Fault-tolerant quantum computation

Author: Alba Guasch Espinosa, aguasces24@alumnes.ub.edu
Facultat de Física, Universitat de Barcelona, Diagonal 645, 08028 Barcelona, Spain.

Advisors: Sofyan Iblisdir, iblisdir@fqa.ub.edu and Alba Cervera, alba.cervera@bsc.es

Abstract: This work analyzes fault-tolerance in quantum computation, namely the use of quantum error correction to prevent the propagation and multiplication of errors in a quantum circuit. A simple quantum circuit for Bell-state preparation is studied and considered in order to theoretically determine the threshold probability p_{th} using Steane code. This threshold corresponds to the maximum admissible error probability for each physical component gate of the circuit. Two error-correction schemes are compared: one applying a single correction at the end of the circuit, another implementing intermediate corrections. In both cases, a threshold of the order of $p_{\text{th}} \sim 10^{-4}$ is obtained, corresponding to a fidelity of 99,99% per gate. But only the second scheme is suitable for large circuits. The theoretical threshold is compared with recent experimental results, demonstrating the practical feasibility of fault-tolerant quantum computation.
Keywords: Quantum Computing, Quantum Error Correction, Quantum Circuits, Qubits.
SDGs: This work is related to the Sustainable Development Goal (SDG) 4: Quality Education.

I. INTRODUCTION

Quantum computation is a computational model based on the principles of quantum mechanics, offering significant advantages over classical computation. Phenomena such as superposition, entanglement, and quantum interference make it possible to design algorithms that can solve certain problems more efficiently than classical methods, for instance, Shor's algorithm [1] and Grover's algorithm [2]. However, quantum systems are extremely sensitive to their environment, meaning that their state can be altered, leading to loss of quantum information. For this reason, it is essential to implement error detection and correction mechanisms [3] in order to guarantee the viability of large-scale quantum computation.

Quantum error correction (QEC) protects quantum information against environmental noise and errors arising from quantum operations themselves. The main idea of fault-tolerant quantum computation is to replace an ordinary quantum circuit with one where actual computations and error correction alternate. In this manner, all along the computation, the number of errors remains low enough that QEC eliminates them before their accumulation and propagation cause irreversibly incorrect results.

The goal of this work is to understand this idea in detail. We start with an overview of the quantum circuit model, including qubits, quantum gates, and a representative example. Next, in Section III, we introduce quantum error correcting codes. Section IV focuses on fault-tolerant quantum computation, describing the implementation of fault-tolerant gates, the threshold theorem, and its application to the example circuit in Section II. We also provide six appendices, which include proofs of the no-cloning and Knill-Laflamme theorems, a discussion of the Steane code, and diagrams illustrating two quantum circuits.

II. QUANTUM CIRCUIT MODEL

Digital Computation. Digital computation is a computational model in which information is represented using bits, which can take the values 0 or 1. Operations on these bits are performed using logical gates, such as NOT, AND, and OR gates [4]. There exist universal sets of gates, for example $\{NOT, AND\}$, that allow the construction of any logical operation. However, for certain problems, such as those mentioned in the introduction, classical computation becomes inefficient, since the number of required operations grows exponentially with the number of bits involved. This motivates the use of quantum computation, for which, in some cases, the number of operations can scale polynomially. Within this computational model, information is encoded in qubits, which can exist in superpositions of the computational basis states, $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, where a and b are complex coefficients satisfying $|a|^2 + |b|^2 = 1$.

Quantum Gates and Universal Gate Sets. Quantum gates are unitary operations acting on one or more qubits and constitute the fundamental building blocks of quantum circuits. Among the most relevant single-qubit gates are the X gate, which exchanges the states $|0\rangle \leftrightarrow |1\rangle$, and the Z gate, which introduces a phase change by leaving the state $|0\rangle$ unchanged and multiplying the state $|1\rangle$ by a factor of -1. A particularly important gate is the Hadamard gate (H), which allows the generation of quantum superpositions. Its action on the computational basis states is given by $H\,|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, H\,|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Among two-qubit gates, the Controlled-NOT ($CNOT$) gate is especially important because it can create entanglement between qubits. In this gate, one qubit acts as the control and the other as the target. The target qubit remains unchanged if the control is in the state $|0\rangle$, and is flipped if the control is in the state $|1\rangle$.

There exist universal sets of quantum gates from which

any unitary operation can be approximated. A common example is $\{H, CNOT, S, T\}$, where S and T are single-qubit gates that modify the phase of a qubit, but their detailed action will not be discussed in this work.

Example: Bell State Circuit. Quantum gates are combined to construct quantum circuits that describe the evolution of one or more qubits. Fig. 1 shows an example of a simple but particularly important circuit. It consists of two qubits initially prepared in the state $|0\rangle$. A Hadamard gate is applied to the first qubit, followed by a $CNOT$ gate, where the first qubit acts as the control and the second as the target. The combined action of these gates transforms the initial state $|00\rangle$ into the Bell state $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, which exhibits maximal entanglement: the outcome of a measurement on one qubit fully determines the outcome on the other.

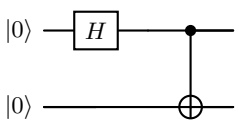

FIG. 1: Quantum circuit for the preparation of a Bell state.

III. QUANTUM ERROR CORRECTION

Error model. In any quantum computing system, physical operations are affected by environmental noise and finite accuracy, which can lead to errors during computation. These errors are not limited to quantum gates; they can also occur during the initial preparation of qubits, the measurement process, or even during the storage of quantum information.

Consider a qubit in an arbitrary state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. The two basic errors that can alter the state of a qubit are: (i) bit-flip errors, which exchange the states $|0\rangle$ and $|1\rangle$, transforming the state of the qubit into $|\psi\rangle = a\,|1\rangle + b\,|0\rangle$ and are represented by the X gate; and (ii) phase-flip errors, which change the relative phase between $|0\rangle$ and $|1\rangle$ without altering the measurement probabilities, resulting in the state $|\psi\rangle = a\,|0\rangle - b\,|1\rangle$, and correspond to the Z gate. Both errors can occur simultaneously on the same qubit, combining a bit flip and a phase flip, which is equivalent to the XZ operation.

Although physical noise is continuous, and in principle a qubit could experience an infinite number of errors, a fundamental result in quantum computing states that any arbitrary physical error affecting a qubit can be expressed as a linear combination of just four operators. These are the identity I (no error), the bit flip X, the phase flip Z, and the combination of both, XZ [3]. This follows from the fact that the Pauli operators form a basis for the space of single-qubit operators.

Preparation of Encoded States. Errors that arise during the execution of a quantum circuit can be detected and corrected using quantum error correcting codes [3]. The fundamental principle of error correction is to introduce redundancy so that the presence of errors can be identified. In classical computation, this is straightforward, as information can simply be copied; for example, in the three-bit repetition code, the logical states 0 and 1 are represented as 000 and 111, respectively.

In quantum computation, the idea is similar but more complex due to the no-cloning theorem (see Appendix A), which forbids the duplication of an unknown quantum state $|\psi\rangle$. Consequently, quantum error correction is based on encoding a logical qubit into multiple entangled physical qubits. This constitutes the first step in implementing quantum error correction. Given a qubit in the state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, the encoding process generates a logical state $|\psi_L\rangle = a\,|0_L\rangle + b\,|1_L\rangle$, where $|0_L\rangle$ and $|1_L\rangle$ are the encoded states defined over n physical qubits, whose explicit form depends on the code employed.

Quantum codes are conventionally denoted using the notation $[n, k, d]$, where k logical qubits are encoded into n physical qubits, and d represents the code distance, which determines its capacity to detect and correct errors. A code with distance d can detect up to $d-1$ errors and correct up to $\frac{d-1}{2}$ arbitrary errors. A simple example is the three-qubit bit-flip code, which encodes a single logical qubit into three physical qubits. The logical states are defined as $|0_L\rangle \equiv |000\rangle$ and $|1_L\rangle \equiv |111\rangle$, so that an arbitrary one logical qubit state transforms as $a\,|000\rangle + b\,|111\rangle$. This encoding can be implemented using a quantum circuit illustrated in Appendix B.

This code does not offer protection against phase-flip errors. One of the central challenges in quantum error correction is to protect quantum information simultaneously against both bit-flip and phase-flip errors. For this reason, more powerful quantum codes have been developed, such as the Shor [5] and Steane codes [6]. In this work, the seven-qubit Steane code is employed, a $[7, 1, 3]$ code that encodes a single logical qubit into seven physical qubits and can correct any error affecting a single qubit. A logical or encoded block is defined as the set of physical qubits representing a logical qubit. Additional details of the code, including the explicit expressions for the logical states $|0_L\rangle$ and $|1_L\rangle$, are provided in Appendix C. Although their preparation requires a more sophisticated circuit, the goal remains the encoding of an arbitrary qubit $|\psi\rangle$ into a logical state $|\psi_L\rangle$.

Error Detection and Correction. Once quantum information is encoded, operations can be performed on logical qubits. However, due to the inevitable presence of noise, errors can occur at any time. To prevent them from accumulating and corrupting the logical state, error detection and correction must be applied frequently throughout the circuit. These procedures identify the error and the qubit affected, so that the appropriate operation can be applied to recover the original state. Since any arbitrary physical error can be decomposed into a superposition of elementary errors, correcting this discrete set suffices to correct any single-qubit error.

The error correction process is divided into two stages:

error detection and correction. The presence of errors is detected by measuring a set of special operators known as the code generators. The encoded states are eigenvectors of these operators with eigenvalue +1. When an error occurs, some of these eigenvalues change to -1. The complete set of measurement outcomes $(\beta_1, \beta_2, ..., \beta_m)$, with $\beta_i = \pm 1$ and m the number of generators, is called the error syndrome. This syndrome indicates which type of error has occurred and on which qubit, as each error produces a characteristic syndrome. Once the syndrome is identified, the inverse of the detected error is applied, which for Pauli errors coincides with the error itself.

To illustrate this mechanism, we consider the three-qubit bit-flip code. The logical state is $|\psi_L\rangle = a\,|000\rangle + b\,|111\rangle$. Measuring the generators Z_1Z_2 and Z_2Z_3 allows one to identify which qubit has suffered a bit-flip error and to apply the correction. Table I shows the possible generator outcomes, the associated syndrome, the affected qubit, and the required correction.

TABLE I: Syndromes and corresponding corrections for the three-qubit bit-flip code.

Z_1Z_2	Z_2Z_3	Syndrome	Affected Qubit	Correction
+1	+1	(+1,+1)	-	I
+1	-1	(+1,-1)	3	X_3
-1	+1	(-1,+1)	1	X_1
-1	-1	(-1,-1)	2	X_2

In more complex codes, such as the Steane code, the procedure is conceptually the same but more elaborate. This code has six independent generators, so the error syndrome consists of six outcomes, allowing the detection and localization of both bit-flip and phase-flip errors on any of the seven physical qubits. The generators and measurement circuit are presented in Appendix D, where we explain how syndromes are obtained using auxiliary qubits, avoiding the destruction of quantum information in the logical qubits during measurement.

The ability of a quantum code to detect and correct errors is not trivial. The Knill-Laflamme theorem provides the mathematical foundation that guarantees errors can be reliably identified and corrected [7]. The detailed proof of this theorem is shown in Appendix E.

IV. FAULT-TOLERANCE

In the previous section, we showed that frequent application of error detection and correction mechanisms makes it possible to mitigate the effects of noise in quantum systems. However, error correction alone does not guarantee the reliability of the system, since quantum error-correcting codes can only correct a limited number of errors. Moreover, the correction procedures themselves may introduce additional errors. For instance, the Steane code is capable of correcting a single error; if two or more errors occur within the same block during a logical operation, the code can no longer correct them. For this reason, fault-tolerance quantum computation is necessary, whose goal is to design quantum operations in such a way that errors do not propagate within blocks.

Fault-tolerant Quantum Gates. An encoded quantum gate is a logical operation performed on encoded qubits and is implemented through physical operations on the constituent qubits of each block. A gate is considered fault-tolerant if a single physical error occurring during its execution results in at most one error per physical qubit in each encoded block, ensuring that the error remains correctable by the code.

Although not always possible, transversality is a desirable strategy for achieving fault tolerance. A gate is transversal when it can be implemented by applying independent physical gates to each qubit of the block, so that any single-qubit error cannot propagate to other qubits within the same block. In the Steane code, many fundamental gates possess this property. For instance, the logical Pauli operators and the Hadamard gate are realized as tensor products of the corresponding single-qubit physical gates applied across all seven qubits of the block: $Z_L = Z^{\otimes 7}$, $X_L = X^{\otimes 7}$ and $H_L = H^{\otimes 7}$. Similarly, the logical $CNOT$ gate, denoted by $CNOT_L$, can be implemented transversally between two encoded blocks by applying a physical $CNOT$ gate to each corresponding pair of qubits in the control and target blocks.

The H, S, and $CNOT$ gates are transversal and thus inherently fault-tolerant. The T gate, which is required to complete the universal set, is not directly transversal but can be implemented fault-tolerantly using more complex procedures. Consequently, it is possible to implement any logical operation in a fault-tolerant manner. Transversality enables the issue of fault tolerance to be reduced to a counting problem.

Threshold Theorem. The threshold theorem states that a quantum circuit with D quantum gates can be simulated, by another quantum circuit, with an overall error probability of at most ϵ using $O(\text{poly}(\log \frac{D}{\epsilon})\, D)$ physical gates, provided that each physical gate has an error probability p below a threshold p_{th}. This theorem is crucial because it shows that scalable quantum computation is possible despite the presence of noise, as long as the physical error rate per gate p is below a threshold. It provides the theoretical foundation for fault-tolerant quantum computation and justifies the use of QEC.

The basic idea behind this theorem is that, without error correction, the probability of an error occurring in a single physical gate is simply p. When using the Steane code for example, fault-tolerant quantum gates combined with error correction reduce this probability to order $O(p^2)$, since the code can correct any error in any single physical qubit of a block. Consequently, a logical error arises only when errors affecting two different qubits occur. Consider, for instance, a $CNOT$ gate acting on two encoded blocks, followed by a fault-tolerant correction, and examine all scenarios in which two faults are

present within a single encoded block at any given stage of the circuit. There are seven possible scenarios leading to two errors within a single encoded block: two preexisting errors, one preexisting error and one error during the $CNOT$ operation, two errors during the $CNOT$, one error during the $CNOT$ and one during the syndrome measurement, two errors during the syndrome measurement, one error during the syndrome measurement and one during the recovery step, and two errors during the recovery. Since each logical operation involves multiple physical gates that can introduce errors, we denote by c_i the number of distinct ways in which scenario i can result in two errors within the encoded block. The total number of two-error combinations is then $c = \sum_i c_i$, giving a probability of roughly cp^2 for two errors within a block. The use of fault-tolerant quantum gates is essential, as a single error in a logical gate could otherwise generate two or more errors within the same encoded block, which the correcting code would no longer be able to correct.

If $cp^2 < p$, the use of error-correcting codes and fault-tolerant operations places the computation below the fault-tolerance threshold. In this regime, even an arbitrarily small but finite separation from the threshold is sufficient: concatenating the code leads to a super-exponential suppression of logical errors, so reliable computation can be achieved with only a polynomial overhead. To illustrate this, a qubit initially encoded in seven physical qubits can be re-encoded into seven blocks, yielding 49 physical qubits. After two levels of concatenation, the error probability is approximately $c(cp^2)^2$. Extending this to k concatenation levels, the error probability per encoded gate can be estimated as $\delta^{(k)} = \frac{(cp)^{2^k}}{c}$.

To ensure that the total error of a circuit with D gates remains below ϵ, we require $\delta^{(k)} \leq \frac{\epsilon}{D}$. From this inequality, the necessary concatenation level k can be determined, provided that the error rate of physical components p is below a critical threshold $p_{\text{th}} = \frac{1}{c}$. This value, known as the fault-tolerance threshold, ensures that if $p < p_{\text{th}}$, the overall computational error can be reduced drastically to reach any desired precision by increasing the level of concatenation.

Concatenating codes increases the circuit size, as each original logical gate is replaced by a fully encoded procedure. If d denotes the maximum number of physical operations required to implement an encoded gate, then after k concatenation levels the total number of physical operations scales as d^k. Expressing k in terms of the desired error ϵ and the number of gates D, the overall circuit size grows polylogarithmically, $O(\text{poly}(\log \frac{D}{\epsilon})\, D)$, which ensures a controlled and efficient scaling.

Application of the Threshold Theorem. This subsection applies the threshold theorem to a simple circuit preparing the logical Bell state $|\Phi^+\rangle_L$ (Fig. 1) in order to obtain an upper bound on the threshold error probability p_{th}. Two error-correction schemes are compared: (i) a single error-correction step applied at the end of the circuit, and (ii) intermediate error-correction steps performed after each logical gate. The aim is to analyze their effect on the fault-tolerance threshold p_{th}.

All physical operations are assumed to fail independently with probability p. Each logical qubit is encoded into a block of seven physical qubits using the Steane code. The circuit consists of two logical gates, a Hadamard and a $CNOT$, both implemented transversally, implying seven physical operations per logical gate. The explicit implementation of these gates on the encoded system is presented in Appendix F.

Error correction in the Steane code requires the measurement of six operators, each involving about ten physical operations, followed by an additional seven operations for the recovery step. Consequently, the approximate number of fault locations during an error-correction cycle in a single block is $c_0 \approx 6 \cdot 10 + 7 \approx 70$. As a result, even after error correction, a failure in any of these c_0 operations may introduce a residual error in the encoded block. Therefore, each block is assumed to contain an initial error with probability proportional to $c_0 p$.

To estimate the probability that the error-correction procedure itself introduces two errors within the same block, all combinations of two independent failures during this process are considered: both occurring during syndrome measurement, one during syndrome measurement and another during recovery, or both during recovery. Since approximately 60 physical operations are involved in the syndrome measurement and 7 in the recovery step, this leads to $c_{corr} \approx \binom{60}{2} + 60 \cdot 7 + \binom{7}{2} \approx 2 \cdot 10^3$.

In both schemes, the threshold is estimated in terms of the parameter c, which quantifies the number of pairs of physical faults capable of producing errors on distinct qubits within a single block. The analysis reduces to counting these fault combinations for each scheme.

SCHEME (i): Single error correction, shown in Fig. 2.

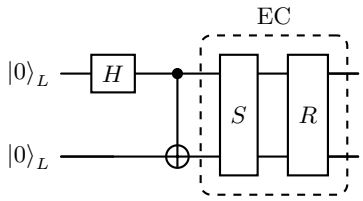

FIG. 2: Quantum circuit for preparing the Bell state $|\Phi^+\rangle_L$ with one error-correction. S, R, and EC denote the syndrome measurement, recovery, and error-correction procedure.

The contributions to the parameter c are listed below. Factors of 2 arise from considering both logical blocks.

1. Two initial residual errors, one in each block: $c_1 \approx c_0^2 \approx 70^2$.
2. One residual error and one fault occurring during the logical gates (14 physical operations): $c_2 \approx 2\, c_0 \cdot 14 \approx 2 \cdot 10^3$.
3. Two faults during the gates: $c_3 = \binom{14}{2} \approx 10^2$.
4. One fault during a logical gate and one during the syndrome measurement: $c_4 \approx 14 \cdot (60 \cdot 2) \approx 2 \cdot 10^3$.
5. Two faults during the final error-correction step: $c_5 = 2\, c_{corr} \approx 4 \cdot 10^3$.

SCHEME (ii): Intermediate error correction (Fig. 3).

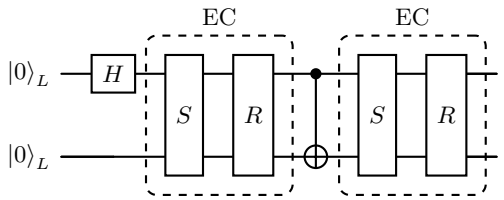

FIG. 3: Quantum circuit for preparing the Bell state $|\Phi^+\rangle_L$ with intermediate error correction. S, R, and EC denote the syndrome measurement, recovery, and error-correction.

1. One initial residual error and one fault during H_L: $c_1 \approx c_0 \cdot 7 \approx 490$.
2. Two faults during H_L: $c_2 = \binom{7}{2} = 21$.
3. One fault during H_L and one during the subsequent syndrome measurement: $c_3 \approx 7 \cdot 60 = 420$.
4. Two faults during the error-correction step following H_L: $c_4 = 2\, c_{corr} \approx 4 \cdot 10^3$.
5. Two residual errors, one in each block, prior to the application of $CNOT_L$: $c_5 \approx c_0^2 \approx 70^2$.
6. One residual error and one fault during $CNOT_L$: $c_6 \approx 2\, c_0 \cdot 7 \approx 10^3$.
7. Two faults during $CNOT_L$: $c_7 = \binom{7}{2} = 21$.
8. One fault during $CNOT_L$ and one during the syndrome measurement: $c_8 \approx 7 \cdot (60 \cdot 2) \approx 10^3$.
9. Two faults during the final error-correction step: $c_9 = 2\, c_{corr} \approx 4 \cdot 10^3$.

By summing all contributions, one obtains $c \sim 1,30 \cdot 10^5$ for scheme (i) and $c \sim 1,60 \cdot 10^5$ for scheme (ii). Corresponding thresholds, defined as $p_{\text{th}} = \frac{1}{c}$, are $p_{(\text{i})} \approx 7,7 \cdot 10^{-5}$ and $p_{(\text{ii})} \approx 6,3 \cdot 10^{-5}$. Both values are of the same order of magnitude, $p_{th} \sim 10^{-4}$, corresponding to a physical gate fidelity of $F = 1 - p \approx 0,9999$. The threshold is slightly more restrictive in the scheme with intermediate error corrections, since in a simple circuit the error correction process itself can introduce more faults than the gates. However, in larger and more complex circuits, periodic error correction is essential to prevent the accumulation and propagation of errors, thereby ensuring scalable and fault-tolerant quantum computation.

V. DISCUSSIONS AND CONCLUSIONS

This work has examined the importance of quantum error detection and correction, as every physical operation in a quantum circuit can introduce errors. In particular, we analyzed the Steane code. Since this code is capable of correcting a finite number of faults, and the correction processes may introduce additional errors, fault-tolerant quantum computation becomes necessary. Its goal is to prevent the propagation and accumulation of errors within encoded gates, ensuring that errors remain within the limits that the code can correct. The central importance of the threshold theorem lies in guaranteeing that, as long as physical error rates p remain below a threshold p_{th}, arbitrarily long quantum computations can be performed reliably using fault-tolerant schemes, with a very low total error rate and only a polynomial overhead. This theorem provides the theoretical foundation that makes scalable quantum computation possible.

Although these thresholds were initially experimentally unattainable, recent advances in gate fidelities have changed this scenario. For instance, the theoretical fidelity obtained with the Steane code using the quantum circuit for Bell-state preparation, $F=$ 99,99%, is comparable to current experimental values: superconducting qubits reach around 99.92% in single-qubit gates and up to 99.4% in two-qubit gates [8]; neutral atoms in optical tweezers achieve two-qubit gate fidelities of approximately 99.5% [9]; and trapped ions show especially high fidelities, with 99.99912(8)% in single-qubit gates and 99.97(1)% in two-qubit gates [10]. These results indicate that fault-tolerant quantum computation is beginning to become experimentally feasible, enabling the implementation of reliable, large-scale quantum circuits.

Acknowledgments

I would like to express my gratitude to my supervisors, Sofyan Iblisdir and Alba Cervera, for their dedication and guidance in the course of this work and to my parents, sister and friends for their support and encouragement.

[1] Shor, P.W., *Algorithms for quantum computation: discrete logarithms and factoring*, Proc. 35th Annu. Symp. Found. Comput. Sci., 124–134 (1994).
[2] Grover, L.K., *A fast quantum algorithm for database search*, Proc. 28th Annu. ACM Symp. Theory Comput., 212–219 (1996).
[3] Nielsen, M.A., Chuang, I.L., *Quantum Computation and Quantum Information*, Cambridge Univ. Press (2010).
[4] Sipser, M., *Introduction to the Theory of Computation*, 3rd ed., Cengage Learning (2012).
[5] Shor, P.W., *Scheme for reducing decoherence in quantum memory*, Phys. Rev. A 52, R2493–R2496 (1995).
[6] Steane, A.M., *Error-Correcting Codes in Quantum Theory*, Phys. Rev. Lett. 77, 793–797 (1996).
[7] Knill, E., Laflamme, R., *A Theory of Quantum Error-Correcting Codes*, Phys. Rev. Lett. 84, 2525–2528 (2000).
[8] Barends, R. et al., *Superconducting quantum circuits at the surface code threshold*, Nature 508, 500–503 (2014).
[9] Evered, S.J. et al., *High-fidelity parallel entangling gates on a neutral-atom quantum computer*, Nature 622, 268–272 (2023).
[10] Blatt, R., Home, J., *Scalable high-fidelity all-electronic control of trapped-ion qubits*, PRX Quantum 6(1), 010101 (2025).

Computació quàntica tolerant a fallades

Author: Alba Guasch Espinosa, aguasces24@alumnes.ub.edu
Facultat de Física, Universitat de Barcelona, Diagonal 645, 08028 Barcelona, Spain.

Advisors: Sofyan Iblisdir, iblisdir@fqa.ub.edu and Alba Cervera, alba.cervera@bsc.es

Resum: Aquest treball analitza la tolerància a fallades en la computació quàntica, és a dir, l'ús de la correcció d'errors quàntics per evitar la propagació i la multiplicació d'errors en un circuit quàntic. S'estudia un circuit quàntic senzill per a la preparació d'un estat de Bell amb l'objectiu de determinar teòricament el llindar de probabilitat p_{th} mitjançant el codi d'Steane. Aquest llindar correspon a la probabilitat màxima d'error admissible per a cada component físic del circuit. Es comparen dos esquemes de correcció d'errors: un que aplica una única correcció al final del circuit i un altre que implementa correccions intermèdies. En ambdós casos s'obté un llindar de l'ordre de $p_{th} \sim 10^{-4}$, equivalent a una fidelitat del 99,99% per porta. Tanmateix, només el segon esquema és adequat per a circuits grans. El llindar teòric es compara amb resultats experimentals recents, mostrant la viabilitat pràctica de la computació quàntica tolerant a fallades.
Paraules clau: Computació Quàntica, Correcció d'Errors Quàntics, Circuits Quàntics, Qubits.
ODSs: Aquest TFG està relacionat amb l'Objectiu de Desenvolupament Sostenible (ODS) 4: Educació de qualitat.

Objectius de Desenvolupament Sostenible (ODSs o SDGs)

1. Fi de la es desigualtats		10. Reducció de les desigualtats	
2. Fam zero		11. Ciutats i comunitats sostenibles	
3. Salut i benestar		12. Consum i producció responsables	
4. Educació de qualitat	X	13. Acció climàtica	
5. Igualtat de gènere		14. Vida submarina	
6. Aigua neta i sanejament		15. Vida terrestre	
7. Energia neta i sostenible		16. Pau, justícia i institucions sòlides	
8. Treball digne i creixement econòmic		17. Aliança pels objectius	
9. Indústria, innovació, infraestructures			

Appendix A: No-Cloning Theorem

The no-cloning theorem states that there exists no physical process capable of perfectly copying an arbitrary unknown quantum state.

Assume that there exists a universal quantum cloning machine described by a unitary operator U. This machine acts on a system consisting of the state to be cloned, $|\psi\rangle$, a qubit in a fixed state $|0\rangle$, and an auxiliary qubit prepared in a fixed state $|s\rangle$, such that $U(|\psi\rangle \otimes |0\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \otimes |s'\rangle$. Since the machine is assumed to be universal, the same transformation must work for any other quantum state $|\phi\rangle$, that is, $U(|\phi\rangle \otimes |0\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle \otimes |s''\rangle$. Because U is a unitary operator, it preserves inner products. Therefore, the inner product between the initial states must be equal to the inner product between the final states. Before the cloning operation, we have $\langle \psi \otimes 0 \otimes s \mid \phi \otimes 0 \otimes s \rangle = \langle \psi \mid \phi \rangle \langle 0 \mid 0 \rangle \langle s \mid s \rangle = \langle \psi \mid \phi \rangle$ since the auxiliary state $|s\rangle$ is normalized. On the other hand, after the cloning operation, the inner product becomes $\langle \psi \otimes \psi \otimes s' \mid \phi \otimes \phi \otimes s'' \rangle = (\langle \psi \mid \phi \rangle)^2 \langle s' \mid s'' \rangle$.

Conservation of the inner product implies $\langle \psi \mid \phi \rangle = (\langle \psi \mid \phi \rangle)^2 \langle s' \mid s'' \rangle$. Since $|\langle s' \mid s'' \rangle| \leq 1$, the only way this equality can hold for arbitrary states $|\psi\rangle$ and $|\phi\rangle$ is if $\langle \psi \mid \phi \rangle = 0$ or $\langle \psi \mid \phi \rangle = 1$. The first case corresponds to orthogonal states, while the second means that $|\psi\rangle$ and $|\phi\rangle$ are identical.

Hence, a unitary transformation can only clone perfectly states that are either identical or orthogonal. Since quantum states are in general unknown and may be non-orthogonal, it follows that perfect cloning of an arbitrary quantum state is impossible.

Appendix B: Encoding Circuit for the Three-Qubit Bit-Flip Code

Fig. 4 shows the quantum circuit used to encode a logical qubit with the three-qubit bit-flip code. The circuit consists of the qubit $|\psi\rangle$ to be encoded together with two auxiliary qubits, both initially prepared in the fixed state $|0\rangle$. Two $CNOT$ gates are then applied, using the original qubit as the control and each auxiliary qubit as a target. The resulting logical state is $|\psi_L\rangle = a\,|000\rangle + b\,|111\rangle$.

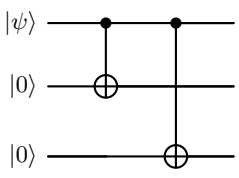

FIG. 4: Encoding circuit for a three-qubit bit-flip code.

Appendix C: The Steane Code

The Steane code belongs to the family of CSS (Calderbank–Shor–Steane) codes, which are constructed from two classical linear codes C_1 and C_2 such that $C_2 \subseteq C_1$. A classical linear code $[n, k, d]$ enables the detection and correction of errors in a system by encoding k information bits into a total of n bits, where the code distance d determines the maximum number of errors that can be detected and corrected. In this framework, the code C_1 is used to correct bit-flip errors, while the dual code $C_2^{\perp}$, whose vectors are orthogonal to all vectors in C_2, corrects phase-flip errors.

For the Steane code, the classical Hamming code $C \equiv$[7,4,3] is employed, with the particular property that $C = C_1 = C_2^{\perp}$, which simplifies its construction due to its symmetry.

A linear code can be defined as the set of all vectors x of length n that satisfy $Hx = 0$, where H is called the parity-check matrix. This matrix provides a systematic way to detect and correct errors. The parity-check matrix of the Hamming code is:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

From this matrix, the logical states of the Steane code can be obtained. The explicit expressions of these states are:

$$\begin{aligned} |0_L\rangle = \frac{1}{\sqrt{8}}(&|0000000\rangle + |1010101\rangle + |0110011\rangle \\ &+ |1100110\rangle + |0001111\rangle + |1011010\rangle \\ &+ |0111100\rangle + |1101001\rangle) \end{aligned}$$

$$\begin{aligned} |1_L\rangle = \frac{1}{\sqrt{8}}(&|1111111\rangle + |0101010\rangle + |1001100\rangle \\ &+ |0011001\rangle + |1110000\rangle + |0100101\rangle \\ &+ |1000011\rangle + |0010110\rangle) \end{aligned}$$

Moreover, the Steane code also belongs to the family of stabilizer codes. In this formalism, a quantum code is defined as the subspace of states that remain invariant under a set of operators called stabilizers, which belong to the Pauli group on n qubits, G_n.

Thus, instead of describing a quantum state directly as a superposition of vectors, we characterize it by the operators that leave it invariant. A stabilizer g is an operator that satisfies:

$$g\,|\psi_L\rangle = |\psi_L\rangle\,.$$

Let S be the group generated by a set of independent stabilizers. The encoded subspace is defined as:

$$V_S = \{|\psi_L\rangle : g_i\,|\psi_L\rangle = |\psi_L\rangle\,, \quad \forall g_i \in S\}.$$

For this subspace V_S to be non-trivial, the stabilizer generators must satisfy two conditions: they must all commute with each other, and none of them can be $-I$.

Within this stabilizer formalism, the Steane code is described as the set of states that remain invariant under the action of a set of six independent operators, $g_1, ..., g_6$, which act on the seven physical qubits. These operators will be presented again and explained in detail in later sections.

Appendix D: Measurement of the Steane Code Generators

In the context of the Steane code, error detection requires the measurement of six operators, which are listed in Table II. Each generator acts on the seven physical qubits comprising a single encoded block.

TABLE II: Generators of the Steane code.

Generator	Operator
g_1	$IIIXXXX$
g_2	$IXXIIXX$
g_3	$XIXIXIX$
g_4	$IIIZZZZ$
g_5	$IZZIIZZ$
g_6	$ZIZIZIZ$

Contrary to the classical scenario, in quantum mechanics it is not possible to directly measure the qubits of an encoded state without destroying the quantum information they carry. For this reason, auxiliary qubits, commonly referred to as ancillas, are employed to perform the measurement of the code generators. Each ancilla is dedicated to measure a specific generator. In this configuration, information about the error syndrome is extracted exclusively from the ancillas, leaving the encoded qubits unaltered and thereby preserving the quantum state.

Fig. 5 illustrates the quantum circuit used to measure the Steane code generators and obtain the corresponding error syndrome. In the diagram, the six upper qubits represent the ancillas, one for each generator of the code, while the seven lower qubits correspond to the physical qubits of the encoded block.

Appendix E: Knill–Laflamme Theorem

Let C be the subspace defining a quantum code, and let P denote the projector onto C. Suppose the system is affected by a quantum noise channel ϵ, which can be described by a set of operators $\{E_i\}$, called Kraus operators, such that the action of the noise on any state ρ is given by $\epsilon(\rho) = \sum_i E_i \rho E_i^\dagger$. Here, ρ is a state in the code space C.

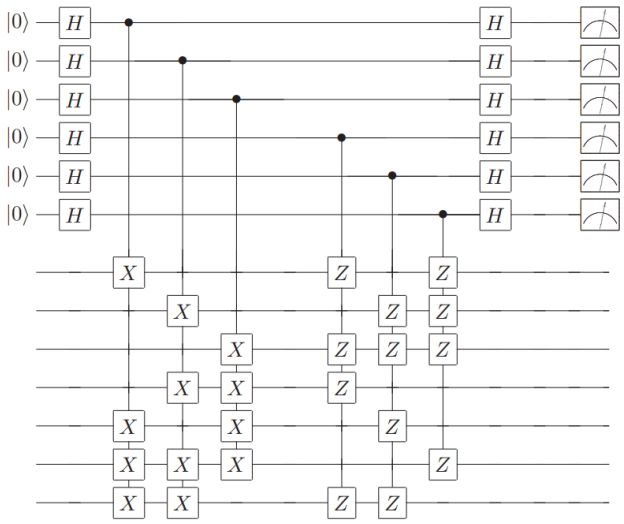

FIG. 5: Quantum circuit for measuring the generators of the Steane code.

The Knill–Laflamme theorem provides a necessary and sufficient condition for quantum error correction. It states that there exists a recovery operation R capable of correcting the effect of the noise on all states of the code C if and only if

$$PE_i^\dagger E_j P = \alpha_{ij} P \tag{E1}$$

where α_{ij} is a Hermitian matrix.

Proof of sufficiency. Assume that the above condition holds. Since α is Hermitian, it can be diagonalized by a unitary matrix u, so that

$$d = u^\dagger \alpha u \tag{E2}$$

We now define new Kraus operators as linear combinations of the original ones:

$$F_k \equiv \sum_i u_{ik} E_i$$

These operators F_k constitute a new set of Kraus operators representing the same noise channel ϵ.

Using the Eq. (E1) and (E2) one finds

$$PF_k^\dagger F_l P = d_{kl} P. \tag{E3}$$

Since d is diagonal, the off-diagonal elements vanish. Therefore, in the new error basis, each F_k maps the code into a subspace that is separate from the others.

Applying the expression $A = U\sqrt{A^\dagger A}$, known as the polar decomposition, to $F_k P$, where A is an operator and U is a unitary matrix, and using Eq. (E3) together with the properties of projectors, we obtain

$$F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}}\, U_k P, \tag{E4}$$

Thus, when F_k acts on any vector in the code space C, it maps it unitarily to another subspace C_k and scales

its norm by $\sqrt{d_{kk}}$. Hence, the encoded information is preserved within each error subspace.

To determine the error subspace in which the system lies, and therefore to identify which error has occurred, we define the rotated projectors using Eq. (E4):

$$P_k \equiv U_k P U_k^\dagger = \frac{F_k P}{\sqrt{d_{kk}}} U_k^\dagger \tag{E5}$$

These projectors are mutually orthogonal, $P_l P_k = 0$ for $l \neq k$, which means that each error subspace can be perfectly distinguished. Indeed, using Eq. (E5) and (E3):

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll}\, d_{kk}}} = \frac{U_l d_{kl} P U_k^\dagger}{\sqrt{d_{ll}\, d_{kk}}} = 0, \quad (l \neq k)$$

since $d_{kl} = 0$ for $l \neq k$.

The recovery operator R, designed to correct the noise affecting the system, is constructed so that, depending on the outcome of the syndrome measurement P_k, it applies the unitary correction $U_k^\dagger$ to return the state to the original code subspace C.

$$R(\sigma) \equiv \sum_k U_k^\dagger P_k \sigma P_k U_k$$

Applying this recovery to $\sigma = \epsilon(\rho) = \sum_l F_l \rho F_l^\dagger$, and simplifying using the properties of the projectors, one obtains

$$R(\sigma) = \left(\sum_k d_{kk} \right) \rho \propto \rho$$

If the noise ϵ is trace-preserving, the proportionality constant is 1, and therefore the recovery reproduces the original state ρ exactly.

Proof of necessity. Suppose there exists a recovery operation R that corrects the effect of the noise ϵ on the code subspace C. This means that for any state ρ in the code, the combined action of ϵ followed by R returns the original state, up to a normalization factor. Mathematically, this can be written as $(R \circ \epsilon)(\rho) \propto \rho$.

Since we are interested in the action of the operation within the code subspace, we can restrict to states of the form $P\rho P$. In this case, the correction hypothesis reads

$$R \circ \epsilon\,(P\rho P) = \beta P \rho P, \tag{E6}$$

where β is a constant, because both sides depend linearly on ρ.

We express the noise channel ϵ and the recovery operation R in terms of their Kraus operators:

$$\epsilon(P\rho P) = \sum_i E_i (P\rho P) E_i^\dagger$$

$$R(\tau) = \sum_j R_j \tau R_j^\dagger.$$

Substituting these expressions into Eq. (E6) gives

$$\sum_{ij} R_j E_i (P\rho P) E_i^\dagger R_j^\dagger = \beta P \rho P. \tag{E7}$$

This equation shows that, when restricted to the code subspace, the set of operators $\{R_j E_i\}$ acts in the same way as a single Kraus operator proportional to the projector P, specifically $\sqrt{\beta} P$. In other words, both quantum channels are equivalent when acting on states contained in C.

If two sets of Kraus operators represent the same operation, their elements are related by a linear transformation. Therefore,

$$R_k E_i = \beta_{ki} P \rightarrow R_k E_i P = \beta_{ki} P \tag{E8}$$

Taking the adjoint of this expression gives

$$P E_i^\dagger R_k^\dagger = \beta_{ki}^* P.$$

Using these relations, one can compute

$$P E_i^\dagger R_k^\dagger R_k E_j P = \beta_{ki}^* \beta_{kj} P.$$

Summing over the index k,

$$\sum_k P E_i^\dagger R_k^\dagger R_k E_j P = \left(\sum_k \beta_{ki}^* \beta_{kj} \right) P.$$

If the recovery operation R is trace-preserving, its Kraus operators satisfy $\sum_k R_k^\dagger R_k = I$, so that

$$P E_i^\dagger E_j P = \left(\sum_k \beta_{ki}^* \beta_{kj} \right) P.$$

Defining $\alpha_{ij} \equiv \sum_k \beta_{ki}^* \beta_{kj}$, we finally obtain the condition

$$P E_i^\dagger E_j P = \alpha_{ij} P.$$

Moreover, the matrix α is Hermitian, since $\alpha_{ij} = \alpha_{ij}^\dagger$. This demonstrates that the existence of a recovery operation R necessarily implies that the error operators satisfy the Knill–Laflamme condition.

Appendix F: Transversal Implementation of the H and CNOT Gates

Fig. 6 illustrates a diagram in which a Hadamard gate is applied to the first encoded block using the Steane code, followed by the application of a $CNOT$ gate between the two encoded blocks. This representation explicitly shows how these logical operations are implemented transversally.

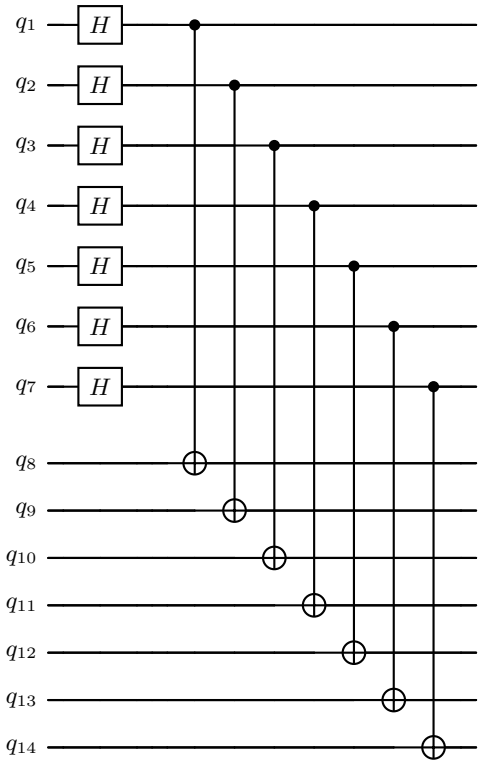

FIG. 6: Transversal implementation of the Hadamard and $CNOT$ gates in the Steane code.