Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane

Nicolas Delfosse, Gilles Zemor

Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane

Nicolas Delfosse and Gilles Zémor
{Nicolas.Delfosse, Gilles.Zemor}@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux, Université Bordeaux 1, France

April 10, 2011

Abstract

We are interested in percolation for a family of self-dual tilings of the hyperbolic plane. We achieve an upper bound on the critical probability for these tilings by taking appropriate finite quotients and associating them with a family of quantum CSS codes. We then relate the probability of percolation to the probability of a decoding error for these codes on the quantum erasure channel.

1 Introduction and overview

Let $\mathcal{G}$ be an infinite graph with edge set E and let μ_p be the probability measure on $\{0,1\}$ defined by $\mu_p(\{1\}) = p$. Consider the product space $\Omega = \{0,1\}^E$ endowed with the product probability measure $P_p = \mu_p^{\otimes E}$. Random events should be seen as subgraphs. Informally, we choose every edge of $\mathcal{G}$ with probability p independently of the other edges, and obtain a random subgraph. The edges of this subgraph are called *open* edges. Percolation theory is interested in the probability that a given edge e is contained in a infinite open connected component (an open *cluster*). This probability depends a priori on the edge e, but not if the graph $\mathcal{G}$ is edge-transitive, for example if $\mathcal{G}$ is the infinite square lattice (Figure 1). The central parameter in percolation theory is the *critical probability* p_c, defined as:

$$p_c(G) = \inf\{p \in [0,1],\ P_p(|\mathcal{E}(e)| = \infty) > 0\},$$

where $\mathcal{E}(e)$ denotes the open cluster containing edge e.

By a famous result of Kesten [9] that stayed a conjecture for 20 years, we have $p_c = 1/2$ for the square lattice. Computing the critical probability

exactly is usually quite difficult, but one class of graphs for which percolation is fairly well understood is trees: in particular it is straightforward to compute the critical probability of a regular tree of degree Δ, in which case we have $p_c = 1/(\Delta - 1)$.

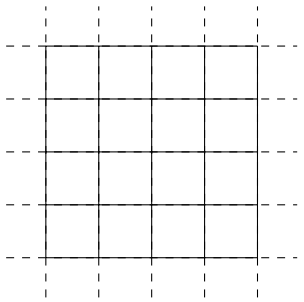

Figure 1: The square lattice

Percolation is relevant to classical coding theory because it can be related to the probability of a decoding error on the erasure channel. Specifically, the critical probability of the infinite Δ-regular tree is an upper bound on the highest tolerable channel erasure probability for the class of cycle codes of Δ-regular graphs. The cycle code of a finite Δ-regular graph is the linear code in the ambiant space $\{0,1\}^E$ generated by the *cycles* of the graphs, viewed as binary vectors of $\{0,1\}^E$ when E is the edge set. The probability of a decoding error on the erasure channel with erasure parameter p is the probability that a random set of edges for the probability measure $\mu_p^{\otimes E}$ contains a cycle. If the finite graph has no cycles of small length, then elementary cycles locally look like long paths. This point of view was taken up in [6, 15] where it was shown that if the channel erasure parameter p is above $p_c = 1/(\Delta - 1)$ then the probability of a decoding error must be bounded away from zero. In [14] it was shown that for some families of Δ-regular graphs a vanishing decoding error probability can be achieved as long as $p < p_c$.

In the present paper we are interested in percolation on an infinite family of graphs that generalize the square lattice. For any integer $m \geq 4$, we denote by $G(m)$ the planar graph which is regular of degree m and tiles the plane by elementary faces of length m. For $m = 4$ the graph $G(4)$ is exactly the square lattice. The local structure of the graph $G(5)$ is shown on Figure 2.

For $m > 4$ these graphs make up regular tilings of the hyperbolic plane. Interest in percolation on hyperbolic tilings was raised in a number of papers e.g. [1, 3] and determining their critical probability is highly non-trivial.

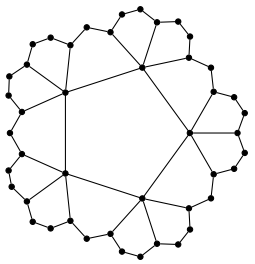

Figure 2: The local structure of the graph $G(5)$

Note that all graphs $G(m)$ are self-dual like the square lattice $G(m)$.

Our purpose is to relate the critical probability for these graphs to the decoding error probability under the *quantum* erasure channel for a well-defined family of quantum codes. Since the critical probability for the graphs $G(m)$ is unknown, this time our objective is a reverse import from coding theory: we will use the known channel capacity of the quantum erasure channel to derive an upper bound on the critical error probability p_c of the graphs $G(m)$. Our strategy is to use a family of finite graphs that locally look like $G(m)$. These graphs will define a family of quantum error-correcting codes that are quantum analogues of cycle codes of graphs (sometimes called surface codes, or topological codes). As in the classical case, qubits will be indexed by the edges of the finite graph. We will see that an uncorrectable quantum erasure pattern is a set of edges that must contain a special type of cycle (a non-trivial homological cycle) in the finite graph, and this event is in turn related to percolation on the infinite graph $G(m)$. Our main result is the following upper bound on the critical probability.

Theorem 1. *For $m \geq 5$, the critical probability of $G(m)$ is bounded from above as:*

$$p_c \leq \frac{2}{m}.$$

2 Percolation on hyperbolic lattices

Regular trees can be seen algebraically as a Cayley graph over a free group. The graphs $G(m)$ can similarly be constructed [12] by appealing to a group slightly more involved than a free group, namely the *triangular group* $T(m)$ defined by the presentation

$$< y, z \,|\, y^m = z^m = (yz)^2 = 1 >,$$

Such a group exists, we will see an explicit realization in the next section.

The left cosets of the subgroups $\langle y \rangle$, $\langle yz \rangle$ and $\langle z \rangle$ correspond respectively to vertices, edges and faces of the graph, or more precisely to the 2-dimensional complex consisting of the graph together with its m-edged faces. A vertex and an edge (or an edge and a face) are declared to be incident whenever the corresponding cosets are non-empty. In the next section we use this construction to obtain finite quotients of $G(m)$ by taking appropriate quotients of the triangular group.

Note that the graph $G(m)$ is self-dual. The dual graph $G^*(m)$ of $G(m)$ has the faces of the original graph for its vertices and two vertices of the dual are declared adjacent if the corresponding faces in the original graph have a common edge. Self-duality is apparent on the group $T(m)$ since it permutes the roles of the generators y and z.

The natural framework of this graph is hyperbolic geometry. In the Poincaré disc, we can construct a hyperbolic regular m-gon centered on 0 of angle $2\pi/m$. Denote by y the hyperbolic rotation of center 0 and angle $2\pi/m$ and by z the hyperbolic rotation of center a fixed vertex of the polygon and angle $2\pi/m$. When we apply the group of hyperbolic isometries generated by y and z to the polygon, we obtain the hyperbolic tesselation $G(m)$. Moreover it can be shown that the group generated by y and z is exactly the triangular group $T(m)$ defined above, and it is the automorphism group of the tiling.

We have the following easy bounds on p_c:

Proposition 2. *The critical probability p_c of $G(m)$ satisfies*

$$\frac{1}{m-1} \leq p_c \leq 1 - \frac{1}{m-1}.$$

Proof. We adapt the proof of [8] page 14 in the case of the square lattice.

Let O be a fixed vertex. To show the first inequality we can say that there are not more than $m(m-1)^{n-1}$ paths from O of length n in $G(m)$ and the probability of such an open path is p^n. So if $p < \frac{1}{m-1}$ the average length of an open path from O is not more than $\sum_{n=1}^{\infty} m(m-1)^{n-1}p^n < \infty$. In this case p is under the critical probability.

For the upper bound remark that if the ball of radius N is totally open and if the open edges of the complementary set of this ball never contains a closed circuit in the dual graph, then there is an infinite open path. The probability to have all the edges of a ball open is strickly positive for all N. For the second condition, we need to study the number of circuits of length n surrounding O in the complementary of the ball of radius N. We fix a shortest path from O to the circle centered on O of radius n. Every circuit

of length n surrounding O contains at least one vertex of the n vertices of the path, and there are at most $m-1$ successors of each bond. So the probability to have a closed circuit in the complementary set is not more than $\sum_{n\geq n_0} n(m-1)^n(1-p)^n$ where n_0 is the minimal length of this kind of circuit. We can take N and consequently n_0 as large as we want. If $p > 1-\frac{1}{m-1}$ and N is large enough then the sum is strickly less than 1. The two events in the ball and in its complementary set are independent so we have an infinite open cluster with positive probability. This gives the upper bound. □

3 Quotient graphs

To study percolation on the hyperbolic tiling $G(m)$, we need a family of increasingly big finite graphs which are locally the same as $G(m)$. We will use a family introduced by Širáň in [12].

Let $P_k(X) = 2\cos(k \arccos(X/2))$ be the k-th normalized Chebychev polynomial and $\xi = 2\cos(\pi/m^2)$. Let y and z be the matrices of $SL_3(\mathbb{Z}[\xi])$ defined by

$$y = \begin{pmatrix} P_m(\xi)^2-1 & 0 & P_m(\xi) \\ P_m(\xi) & 1 & 0 \\ -P_m(\xi) & 0 & -1 \end{pmatrix}$$

$$z = \begin{pmatrix} -1 & -P_m(\xi) & 0 \\ P_m(\xi) & P_m(\xi)^2-1 & 0 \\ P_m(\xi) & P_m(\xi)^2 & 1 \end{pmatrix}.$$

These two matrices generate the triangular group $T(m)$ [12, 11]. To obtain a finite graph we can reduce the entries of the matrices modulo a prime number p. The coefficients are in the ring $\mathbb{Z}[\xi]$ which is isomorphic to the quotient $\mathbb{Z}[X]/h(X)$ where h is the minimal polynomial of the algebraic integer ξ. Reducing coefficients modulo p, we obtain a group homomorphism from $SL_3(\mathbb{Z}[\xi])$ to $SL_3(\mathbb{F}_p[X]/(h(X))$. The image of $T(m)$ will be called $\bar{T}(m)$.

Let $\bar{G}(m)$ be the graph defined like $G(m)$ but with the group $\bar{T}(m)$, in other words the vertices, edges and faces of $\bar{G}(m)$ are defined as the left cosets of $\langle\bar{y}\rangle$, $\langle\bar{y}\bar{z}\rangle$ and $\langle\bar{z}\rangle$ respectively. There is a surjection s from $G(m)$ to $\bar{G}(m)$ which sends $u\langle y\rangle$ to $\bar{u}\langle\bar{y}\rangle$.

Following Širáň, let us define the *injectivity radius* of the graph $\bar{G}(m)$ as the largest integer r such that the restriction of the surjection s to a ball of radius r is one-to-one. It is shown in [12] that we can choose p so as to

have r arbitrarily large. Loosely speaking, Širáň's argument is that if two distinct vertices $u\langle y\rangle$ and $v\langle y\rangle$ in $G(m)$ have the same image under s then $u^{-1}v$ in $T(m)$ must project to the identity element in $\bar{T}(m)$. But this means that the matrix $u^{-1}v$ has polynomial entries that, properly reduced modulo $h(X)$, can only be expressed with coefficients at least one of which exceeds p: this implies that $u^{-1}v$ can only be expressed as a product of a large number of matrices y and z, which in turn means that the original vertices $u\langle y\rangle$ and $v\langle y\rangle$ have to be far apart in $G(m)$.

The above construction enables us to define a family of finite graphs $(G_r(m))_{r\geq 1}$ such that each graph $G_r(m)$ has injectivity radius at least r, for every integer r.

Let us now define random subgraphs of $G_r(m)$ through the product measure $\mu_p^{\otimes E_r}$, where E_r denotes the edge set of $G_r(m)$. In other words the open subgraph of $G(m)$ is created by declaring every edge open with independent probability p.

For any fixed edge e, let $\mathcal{E}_r(e)$ be the (possibly empty) connected component of the random subgraph of $G_r(m)$ that contains e and call it again the open cluster containing e. Let $f_r(p)$ be the probability that $|\mathcal{E}_r(e)| > r$. We have:

Proposition 3. *If $p < p_c(m)$ then $f_r(p)$ goes to 0 when r goes to infinity.*

Proof. Notice that the probability $1 - f_r(p)$ that the open cluster containing e has cardinality not more than r is the same for the random subgraph defined on the finite graph $G_r(m)$ and the random subgraph defined on the infinite graph $G(m)$. This is because this event depends only on the ball of radius r centered on an endpoint of e, and these balls in $G_r(m)$ and $G(m)$ are isomorphic.

We can therefore consider $f_r(p)$ to mean the probability of the event F_r that $|\mathcal{E}(e)| > r$ in the infinite graph $G(m)$. Now $(F_r)_{r\geq 1}$ is a decreasing sequence of events, and $P_p(\cap_{r\geq 1} F_r)$ is exactly the probability of percolation, which is 0 since we have supposed $p < p_c$. By monotone convergence we therefore have $f_r(p) = P_p(F_r) \to 0$. □

4 hyperbolic quantum codes and the quantum error channel

4.1 CSS codes

The quantum codes we will consider are CSS codes [4, 13]. A CSS code of length n is determined by two binary parity-check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ of

two classical codes of length n, C_X and C_Z respectively, with the property that every row of $\mathbf{H}_X$ is orthogonal to every row of $\mathbf{H}_Z$, in other words the row-spaces $C_X^\perp$ and $C_Z^\perp$ of $\mathbf{H}_X$ and $\mathbf{H}_Z$ are orthogonal subspaces of $\mathbb{F}_2^n$. The parameters of the associated quantum code are $[[n, k, d]]$, where n is the blocklength, k is its dimension and is given by $n - \dim C_X^\perp - \dim C_Z^\perp$, and the minimum distance d is given by the minimum weight of the non-zero vectors that are either in C_X but not in $C_Z^\perp$ or in C_Z but not in $C_X^\perp$.

4.2 The quantum codes $Q_r(m)$ associated to the graphs $G_r(m)$

Every finite graph $G_r(m)$ gives rise to a CSS quantum code $Q_r(m)$ whose coordinate set is the edge set E of the graph. We will have therefore a quantum code of length $n = |E|$. The matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ are defined as follows: the rows of $\mathbf{H}_X$ are in one-to-one correspondence with the vertices of the graph. Every vertex x yields a row of $\mathbf{H}_X$ whose support is exactly the set of edges incident to x. Every row of $\mathbf{H}_X$ therefore has weight m. The rows of the other matrix $\mathbf{H}_Z$ is in one-to-one correspondence with the set of faces of the graph. Every face yields a row whose support is equal to the set of edges making up the face. Since faces are m-gons, every row of $\mathbf{H}_Z$ also has weight m. It should be clear that rows of $\mathbf{H}_X$ and $\mathbf{H}_Z$ meet in either 0 or 2 edges, so any row of $\mathbf{H}_X$ is orthogonal to any row of $\mathbf{H}_Z$ and we have a quantum CSS code.

Note that the classical binary linear code C_X is exactly the cycle code of the graph $G_r(m)$. Note also that the code C_Z can be seen as the cycle code of the *dual graph* $G_r^*(m)$ of $G_r(m)$.

If v is the number of vertices $G_r(m)$, then the dimension of the cycle code C_X is $n - v + 1 = n - 2n/m + 1$. The graph $G_r(m)$ is easily seen to have the same number of faces as the number of vertices so that we have $\dim C_X = \dim C_Z$. Therefore:

Proposition 4. *The dimension k of the quantum code $Q_r(m)$ equals:*

$$k = \left(1 - \frac{4}{m}\right) n + 2.$$

We remark that for $m = 4$, the graph $G_r(4)$ is a combinatorial torus and the quantum code $Q_r(4)$ is a version of Kitaev's toric code [10]. For $m \geq 5$ the quantum codes $Q_r(m)$ have positive rate bounded away from zero and minimum distance at least $2r$ (see the remark after the proof of Proposition 7 below) which is a quantity which behaves as $\log n$. See [16] for a discussion of similar families of quantum codes (surface codes).

4.3 Quantum erasures

The *quantum erasure channel* can be defined in several equivalent ways. Loosely speaking, an erasure on coordinate i corresponds to the "loss" of this coordinate. On the erasure channel with transition parameter p, coordinates are declared "erased" independently and with probability p. In the CSS setting, the only feature we need to keep in mind [7] can be formulated as follows, identifying codewords with their supports: An erasure pattern is decodable if and only if it is a set of coordinate positions that contains no codeword of C_Z not in $C_X^{\perp}$ and no codeword of C_X not in $C_Z^{\perp}$.

The capacity of the quantum erasure channel of erasure parameter p is known to equal $1-2p$, see for example [2]. For our purposes, it can be shown that this translates into the following:

Proposition 5. *There does not exist a family of quantum CSS codes with rate $R > 1-2p$ such that, for the quantum erasure channel with parameter p, the erasure vector is decodable with vanishing probability when the blocklength n goes to infinity.*

5 Upper bound on the critical probability and proof of Theorem 1

Consider an arbitrary member of the family of quantum codes $Q_r(m)$ associated to the graphs $G_r(m)$. The erasure vector can be identified with a random set of edges of $G_r(m)$ and we will denote it by $\mathcal{E}$. According to the definition of $G_r(m)$ and the characterization of decodable erasure vectors given just above, the random erasure pattern $\mathcal{E}$ is decodable if and only if it either contains a cycle of $G_r(m)$ which is not a sum of faces, or $\mathcal{E}$, viewed as a set of edges of the dual graph $G_r^*(m)$ of $G_r(m)$, contains a cycle of $G_r^*(m)$ that is not a sum of faces of $G_r^*(m)$. Because the original graph $G(m)$ is self-dual, all arguments involving $G_r(m)$ will be seen to hold for its dual graph $G_r^*(m)$ and we will focus on the probability that the random erasure pattern $\mathcal{E}$ contains a cycle that is not a sum of faces in the original graph $G_r(m)$.

We would like to derive the upper bound on p_c in Theorem 1 by claiming the following: if $p < p_c$, then for the family of graphs $G_r(m)$, the probability that the random set of edges $\mathcal{E}$ contains a cycle which is not a sum of faces vanishes. If this is true, then the rate R of the quantum code $Q_r(m)$ must satisfy $R < 1-2p$ for every $p < p_c$ so that $R \leq 1-2p_c$ and Proposition 4 gives the result since $R = 1 - 4/m$.

Unfortunately, we do not know whether for every $p < p_c$, the erasure pattern $\mathcal{E}$ contains no cycle that is not a sum of faces with high probability. What we will prove however, is that if $\mathcal{E}$ contains a cycle that is not a sum of faces, then with high probability one of the representatives of this cycle modulo the space of faces must have very small weight. To violate the capacity of the erasure channel we will therefore use, not $Q_r(m)$ directly, but an "improved" version $Q'_r(m)$ of $Q_r(m)$ that we now introduce.

Proposition 6. *Let $Q_r(m)$ be a hyperbolic code, n its length and R its rate. Suppose $\rho \in]0, \frac{1}{2}[$ and $\alpha \in]0, 1[$ are such that*

$$h(\rho) < \alpha < \frac{R}{2},$$

where $h(\rho) = -\rho \log_2 \rho - (1-\rho)\log_2(1-\rho)$ denotes the binary entropy function. Then we can add αn rows to the parity-check matrix $\mathbf{H}_X$ and αn rows to the parity-check matrix $\mathbf{H}_Z$ of $Q_r(m)$ to obtain a CSS code $Q'_r(m)$ of length n, rate $R - 2\alpha$ and distance $d \geq \rho n$.

Proof. Denote by r_X and r_Z the dimension of the code $C_X^\perp$ and $C_Z^\perp$ respectively. We have $r_X = r_Z = \frac{2}{m}n - 1$.

We will construct a matrix $\mathbf{H}'_X$ by adding αn rows to the matrix $\mathbf{H}_X$ such that the rows of $\mathbf{H}'_X$ are orthogonal to the rows of $\mathbf{H}_Z$ and the rank of $\mathbf{H}'_X$ is $r_X + \alpha n$. Let C'_X be the code of parity-check matrix $\mathbf{H}'_X$.

For $\rho \in]0, 1/2[$, we define X_ρ by

$$X_\rho(\mathbf{H}'_X) = |\{v \in C'_X \backslash C_Z^\perp | w(v) \leq \rho n\}|.$$

We can write X_ρ as a sum a random variables to see that

$$E(X_\rho) = \sum_{\substack{v \in C_X \backslash C_Z^\perp \\ v \in B(0, \rho n)}} \frac{|\{\mathbf{H}'_X | v \in C'_X\}|}{|\{\mathbf{H}'_X\}|}.$$

Let $L_1, L_2, \ldots L_{r_X}$ be r_X rows of $\mathbf{H}_X$. The number of suitable matrices $\mathbf{H}'_X$ is the number of families $L'_1, L'_2, \ldots L'_{\alpha n}$ of vectors of $\mathbb{F}_2^n$ such that $L'_j \in C_Z$ for all j and $(L_1, L_2, \ldots L_{r_X}, L'_1, L'_2 \ldots, L'_{\alpha n})$ are linearly independant.

We can construct a suitable matrix $\mathbf{H}'_X$ if and only if $r_X + \alpha n \leq \dim(C_Z)$ this gives the condition $\alpha < (1 - \frac{4}{m}) - \frac{2}{n}$. In this case the number of matrices is

$$\prod_{i=r_X}^{r_X + \alpha n - 1} (2^{n - r_Z} - 2^i).$$

To evaluate the cardinality $|\{\mathbf{H}'_X | v \in C'_X\}|$ with v in $C_X \backslash C_Z^\perp$, it suffices to add the condition $L'_j \in \{v\}^\perp$ for all j. We get

$$\prod_{i=r_X}^{r_X+\alpha n-1} (2^{n-r_Z-1} - 2^i).$$

So we have

$$\frac{|\{\mathbf{H}'_X | v \in C'_X\}|}{|\{\mathbf{H}'_X\}|} = \frac{2^{n-r_X-r_Z-\alpha n}-1}{2^{n-r_X-r_Z}-1} \leq 2^{-\alpha n}.$$

This bound doesn't depend of v so we can give an upper bound on the expectation of X_ρ because we know that the number of words in the ball of radius ρn is less than $2^{nh(\rho)}$. We find

$$E(X_\rho) \leq 2^{n(h(\rho)-\alpha)}.$$

If $\alpha > h(\rho)$ the mean goes to 0. Since X_ρ has integer values there exists $\mathbf{H}'_X$ such that $X_\rho(\mathbf{H}_X) = 0$. We obtain a CSS code of matrix $\mathbf{H}'_X$ with $r'_X = r_X + \alpha n$ and $\mathbf{H}_Z$ unchanged such that the minimum weight of a word of $C'_X \backslash C_Z^\perp$ is at least ρn.

We want to repeat this argument to have the minimum weight of a word of $C'_Z \backslash C_X'^\perp$ higher than ρn. It suffices to choose $\alpha < \frac{1}{2}(1 - \frac{4}{m}) + \frac{1}{n}$ because in this case $r_Z + \alpha n < \dim(C_X)$. □

Let $\mathcal{E}$ be an erasure. We can write

$$\mathcal{E} = \mathcal{E}_C + \mathcal{E}_P \tag{1}$$

where $\mathcal{E}_C$ is the sum of the connected components which do not cover a cycle which is not a sum of faces. The *problematic* part $\mathcal{E}_P$ of $\mathcal{E}$ is the union of the others components.

In the graph $G_r(m)$, define $g_r(p)$ to be the probability that that the open cluster $\mathcal{E}_r(e)$ covers a cycle which is not a sum of faces. We have:

Lemma 7. *If $p < p_c(m)$ then $g_r(p)$ goes to 0 when r goes to infinity.*

Proof. Recall that $f_r(p)$ denotes the probability that $|\mathcal{E}_r(e)| > r$. We prove that $g_r(p) \leq f_r(p)$ and apply Proposition 3. If $|\mathcal{E}_r(e)| \leq r$ then the open cluster $\mathcal{E}_r(e)$ is included in a ball of radius r of the graph $G_r(m)$. Since this ball is isomorphic to the ball of the same radius in the planar graph $G(m)$, it is planar. In any planar graph every cycle is a sum of faces so $\mathcal{E}_r(e)$ covers a cycle which is not a sum of faces only if $|\mathcal{E}_r(e)| > r$, hence $g_r(p) \leq f_r(p)$. □

Remark: By the same planarity argument as above, every cycle of length less than $2r$ in the graph $G_r(m)$ is a sum of faces. This proves that the distance of the quantum code $Q_r(m)$ is at least $2r$.

Proposition 8. *If we consider the erasure channel of probability $p < p_c$ then $\forall \varepsilon > 0, \exists r_0 \in \mathbb{N}$ such that if $r \geq r_0$ then the expectation of the weight of $\mathcal{E}_P$ defined as in* (1) *satisfies*

$$E(|\mathcal{E}_P|) \leq \varepsilon n.$$

Proof. For any edge e of $G_r(m)$, let $X_{r,e}$ be the random variable which take the value 1 if the connected component $\mathcal{E}_r(e)$ of e in $G_r(m)$ covers a cycle which is not a sum of faces and the value 0 otherwise. Then we have:

$$|\mathcal{E}_P| = \sum_e X_{r,e}.$$

To conclude note that $E(X_{r,e}) = g_r(p)$ and apply Lemma 7. □

The next Lemma states that if the erasure vector $\mathcal{E}$ has a large "problematic" part $\mathcal{E}_P$ then it must be correctable by the "improved" codes given by Proposition 6.

Lemma 9. *Let $Q'_r(m)$ be one of the quantum codes given by Proposition 6 and let d be its minimum distance. Suppose the part $\mathcal{E}_P$ of the erasure vector $\mathcal{E}$ defined in* (1) *satisfies $|\mathcal{E}_P| < d$. Then $\mathcal{E}$ is correctable by $Q'(m)$.*

Proof. Denote by C_X and C_Z the binary linear codes associated with the quantum code $Q_r(m)$ and by C'_X, C'_Z their binary sub-codes associated to the quantum code $Q'_r(m)$ introduced in Proposition 6 and defined by augmenting the parity-check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ of $Q_r(m)$.

If the erasure vector $\mathcal{E}$ covers an element x of $C'_X \backslash C'^{\perp}_Z$ then x must belong to $C_X \backslash C_Z^{\perp}$ *i.e.* x is a cycle of $G_r(m)$ which is not a sum of faces. The restriction of this cycle to $\mathcal{E}_C$ defined in (1) is another cycle y and the definition of $\mathcal{E}_C$ implies that y is a sum of faces. We obtain that $x + y$ is included in $\mathcal{E}_P$ with $y \in C_Z^{\perp} \subset C'^{\perp}_Z$, i.e. $x + y \in C'_X \backslash C'^{\perp}_Z$ but this is a contradiction whenever the part $\mathcal{E}_P$ of the erasure $\mathcal{E}$ has weight strictly less than the minimum distance d of the improved code $Q'(m)$. □

We now conclude the proof of our main result, Theorem 1.

Let $R = 1 - \frac{4}{m}$ and fix $p < p_c$. For any α such that $0 < \alpha < R/2$, Proposition 6 gives us a quantum code $Q'(m)$ with minimum distance $d \geq \rho n$

where $\rho = h^{-1}(\alpha/2)$ and rate $R - 2\alpha$. For such a code the probability of a decoding error satisfies:

$$P_{err} \leq P(|\mathcal{E}_P| \geq \rho n).$$

For any $\varepsilon > 0$ we can take r large enough so that Proposition 8 applies, and together with Markov's inequality we have

$$P_{err} \leq P(|\mathcal{E}_P| \geq \frac{\rho}{\varepsilon}\varepsilon n) \leq \frac{\varepsilon}{\rho}.$$

For every $\varepsilon > 0$ we take $\rho = \sqrt{\varepsilon}$. Then $\rho(\varepsilon)$ and $\frac{\varepsilon}{\rho(\varepsilon)}$ simultaneously go to zero when ε goes to zero. Defining α by $\alpha = 2h(\rho)$ and choosing a decreasing sequence of ϵ's that tends to zero, we obtain a family of quantum codes $Q'_r(m)$ with decoding error probability tending to zero and rate $R-2\alpha$ tending to R.

By Proposition 5 we can conclude that the quantity $R - 2\alpha$ is under the capacity of the quantum erasure channel. So we have $1 - \frac{4}{m} - 2\alpha \leq 1 - 2p$ if $p < p_c$. Since α can be taken to tend to 0, we find $1 - \frac{4}{m} \leq 1 - 2p$ for all p such that $p < p_c$. Hence $1 - \frac{4}{m} \leq 1 - 2p_c$.

Acknowledgment

This work was supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project).

References

[1] I. Benjamini and O. Schramm, "Percolation beyond $\mathbb{Z}^d$, many questions and few answers," *Elect. Comm. in Probab.*, 1 pp. 71–82, 1996.

[2] C. H. Bennet, D. P. Divincenzo and J.A Smolin, "Capacities of Quantum Erasure Channels," *Phys. Rev. Lett.*, 78:3217–3220, 1997.

[3] S.K. Baek, P.Minnhagen and B. J. Kim, "Percolation in hyperbolic lattices," *Phys. Rev. E*, 79, 011124, 2009.

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

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

[6] L. Decreusefond and G. Zémor, "On the error-correcting capabilities of cycle codes of graphs," *Combinatorics, Probability & Computing*, vol. 6, pp. 27–38, 1997.

[7] M. Grassl, T. Beth and T. Pellizzari, "Codes for the Quantum Erasure Channel," *Phys. Rev. A*, vol. 56, no. 1, July 1997, pp. 33–38.

[8] G. Grimmett, *Percolation*. Springer-Verlag, 1989.

[9] H. Kesten, "The critical probability of bond percolation on the square lattice equals 1/2," *Comm. Math. Phys.*, 74, pp. 41–59, 1980.

[10] A. Kitaev, Quantum error correction with imperfect gates, in *Proc. 3rd nt. Conf. of Quantum Communication and Measurement*, 1997.

[11] J. Mennicke, "Eine Bermerkung über Fuchssche Gruppen," *Invent. Math.*, 2, pp. 301-305, 1967.

[12] J. Širáň, "Triangle group representations and constructions of regular maps," *Proc. London Math. Soc.*, Vol. 82, No 3, pp. 513–532, 2001.

[13] A. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. Lond. A*, 452:2551, 1996.

[14] J-P. Tillich and G. Zémor, "Optimal cycle codes constructed from Ramanujan graphs," *Siam Journal on Discrete Math.*, vol. 10, No 3, pp. 447–459, 1997.

[15] G. Zémor, "On iterative decoding of cycle codes of graphs," *Codes, Systems, and Graphical Models*, in Vol. 123 of IMA Volumes in Math. and its Applications, Springer-Verlag, 2001, pp. 311–326.

[16] G. Zémor, "On Cayley graph, surface codes and the limit of Homological coding for quantum error correction," in *Coding and Cryptology, (IWCC 2009)*, LNCS 5557, Springer pp. 259–273.