \mp 1 \end{pmatrix}\right)$$

Case $\left(\binom{1}{1}\binom{1}{0}\binom{0}{1}\right)$

We get a similar reduction.

Therefore by lemma 17

$$p^2 \leq Fibonacci(girth(\pi_p') + 2)$$

Therefore for large p, $girth(\pi_p') < p$, where p is the size of the faces on the surface of the tessellations, and therefore for large p, $snc(\pi_p') = girth(\pi_p')$.

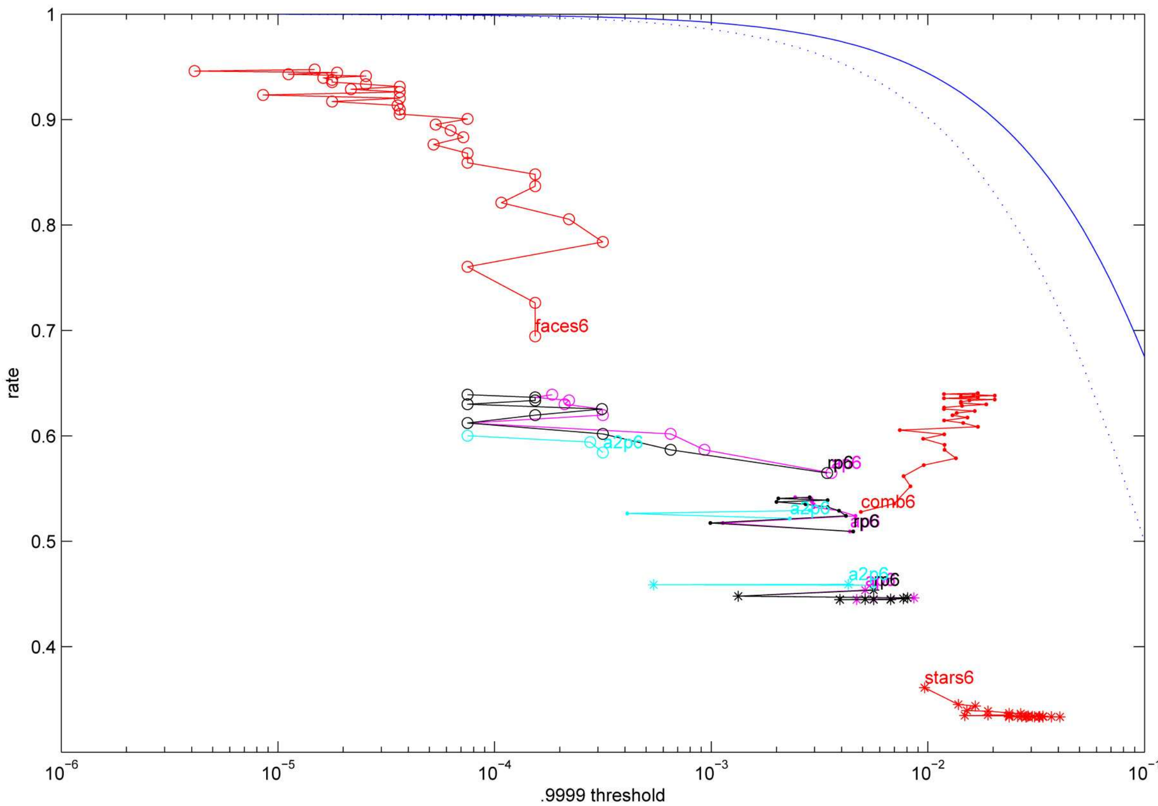
VI. Belief-propagation decoding

We decode the platonic codes using belief propagation by simulating the 4-ary symmetric channel as two independent binary symmetric channels in order to make them comparable to MacKay's sparse-graph quantum codes [8]. Each decoding simulation round either finds the correct decoding or a block error. Block error probability is calculated as a function of the flip probability f_m [8]. This is the probability with which we independently flip each bit. In particular we show the flip probability f_m at which the probability of decoding error is $10^{-4}(.9999)$.

We provide a summary of the simulated decodings of the Platonic codes and derived subfamilies in figure VI. The smooth curve shown in the figure is the Shannon limit and the dotted curve is the Gilbert-Varshamov bound for dual-containing quantum error-correcting codes [8].

All simulation labels start at Platonic $n = 6$. The red line represents the Platonic quantum codes without subtessellations. Their Z^{face} parity-check simulations starting at $n = 6$, are labeled $faces6$, and each additional matrix is denoted by a circle. Note that their rate approaches 1 as shown in remark 9. Their X^{vertex} parity-check simulations are labeled $stars6$, and each additional matrix is denoted by a star. Their rate approaches $\frac{1}{3}$ as shown in remark10.

Their Z^{face} and X^{vertex} average simulation performance is labeled as $comb6$ and each additional code decoding simulation is denoted by a dot. Their rate approaches $\frac{2}{3}$ as shown in remark 11. The average performance of the Platonic quantum codes without subtessellations is better than the Platonic quantum codes with subtessellations.



Results for the quantum codes derived from Platonic surfaces. The Y coordinate is the code rate. The X coordinate represents the flip probability f_m at which the probability of decoding block error is 10^{-4} (0.9999 threshold). All simulation labels start at Platonic $n = 6$. For more information about the labels, read the section results. The dotted curve shown in blue is the Gilbert-Varshamov bound for dual-containing quantum error-correcting codes and the smooth curve shown in blue is the Shannon bound.

We also obtain subfamilies of Platonic codes by subtessellating the Platonic $n-gons$. Each face in π'_n for $n \geqslant 6$ is subtessellated with pentagons in order to obtain better distance parameters. We obtain two subfamilies depending on the alignment of the subtessellations, both random and symmetric, and on the depth of the recursion. Symmetric subtessellations have neighboring $n-gons$ whose subtessellations are aligned.

The black line represents Platonic quantum codes with randomly aligned pentagon subtessellations. Their Z^{face} parity-check simulations are labeled as $rp6$, and each additional matrix is denoted by a circle. Their X^{vertex} parity-check simulations are labeled $rp6$, and each additional matrix is denoted by a star. Their X^{vertex} and Z^{face} average simulation performance starting at $n = 6$ is labeled $rp6$, and each additional code decoding simulation is denoted by a dot.

The purple line represents Platonic quantum codes with symmetrically aligned pentagon subtessellations, labeled as $ap6$, and the blue line represents codes with higher-level pentagon subtessellations, labeled as $a2p6$. The average decoding of the Platonic quantum codes without subtessellations is better than that of the Platonic quantum codes with subtessellations.

VII. Conclusion and Open Problems

We have addressed Mackay's conjecture about the existence of good families of dual-containing quantum LDPC error-correcting codes with nonzero rate, growing minimum distance and good decoding behavior. This family is derived from Platonic topological tessellations of 2-manifolds. We analyzed their sparsity, proved a logarithmic lower bound on their distance, showed the no-zero rate of their X^{vertex} and Z^{face} operators, and of their average combined rate, and simulated their decoding with belief-propagation.

With respect to the distance of the codes, it is a major open problem in the theory of Riemann surfaces to improve on the logarithmic lower bound of their systoles [10]. The 1-dimensional systole of a 2-dimensional manifold M is the infimum of all nontrivial 1-dimensional cycles in M.

It seems not likely that there exist families of topological quantum codes derived from regular algebraic tessellations of 2-manifolds that have provably better than logarithmic distance properties. Nevertheless it is possible that irregular or random tessellations might yield better short noncontractible distance bounds.

Quantum error-correction is foundational to the development of practical quantum computers. In this paper we have presented a good family of quantum low-density parity-check error-correcting codes derived from tessellations of topological surfaces. Physical implementations of quantum computers using these codes would require few sparse local physical interactions. Therefore the study of surface quantum LDPC codes can impact the development of scalable quantum computers.

References

[1] N. Biggs. Graphs with large girth. *ArsCombinatorica*. 25C: 73–80. 1988.

[2] R. Brooks. Spectral geometry and the cheeger constant. In *DIMACS Workshop Proceedings*. AMS. pp. 5–19, 1993.

[3] C. Bennet and P. Shor. Quantum Information Theory. *IEEE Trans. on Info. Theory. 44: 2724–2742, 1998.*

[4] A. Calderbank and P. Shor. Good quantum error-correcting codes exist. Phys. Rev. A, 54: 1098–1106, 1996.

[5] R. Gallager. Low-density parity-check codes. *PhD Thesis. Massachusetts Institute of Technology.* Cambridge, MA. 1963.

[6] A. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics. 303: 2–30, 2003.*

[7] D. MacKay. Good error correcting codes based on very sparse matrices. *IEEE Trans. on Info. Theory. 45: 399–431, 1999.*

[8] D. MacKay, G. Mitchison and P. McFadden. Sparse-graph codes for quantum error correction. *IEEE Trans. on Info. Theory. 50: 2315–2330, 2004.*

[9] D. MacKay, S. Willson and M. Davey. Comparison of Constructions of Irregular Gallager Codes. *IEEE Trans. on Communications. 47: 1449–1454, 1999.*

[10] J. Quine and P. Sarnak. “Extremal Riemann Surfaces,” presented at the American Mathematical Society special session. San Francisco, California. January 4-5, 1995.