A Note on the Minimum Distance of Quantum LDPC Codes

Nicolas Delfosse¹, Zhentao Li², and Stéphane Thomassé³

¹ Département de Physique, Université de Sherbrooke,
Sherbrooke, Québec, J1K2R1, Canada
nicolas.delfosse@usherbrooke.ca
² Département d’Informatique UMR CNRS 8548, École Normale Supérieure, France
zhentao.li@ens.fr
³ LIP, UMR 5668, École Normale Supérieure de Lyon - CNRS - UCBL - INRIA,
Université de Lyon, France
stephan.thomasse@ens-lyon.fr

Abstract. We provide a new lower bound on the minimum distance of a family of quantum LDPC codes based on Cayley graphs proposed by MacKay, Mitchison and Shokrollahi [14]. Our bound is exponential, improving on the quadratic bound of Couvreur, Delfosse and Zémor [3]. This result is obtained by examining a family of subsets of the hypercube which locally satisfy some parity conditions.

1 Introduction

A striking difference between classical and quantum computing is the unavoidable presence of perturbations when we manipulate a quantum system, which induces errors at every step of the computation. This makes essential the use of quantum error correcting codes. Their role is to avoid the accumulation of errors throughout the computation by rapidly identifying the errors which occur.

One of the most satisfying construction of classical error correcting codes capable of a rapid determination of the errors which corrupt the data is the family of Low Density Parity–Check codes (LDPC codes) [9]. It is therefore natural to investigate their quantum generalization. Moreover, Gottesman remarked recently that this family of codes can significantly reduce the overhead due to the use of error correcting codes during a quantum computation [10]. Quantum LDPC codes may therefore become an essential building block for quantum computing.

Quantum LDPC codes have been proposed by MacKay, Mitchison, and MacFadden in [15]. One of the first difficulty which arises is that most of the families of quantum LDPC codes derived from classical constructions lead to a bounded minimum distance, see [20] and references therein. Such a distance is generally not sufficient and it induces a poor error-correction performance.

Only a rare number of constructions of quantum LDPC codes are equipped with an unbounded minimum distance. Most of them are inspired by Kitaev toric codes constructed from the a tiling of the torus [12] such as, color codes.
which are based on 3-colored tilings of surfaces \cite{1}, hyperbolic codes which are defined from hyperbolic tilings \cite{8,21}, or other constructions based on tilings of higher dimensional manifolds \cite{8,11}. These constructions are based on tilings of surfaces or manifolds and their minimum distance depends on the homology of this tiling. The determination of the distance of these codes is thus based on homological properties and general bounds on the minimum distance can be derived from sophisticated homological inequalities \cite{6,4}.

In this article, we study a construction of quantum LDPC codes proposed by MacKay, Mitchison and Shokrollahi \cite{15} based on Cayley graphs and studied in \cite{3}. This family does not rely on homological properties and thus homological method cited earlier seems impossible to apply. We relate their minimum distance to a combinatorial property of the hypercube. Then, using an idea of Gromov, we derive a lower bound on the minimum distance of these quantum codes which clearly improves the results of Couvreur, Delfosse and Zémor \cite{3}.

The remainder of this article is organized as follows. In Section 2 we recall the definition of linear codes and a construction of quantum codes based on classical codes. Section 3 introduces the quantum codes of MacKay, Mitchison and Shokrollahi \cite{14}. In order to describe the minimum distance of these quantum codes based on Cayley graphs, we introduced two families of subsets of these graphs that we call borders and pseudo-borders in Section 4. We are then interested in the size of pseudo-borders of Cayley graphs. In Section 5, we reduce this problem to the study of \( t \)-pseudo-borders of the hypercube, which are a local version of pseudo-borders. Theorem 1, proved in Section 6, establishes a lower bound on the size of \( t \)-pseudo-border. As a corollary, we derive a lower bound on the minimum distance of Cayley graphs quantum codes.

## 2 Minimum Distance of Quantum Codes

A code of length \( n \) is defined to be a subspace of \( \mathbb{F}_2^n \). It contains \( 2^k \) elements, called codewords, where \( k \) is the dimension of the code. The minimum distance \( d \) of a code is the minimum Hamming distance between two codewords. By linearity, it is also the minimum Hamming weight of a non-zero codeword. This parameter plays an important role in the error correction capability of the code. Indeed, assume we start with a codeword \( c \) and that \( t \) of its bits are flipped. Denote by \( c' \) the resulting vector. If \( t \) is smaller than \( (d - 1)/2 \) then we can recover \( c \) by looking for the closest codeword to \( c' \). Therefore, we can theoretically correct up to \( (d - 1)/2 \) bit-flip errors. The parameters of a code are denoted \([n, k, d]\).

Every code can be defined as the kernel of a binary matrix \( H \), called a parity–check matrix of the code. Alternatively, a code can be given as the space generated by the rows of a matrix called a generator matrix of the code. For instance, the following parity–check matrix defines a code of parameter \([7, 4, 3]\).

\[
H = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}
\] \hspace{1cm} (1)

The code which admits \( H \) as a generator matrix has parameters \([7, 3, 4]\).