# Semiclassical grounds of the Calderbank-Shor-Steane quantum error correction codes.

Manuel Avila Aoki[1]
[1] Centro Universitario UAEM Valle de Chalco, UAEMex, Estado de Mexico, México
Phone (55) 59 71 49 40 E-mail:mavilaa@uaemex.mx

## Abstract

**A valid Calderbank-Shor-Steane (CSS) error correction code requires two classical linear codes for the preparation of the initial state (codewords). This code allow to correct for certain errors caused by an unwanted interaction which produces a degraded quantum state. However, this initial seven qubits encoding can be obtained from a maximally entangled Bell state $(|\mathbf{0000000}\rangle + |\mathbf{1111111}\rangle)/\sqrt{2}$ through an operation $\mathbf{H_{int}}$ whose explicit expression is derived in the present work. The price the CSS syndrome has to pay due to its classical grounds is that the operator $\mathbf{H_{int}}$ is not unitary. In other words, $\mathbf{H_{int}}$ is not a valid quantum gate i. e. this does not represent a logical operation. Consequently, the final state is not completely robust for the standard cryptography of Quantum Computation.**

**Besides to be a non unitary operator, $\mathbf{H_{int}}$, is not reversible introducing with this dissipative effects that destroy the coherence in the quantum computer. Additionally, this operator is not invariant under rotations of the protector qubits inducing then preferred directions of the propagation of the logical information. These are indeed the reasons that prompt us for extending the semi classical CSS quantum error correction codes formalism to a pure quantum Hamming codes.**

Key words: Quantum information; quantum computation; linear classical correction codes; encoding; syndrome; quantum error correction codes

## I. INTRODUCTION

Quantum information processing (QIP) can be used to solve problems in physics simulation, crypto analysis, and secure communications for which there are no known efficient solutions based on classical information processing. There are several well-established physical models that, under ideal conditions, allow for exact realizations of quantum information and its manipulation [1]. However, real physics systems never behave exactly like the ideal models. One of the main problems is the environmental noise, which is due to incomplete isolation of the system of the rest of the world. Another problems are the control errors, which are caused by calibration errors and random fluctuations in control parameters.

Soon after Peter Shor published the efficient quantum factoring algorithm with its applications to breaking commonly used public-key cryptosystems, Andrew Steane [2] and Shor [3] gave the first constructions of quantum error-correcting codes. These codes make it possible to store quantum information so that one can reverse the effects of the most likely errors. They showed that it is possible to protect against environmental noise when storing or transmitting information. Thus, immediately arose the question whether it is possible to quantum compute in a fault-tolerant manner. The answer was given by the accuracy threshold theorems [4]-[14]. According to these theorems, if the effects of all errors are sufficiently small per qubit and computation step, then it is possible to process quantum information arbitrarily accurately with reasonable resources overheads. The requirement on errors is quantified by a maximum tolerable error rate called the threshold. All threshold theorems require that errors at different times and locations be independent and that the basic computational operations can be applied in parallel. The sense in which quantum information can be accurately stored in a noisy system needs to be defined without reference to an observer. There are two ways of accomplishing this task. The first is to define stored information to be the information that can, in principle, be extracted by a quantum decoding procedure. The second is to explicitly define subsystems (particle-like aspects of the quantum device) that contain the desired information. The quantum error correction codes theory deals with the first approach.

Among the most important quantum correction codes are the so called CSS codes which are built in terms of two classical correction codes. CSS codes are an important subclass of the more general class of stabilizer codes. Stabilizer codes are useful because they

make it easy to determine which Pauli product errors are detectable and because they can be interpreted as special types of classical, linear codes. In other words, the CSS codes are a method of converting certain classical error correcting codes into quantum ones.

In the past, there have been intuitive approaches for justifying the necessity of extending the CSS codes to a genuine quantum Hamming codes [15]. However, these attempts have failed due to the lack of a self consistent formalism. The purpose of this letter is to make explicit that the CSS codes are plagued of inconsistencies. This is done in a natural fashion by employing a self consistent formalism. Thus, we prove that the CSS interaction $H_{int}$ is not unitary. This makes that $H_{int}$ becomes unsuitable for performing logical operations. Another deficiency is that this operator is not invariant under rotations of the logical qubits. Besides such interaction introduces unwelcome noise by heating the quantum computer, destroying with this its coherence necessary for the processing of the information. The way we proceed is as follows: in Section 2 it is given a brief account of the CSS codes. Meanwhile, the explicit calculation of the usual expression for the Steane seven qubits encoding is done in the Appendix. In Section 3 it is derived an expression for the operator $H_{int}$ which to act over the maximally entangled Bell-like state $(|0000000\rangle + |1111111\rangle)/\sqrt{2}$, prepares the seven qubits code words. In the same section it is shown that $H_{int}$ is not unitary. The paper is concluded by giving a discussion on the obtained results.

## II. CALDERBANK-SHOR-STEANE CODES

The CSS quantum codes extend the classical linear codes and let us identify and correct large qubit errors, i.e., errors described by Pauli matrices. CSS quantum codes derive from classical linear codes. In order to construct a CSS code it is necessary to start from two classical linear codes, let say $C_1[n, k_1]$ and $C_2[n, k_2]$ such that $C_2 \subset C_1$. The sets $C_1$ and $C_2$ are defined as the set of possible code words generated by that code The resulting code is a quantum code called CSS($C_1/C_2$) which encodes $k_1 - k_2$ logical qubits in $n$ "physical qubits", so this code is $[n, k_1 - k_2]$ [16]. Observe that the codes $C_1$ and $C_2$ can be dual as long as $C_2 \subset C_1$. In this case $C_1 = C_1[n, k]$ and $C_2 = C_2[n, n - k]$ and the resulting code is CSS$[n, 2k-n]$. In general, for a CSS code encoding $k_1 - k_2$ qubits, we map the first $2^{k1-k2}$ binary numbers (starting from 0) to code words in $C_1$. The encoding is a vector space spanned by all states constructed by taking a codeword $x \in C_1$ and then adding to it the whole of $C_2$, that is

$$|x +_2 C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x +_2 y\rangle, \qquad (1)$$

where $+_2$ is a *mod*2 sum and $| C_2 |$ is the number of elements in $C_2$. In Figure 1 it is sketched the quantum circuit representing the whole CSS quantum error correction codes.

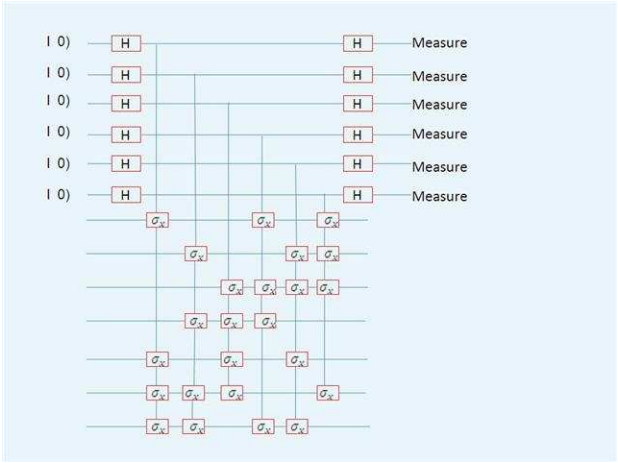


**Figure 1**: A quantum circuit for measuring the error syndrome for the CSS code. The bottom 7 lines represent the 7-qubit register, which encodes a single logical qubit. The 6 lines represent the ancilla

In order to derive the CSS wave function to be transmitted out we start with the $C_1[7, 4]$ classical Hamming linear code and its $C_2[7, 3]$ dual with which it is constructed the corresponding [7,1]CSS($C_1/C_2$). The code words of $C_1[7, 4]$ are spanned by the columns of the generator matrix

$$\mathbf{G} = \begin{pmatrix} 0001 \\ 0010 \\ 1100 \\ 1000 \\ 0110 \\ 0101 \\ 1011 \end{pmatrix} \qquad (2)$$

The code words of C2[7, 3] are spanned by the rows of the check matrix (see the Glossary)

$$\mathbf{H} = \begin{pmatrix} 0001111 \\ 0110011 \\ 1010101 \end{pmatrix} \qquad (3)$$

To prove that $C_2 \subset C_1$ is straightforward if we observe that the rows of H are constructed by adding rows of $\mathbf{G}^T$. That is, 0001111 = 0011001 $+_2$ 0010110, 0110011 = 0010110 $+_2$ 0100101, and 1010101 = 0010110 $+_2$ 1000011 where use has been made of the binary sums $0 +_2 0 = 0$, $0 +_2 1 = 1$, and $1 +_2 1 = 0$.

A good initialization protocol must assure that all of the superposed states in the initial state have the same

probability of occurrence. Thus, the Steane seven qubits encoding that must be transmitted is

$$|\psi\rangle_{\mathrm{CSS}} = \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L) = \frac{1}{4}\Big[\Big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle + |0111100\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle\Big) + (|1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle + |1000011\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle)\Big]. \quad (4)$$

In the Appendix an explicit derivation of the above $|0\rangle_L$ and $|1\rangle_L$ Steane states is given. We observe that this derivation is not done in the majority of works dealing with the CSS syndrome

## III. NON UNIVERSALITY OF THE SEVEN QUBITS CSS ENCODING

In order to derive the generating interaction of $|\psi\rangle_{\mathrm{CSS}}$ from Eq. (4) we first note that the x-Pauli matrix,$\sigma_x = \binom{01}{10}$, is a spin flip operator e. g. $\sigma_x|0\rangle = |1\rangle$ and $\sigma_x|1\rangle = |0\rangle$. Therefore, the seven qubits encoding $|\psi\rangle_{\mathrm{CSS}}$ can be generated from the maximally entangled Bell-like state $(|0000000\rangle + |1111111\rangle)/\sqrt{2}$ through the quadrupolar interaction

$$\mathrm{H_{int}} = \frac{1}{\sqrt{8}}\big(1 + \sigma_x^{(0)}\sigma_x^{(2)}\sigma_x^{(4)}\sigma_x^{(6)} + \sigma_x^{(1)}\sigma_x^{(2)}\sigma_x^{(5)}\sigma_x^{(6)} + \sigma_x^{(3)}\sigma_x^{(4)}\sigma_x^{(5)}\sigma_x^{(6)} + \sigma_x^{(1)}\sigma_x^{(2)}\sigma_x^{(3)}\sigma_x^{(4)} + \sigma_x^{(0)}\sigma_x^{(2)}\sigma_x^{(3)}\sigma_x^{(5)} + \sigma_x^{(0)}\sigma_x^{(1)}\sigma_x^{(4)}\sigma_x^{(5)} + \sigma_x^{(0)}\sigma_x^{(1)}\sigma_x^{(3)}\sigma_x^{(6)}\big). \quad \mathbf{(5)}$$

In other words, Eq. (4) can be rewritten as

$$|\psi\rangle_{\mathrm{CSS}} = \mathrm{H_{int}}(|0000000\rangle + |1111111\rangle)/\sqrt{2}. \quad (6)$$

Clearly the CSS's seven qubits encoding given by the above equation is not universal. This can be easily seen by observing that the generating operator $\mathrm{H_{int}}$ is not unitary. In fact,

$$\mathrm{H_{int}H_{int}^{\dagger}} = \mathrm{H_{int}^2} = \sqrt{8}\mathrm{H_{int}} \neq \mathrm{I}, \quad (7)$$

where $\mathrm{H_{int}^{\dagger}}$ is the hermitian operator given by Eq. (5). Furthermore,

$$\mathrm{H_{int}^n} = 8^{\frac{n-1}{2}}\mathrm{H_{int}}. \quad (8)$$

Eqs. (7) and (8) reflect the fact that the syndrome corresponding to the CSS quantum correction codes is not reversible. This means that to encoding one logic qubit into seven physical qubits makes that these protectors qubits dissipate energy in form of heat. This energy, introduces noise that spoils the desired coherence of the quantum computer. Likewise, the non-unitarity of $\mathrm{H_{int}}$ is equivalent to say that to apply recurrently the Steane seven qubits encoding to the CSS state leads to an unphysical state that it is not normalizable.

$$H_{int}^n|\psi\rangle_{CSS} = 8^{n/2}|\psi\rangle_{CSS.} \quad (9)$$

From Eqs. (7) and (9) one can see that the time evolution operator $e^{iH_{int}t}$ is not unitary and it leads the state $|\psi\rangle_{CSS}$ to an unrenormalized final state. On the other hand, as it is well known any unitary operator specifies a valid quantum gate [17] (see the Glossary). Amazingly, the unitary constraint is the only one which the quantum gates are subjected. Consequently, the Steane seven qubits encoding of Eq. (6) rely on a non-valid quantum gate. This restricts severely the direction of the flow of logic information (the transmission of the data) for the CSS syndrome. Indeed, within the mean field theory approximation the effective magnetic field acting on the spin $\sigma_x^{(2)}$ is $B^{(2)} = -\frac{\partial H^{int}}{\partial \sigma_x^{(2)}} = -\big(\sigma_x^{(0)}\sigma_x^{(4)}\sigma_x^{(6)} + \sigma_x^{(0)}\sigma_x^{(0)}\sigma_x^{(0)} + \sigma_x^{(0)}\sigma_x^{(0)}\sigma_x^{(0)} + \sigma_x^{(0)}\sigma_x^{(0)}\sigma_x^{(0)}\big)/\sqrt{8}$. Consequently, the effective Poynting vector (see the Glossary) associated to the qubit two should be $S^{(2)} = \frac{c\left(B^{(2)}\right)^2}{\mu_0} = \frac{\mu_0\left(1+\sigma_x^{(0)}\sigma_x^{(1)}\sigma_x^{(4)}\sigma_x^{(5)}+\sigma_x^{(0)}\sigma_x^{(1)}\sigma_x^{(3)}\sigma_x^{(6)}+\sigma_x^{(3)}\sigma_x^{(4)}\sigma_x^{(5)}\sigma_x^{(6)}\right)}{2c}$. One can see from the above expression that only the spin of the qubit two keeps invariant under rotations. The operator $S^{(2)}$flips the spin of the resting qubits. To chek that $S^{(2)}$ is not unitary, results a simple task. By this reason, this operation is not a valid quantum gate i.e. this does not represent any logical operation. This means that the propagation of the information carried by the qubit two, which is given by the Poynting vector $S^{(2)}$ , is dissipative and dispersive. Therefore, this operator introduces unwelcome decoherence into the system. A similar analysis follows for the other six protector qubits.

On the other hand, one must note that the CSS interaction as given by Eq. (5) is not invariant under rotation (permutations) of the qubits. This makes that the CSS encoding has a preferring direction of both propagation and correction of the errors.

## CONCLUSIONS

Due that the CSS quantum correction codes are based on two classical linear codes, they are not universal, as Eqs. (6) and (7) indicate. From Eq. (5) we conclude that the

CSS interaction is not invariant under permutation of the qubits which indicates a preferred direction of the propagation of the error. Another conclusion that we state is that in order to have ideal, non dissipative, and genuine quantum codes, the CSS codes must be extended to encoding invariant under rotations of the protector qubits independently of the number of them. The feasibility of this possibility relies on the Fault Tolerant Quantum Computing theories (reviewed in the book of Nielsen and Chuang) due that they provide a careful qualitative explanation of how quantum error correction is possible.

## APPENDIX

By construction, the $C_1/C_2$ Steane states are such that

$$|0\rangle_L = \frac{1}{\sqrt{|C_2|}}\sum_{\mathbf{y}\in C_2}(|0000000\rangle +_2 |\mathbf{y}\rangle), \quad \text{(A1)}$$

$$|1\rangle_L = \frac{1}{\sqrt{|C_2|}}\sum_{\mathbf{y}\in C_2}(|1111111\rangle +_2 |\mathbf{y}\rangle), \quad \text{(A2)}$$

where $|C_2| = 8$. In Eq. (A1) obviously, $|0000000\rangle$ must belong to $C_1$. On the other hand, in Eq. (A2) the vector $|1111111\rangle$ does not belong to $C_2$ but to $C_1$ because it is obtained by adding the last two rows of $\mathbf{G}^T$ of Eq. (2) plus all of the rows of this new matrix together, that is

$$1111111 = 0100101 +_2 1000011 +_2 0011001$$

Let us find now the eight 7-qubit vectors $|\mathbf{y}\rangle$ which are spanned by the rows of the matrix **H** of Eq. (3). One has that

$$\begin{aligned}
\mathbf{y}_0 &= 0000000 \\
\mathbf{y}_1 &= 0001111 \\
\mathbf{y}_2 &= 0110011 \\
\mathbf{y}_3 &= 1010101 \\
\mathbf{y}_4 &= 0111100 \\
&= 0001111 +_2 0110011 \\
\mathbf{y}_5 &= 1011010 \\
&= 0001111 +_2 1010101 \\
\mathbf{y}_6 &= 1100110 \\
&= 0110011 +_2 1010101 \\
\mathbf{y}_7 &= 1101001 \\
&= \mathbf{y}_4 +_2 1010101
\end{aligned} \quad \text{(A3)}$$

By substituting Eq. (A3) in Eqs. (A1) and (A2) the Steane seven qubit encoding of Eq. (4) follows.

## GLOSSARY

*Parity check matrix*: In coding theory a parity checking matrix $H_{m\times n}$ of a linear block code C is a generator matrix of a dual code. As such, a codeword $c^T = (c_1, c_2, c_2, \ldots, c_n)$ is in C if and only if the matrix vector product $\mathrm{H^T c}=0$ [18]. For example, the parity check matrix

$$H = \begin{bmatrix}0011\\1100\end{bmatrix},$$

specifies that for each codeword, digits 1 and 2 should sum to zero and digits 3 and 4 should sum to zero.

*Poynting vector*: In physics, the Poynting vector $\vec{S}$ can be thought of as representing the energy flux (in $W/m^2$) of an electromagnetic field [19]. This is defined as $\vec{S} = \vec{E} \times \vec{B}$ where $\vec{E}$ is the electric field and $\vec{B}$ is the auxiliary magnetic field [19].

*Quantum gate*: A quantum gate or quantum logic gate is a basic quantum circuit operating on a small number of qubits. They are the analogues for quantum computers to classical logic gates for conventional digital computers. Quantum logic gates are reversible, unlike many classical logic gates. Quantum logic gates are represented by unitary matrices. See Reference [20] for further details.

## ACKNOWLEDGMENT

We thank Laura Alejandra Peñaloza for the capture of the manuscript in Word format.

## REFERENCES

[1] S. L. Braunstein and H. K. Lo, eds. Special Focus Issue on Experimental Proposals for Quantum Computation: Forward, Fortschr. Phys., Vol. 48, 2000, pp. 76-81.

[2] A. Steane, " Multiple-Particle Interference and Quantum Error Correction", Proc. R. Soc. London, Ser. A, Vol. 452, No. 1954, 1996, pp. 2551-2577.

[3] P. Shor, “Scheme for reducing decoherence in a quantum computer memory”, Phys. Rev., Vol. A52, 1995, pp. 2493- 2496.

[4] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound”, Phys. Rev., Vol. A54, 1996, pp. 1862-1868.

[5] A. R. Calderbank, E.M. Rains, P. W. Shor, and A. J. Sloane, “Quantum error correction and orthogonal geometry”, Phys. Rev., Vol. A78, 1997, pp. 405-409.

[6] A. R. Calderbank, E.M. Rains, P. W. Shor, and A. J. Sloane, “Quantum error correction via codes over gf(4)”, IEEE Trans. Inf. Theory, Vol. 44, 1998, pp. 1369-1372.

[7] P. Shor, “Fault-tolerant quantum computation”, Proceedings of the 37th Symposium on the Foundations of Computer Sciences (FOCS), 1995, 37 Los Alamitos, CA: IEEE Press, pp. 56-57.

[8] A. Y. Kitaev, “Quantum Error Corrections with Imperfect Gates”. In *Quantum Communication and Computing and Measurement*. Edited by O. Hirota et al Plenum, New York.

[9] E. Knill, and R. Laflamme; “Concatenated Quantum Codes”, arxiv:quant-ph/9608012.

[10] D. Aharonov, and M. Ben-Or; “Fault-Tolerant Quantum Computation With Constant Error Rate”, arxiv:quantph/ 9906129.

[11] E. Knill, R. Laflamme, and W. H. Zurek, “Resilient Quantum Computation”, Science, Vol. 279, 1998, pp. 342-345.

[12] E. Knill, R. Laflamme, and W. H. Zurek, “Resilient quantum computation: error models and thresholds”, Proc. R. Soc. London Ser. A, Vol. 454, No. 1969, 1998, pp. 365-384.

[13] D. Gottesman, “Theory of fault-tolerant quantum computation”, Phys. Rev., Vol. A57, 1998, pp. 127-137.

[14] J. Preskill, “ Reliable quantum computers”, Proc. R. Soc. London, Ser. A, Vol. 454, No. 1969, 1998. pp. 385-410.

[15] A. Skander, M. Nadjim, and M. Benslama, “A New Error

Correction Intuitive Approach in Quantum Communications Protocols”, Am. J. Appl. Sci., Vol. 4, No. 8, 2007, pp. 597-604.

[16] A. Calderbank, and P. Shor, “Good quantum errorcorrecting codes exist”, Phys. Rev. Vol. A 54, 1996, pp. 1098-1105.

[17] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[18] H. A. Van Lint, *Introduction to coding theory*, (2nd Ed), Springer Verlag, (1992) pp. 34-35.

[19] J. Edminister, *Schaum’s outline of theory and problems of electromagnetism*, New York: McGraw-Hill Professional (1995) p. 225.

Received:Dec. 2008. Accepted: July 2009