

Quantum LDPC Codes Derived from Combinatorial Objects and *Latin* Squares

Salah A. Aly

salah at cs.tamu.edu

PhD Candidate
Department of Computer Science
Texas A&M University

November 11, 2007

Overview

Example
- Stabilizer

LDPC

Latin Square

LDPC& Latin

Quantum
LDPC

- Quantum computers (QC) can solve certain problems more efficiently.
Ex. Shor's factoring algorithm
- QC are useful for many applications.
cryptography, search, etc
- QC take advantage of quantum mechanical phenomena.
Ex. superposition and entanglement
- Quantum information gets affected by noise and environment.
- Quantum computers can not be build without quantum error corrections.

A quantum bit is the unit of quantum information.

- Two distinguishable states, $|0\rangle$ and $|1\rangle$, forms an orthonormal basis of C^2 . Ex. $0 \rightarrow |0\rangle$ and $1 \rightarrow |1\rangle$.
- New quality: Any linear combination $|\psi\rangle = a|0\rangle + b|1\rangle$ with probability $|a|^2 + |b|^2 = 1$ is a possible state of a quantum bit.

- Measurement of $a|0\rangle + b|1\rangle$ in the computational basis yields
 $|0\rangle$ with probability $|a|^2$
 $|1\rangle$ with probability $|b|^2$

Measurements destroy a superposition.

- Different errors affect a single qubit, bit flip and phase flip errors.

Bit flip: $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$

Phase flip: $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow -|1\rangle$

Introductory Example

- Let $\mathbf{F}_2 = \{0, 1\}$ be a binary field. A possible repetition code is

$$|0\rangle \longrightarrow |00000\rangle, \quad |1\rangle \longrightarrow |11111\rangle$$

- A logical qubit in the state $|\phi\rangle = a|0\rangle + b|1\rangle$ is mapped to

$$|\psi\rangle = a|00000\rangle + b|11111\rangle$$

- Suppose that a bit flip affects one of the qubits,

$$|\psi'\rangle = a|00010\rangle + b|11101\rangle$$

How to correct it? majority logic.

- Suppose that a phase flip affects this bit, then we get $a|00000\rangle - b|11111\rangle$

We cannot correct this error, it is the encoding of the state $a|0\rangle - b|1\rangle$.

- What if there are many errors?

We need good strategies for error corrections that correct many errors.

Definition: A Classical Code

An $[n, k, d]_q$ classical code is a subspace of dimension k :

- Encodes k bits in n bits
- Generator matrix G , parity check matrix H , $GH^T = 0$
- q levels (or q -ary alphabet), for binary $q = 2$
- Min. dist. between codewords d , corrects upto $t = \lfloor (d - 1)/2 \rfloor$ errors

Example over $F_2 = \{0, 1\}$, an $[6, 3, 3]_2$ code

$C = \{(1, 1, 0, 1, 0, 0); (1, 0, 1, 0, 1, 0), (1, 1, 1, 0, 0, 1), \dots\}$ all linear combinations,
 $d = \min\{wt(c) : c \in C\} = 3$ and $t = \lfloor (3 - 1)/2 \rfloor = 1$ error correcting.

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

Notations: A quantum code Q has parameters $[[n, k, d]]_q$.

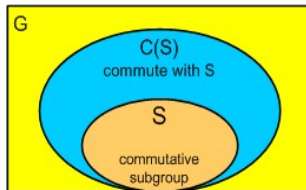
Definition

An $[[n, k, d]]_q$ quantum code Q is a q^k dimensional subspace of the complex space \mathbb{C}^{q^n} that can correct up to $\text{floor}((d-1)/2)$ errors

A stabilizer code Q is the joint eigenspace of a commutative subgroup S of an error group G , that is,

$$E|v\rangle = |v\rangle, \text{ for all } E \in S, |v\rangle \in Q$$

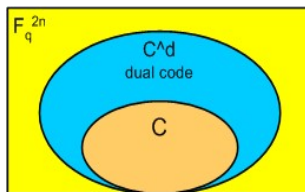
Stabilizer codes are popular since they compactly described by a group S .



$$\text{If } E, F \in S \text{ then } EF = FE$$

Quantum Stabilizer Codes

- The stabilizer S can be mapped to a classical self-orthogonal code C .
- The classical code C and its dual C^\perp allows one to characterize dimension and the errors detectable by the corresponding stabilizer code.
- The CSS construction is one example of a technique to construct stabilizer codes from classical codes.



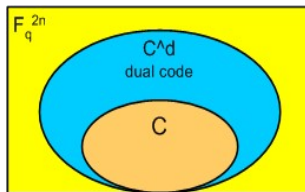
$$C^\perp = \{u \in F_q^n : (u, v) = \sum_i u_i v_i = 0\} \text{ for all } v \in C$$

Quantum Stabilizer Codes

Constructing stabilizer code Q reduces to constructing Euclidean self-orthogonal classical code C over \mathbb{F}_q^n .

Lemma: CSS construction

If C is an $[[n, k, d]]_q$ classical linear code such that $C \leq C^\perp$, self-orthogonal, then there exists a $[[n, 2k - n, d]]_q$ stabilizer code.



$$C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = \sum_i u_i v_i = 0\} \text{ for all } v \in C$$

- LDPC Overview.
- In this talk, the parity check matrices of these codes are constructed by permuting orthogonal *Latin* squares of order n in block-rows and block-columns.
- I show that the constructed LDPC codes are self-orthogonal and their minimum and stopping distances are bounded.
- This helps us to construct a family of quantum LDPC block codes.

Definition (Regular LDPC codes)

We can define a regular LDPC code over \mathbb{F}_2 , as the null-space of the matrix \mathbf{H} of sparse circulants of equal size. The matrix \mathbf{H} , with parameters (ρ, λ) , has the following properties.

- i) ρ is the weight of a column c_i ,
- ii) λ is the weight of a row r_i ,
- iii) each two rows (two columns) intersect at most in one nonzero position. This is called the row column constraint (RC), and it guarantees that cycles of length 4 are lacking.

Definition

A (ρ, λ, n) -LDPC code is a dual-containing code if it has a parity check matrix H over \mathbb{F}_2 such that:

- i) Every row has fixed weight λ and every column has fixed weight ρ .
- ii) Every pair of rows in H has an even overlap, and every row has even weight, meaning every pair of rows is *multiplicity even*.

A *Latin square* of order n is a square matrix of size $n \times n$ defined over \mathbf{F}_q^* or (i.e., \mathbf{Z}_q) such that each element $\alpha^i \in F_q^*$ appears only once in every row and column.

We can also study properties of some classes of *Latin squares*.

Definition

Let L and L' be two *Latin squares* of order n

- i) L is orthogonal to L' if the cell (i, j) in L is different from the cell (i, j) in L' for all $2 \leq i \leq n$ and $1 \leq j \leq n$.
- ii) There are at most $n - 1$ *mutually orthogonal Latin squares* of order n . Therefore, the set L_1, L_2, \dots, L_{n-1} is *mutually orthogonal* if L_i and L_j are orthogonal for $1 \leq i < j \leq n - 1$.

As an example, two orthogonal *Latin* squares of order $n = 4$ are given by

$$L_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, L_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}. \quad (1)$$

One way to obtain all orthogonal *Latin* squares is by fixing the first row and permute all other rows by one to obtain a new square matrix. Therefore, we have $n - 1$ permuted orthogonal *Latin* squares.

Latin Square

Let α^i be a nonzero primitive element in \mathbf{F}_q , for q prime power and $n=q-1$. Let $n = q - 1$, the vector operator $\mathbf{z} : \mathbf{F}_q^* \rightarrow \mathbf{F}_2^n$ as a zero vector of length n except at position i . Hence,

$$\mathbf{z}(\alpha^i) = (z_1, z_2, \dots, z_n) \quad (2)$$

for $z_i = 1$ and all $z_j = 0$ where $i \neq j$. For example, $\mathbf{z}(\alpha^2) = (0, 1, 0, \dots, 0)$. Define a circulant matrix A based on the vector $\mathbf{z}(\alpha^i)$ as follows.

Definition

Let A be an $n \times n$ matrix with elements from \mathbf{F}_2 .

$$A(\mathbf{z}(\alpha^i)) = \begin{pmatrix} \mathbf{z}(\alpha^i) \\ \mathbf{z}(\alpha^{i+1}) \\ \vdots \\ \mathbf{z}(\alpha^{i+n-1}) \end{pmatrix} \quad (3)$$

We can form the matrix G of size $n \times n$ as a result of the multiplicative group $\mathbf{Z}/q\mathbf{Z}$

$$\begin{aligned} G &= \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{pmatrix} = (h_1 \quad h_2 \quad \dots \quad h_n) \\ &= \begin{pmatrix} \alpha^1 & \alpha^2 & \alpha^3 & \dots & \alpha^n \\ \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \\ \alpha^n & \alpha^{n-1} & \alpha^{n-2} & \dots & \alpha^1 \end{pmatrix}, \end{aligned} \tag{4}$$

where g_i is the i th row in G and h_j is the j th column in G . The matrix G has the following structure:

- i) any two distinct rows differ in all positions.
 - ii) any two distinct columns differ in any positions.
 - iii) all elements of the field are presented in a row (column).
- This matrix G is equivalent to the *Latin* square of order n .

This matrix G is equivalent to the *Latin* square of order n . The $n - 1$ orthogonal *Latin* squares of order n , we call them B_1, B_2, \dots, B_{n-1} where $G = B_1$.

We form the matrix B by permuting rows of the matrix G in a certain order. So, the matrix B_j is a permutation of the matrix B_i under row permutation.

$$B = (B_1 \quad B_2 \quad \dots \quad B_{n-1}). \quad (5)$$

We have formed an $n \times (n - 1)n$ matrix B where every row in G is extended horizontally $(n - 1)$ times.

Corollary

Any two rows in the matrix B differ in all positions. I.e., B is a self-orthogonal matrix.

We can also extend every matrix B_j in B vertically to form the matrix

$$\begin{aligned}
 H_j &= \begin{pmatrix} B_j \\ B_{j+1} \\ \dots \\ B_{j+\rho-1} \end{pmatrix} \\
 &= \begin{pmatrix} h_{1,j} & h_{2,j} & \dots & \dots & h_{n,j} \\ h_{1,j+1} & h_{2,j+1} & \dots & \dots & h_{n,j+1} \\ h_{1,j+2} & h_{2,j+2} & \dots & \dots & h_{n,j+2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{1,(j+\rho-1)} & h_{2,(j+\rho-1)} & \dots & \dots & h_{n,(j+\rho-1)} \end{pmatrix},
 \end{aligned} \tag{6}$$

where the element $h_{i,j+\ell}$ is a column of n elements. Now the matrix H_j has size $(\rho)n \times n$.

Therefore we formed a $(\rho)n \times (n-1)n$ matrix H .

$$H = \left(H_1 \ H_2 \ H_3 \ \dots \ H_{(n-1)} \right). \quad (7)$$

The matrix H_j has the following properties:

- i) Every n components of every column are distinct and they form all the n nonzero elements of \mathbf{F}_q^* .
- ii) any two columns differ in every position.
- iii) Any two rows have even number of elements in common.

Lemma

For $1 \leq i, j \leq \rho n$, $i \neq j$, any two rows g_i and g_j in H have no common symbol from \mathbf{F}_q or they have an even number of symbols in common.

We now can replace every entry in H by its location vector to obtain a $(\rho)n \times (n-1)n^2$ matrix

$$\mathcal{G}_j = [A_{j,1} \quad A_{j,2} \quad \dots \quad A_{j,n-1}], \quad (8)$$

We construct the $\rho \times (n-1)n$ matrix \mathbf{H} of $n \times n$ submatrices over \mathbf{F}_2 .

$$\mathbf{H} = \begin{pmatrix} \mathcal{G}_1 \\ \mathcal{G}_2 \\ \dots \\ \mathcal{G}_\rho \end{pmatrix} = \begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,n-1} \\ A_{2,1} & A_{2,2} & \dots & A_{2,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ A_{\rho,1} & A_{\rho,2} & \dots & A_{\rho,n-1} \end{pmatrix}$$

and the matrices $A'_{i,j}$ s are $n \times n^2$ circulant permutation matrices of *Latin* squares.

By this construction we built an $\rho n \times (n-1)n^2$ matrix \mathbf{H} over \mathbf{F}_2 , where we replace α^i by 1 at position i in the vector $\mathbf{z}(\alpha^i)$.

Let ρ and λ be two integers such that $1 \leq \rho < \lambda < n$.

Theorem

For a prime integer q , the regular LDPC code generated by the parity check matrix \mathbf{H} is dual-containing and it has rate $\frac{\lambda - \rho}{\lambda}$, where $\lambda = (n - 1)n$

Example

Let $q = 5 = n + 1$ and $\alpha \in \mathbf{F}_q^*$. Let $\lambda = (n - 1)n$ and $\rho = 2$, the generator matrix is given by

$$G = \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix} = (h_1 \quad h_2 \quad h_3 \quad h_4) = \begin{pmatrix} \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 \\ \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \end{pmatrix}$$

The matrices B , H and \mathbf{H} are computed, and the matrix $\mathbf{H}(2, 12)$ is self-orthogonal.

The matrix B is given by

$$B = (B_1 \quad B_2 \quad B_3), \quad (9)$$

where $B_1 = G$ and

$$B_2 = \begin{pmatrix} \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 \\ \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \\ \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 \end{pmatrix}, B_3 = \begin{pmatrix} \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \\ \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 \end{pmatrix}.$$

Latin Square

$$H = \left(\begin{array}{cccc|cccc|cccc} \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 \\ \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \\ \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 \\ \hline \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^3 & \alpha^1 & \alpha^4 & \alpha^2 \\ \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^1 & \alpha^3 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \end{array} \right) \quad (10)$$

$$H = \left(\begin{array}{cccc|cccc|cccc|c} 1000 & 0100 & 0010 & 0001 & 0100 & 0001 & 1000 & 0010 & 0010 & 1000 & 0001 & 0100 \\ 0100 & 0001 & 1000 & 0010 & 0010 & 1000 & 0001 & 0100 & 0001 & 0010 & 0100 & 1000 \\ 0010 & 1000 & 0001 & 0100 & 0001 & 0010 & 0100 & 1000 & 1000 & 0100 & 0010 & 0001 \\ 0001 & 0010 & 0100 & 1000 & 1000 & 0100 & 0010 & 0001 & 0100 & 0001 & 1000 & 0010 \\ \hline 0100 & 0001 & 1000 & 0010 & 0010 & 1000 & 0001 & 0100 & 1000 & 0100 & 0010 & 0001 \\ 0010 & 1000 & 0001 & 0100 & 0001 & 0010 & 0100 & 1000 & 0100 & 0001 & 1000 & 0010 \\ 0001 & 0010 & 0100 & 1000 & 1000 & 0100 & 0010 & 0001 & 0010 & 1000 & 0001 & 0100 \\ 1000 & 0100 & 0010 & 0001 & 0100 & 0001 & 1000 & 0010 & 0001 & 0010 & 0100 & 1000 \end{array} \right)$$

CSS Construction: A well-known construction of quantum codes from two classical nested codes is called CSS (i.e Calderbank, Shor and Steane). The CSS construction assumes that the stabilizer subgroup (matrix) can be written as

$$S = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{G} \end{array} \right) \quad (12)$$

where \mathbf{H} and \mathbf{G} are $k \times n$ matrixes satisfying $\mathbf{HG}^T = \mathbf{0}$. The quantum code with stabilizer S is able to encode $n - 2k$ logical qubits into n physical qubits. If $\mathbf{G} = \mathbf{H}$, then the stabilizer has the form

$$S = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{H} \end{array} \right) \quad (13)$$

and the self-orthogonality or dual-containing condition becomes $\mathbf{HH}^T = \mathbf{0}$. If C is a code that has a parity check matrix \mathbf{H} , then $C^\perp \subset C$, where C^\perp is the dual code.

proposition

A quantum LDPC code Q with rate $(n - 2k)/n$ is a code whose stabilizer matrix S_{stab} of size $2k \times 2n$ has a parity check matrix \mathbf{H} with pair (ρ, λ) where ρ is the number of non-zero error operators in a column and λ is the number of non-zero error operators in a row.

We now give a family of quantum LDPC codes constructed from self-orthogonal LDPC codes that is based on elements of *Latin* squares.

Lemma

Let n be the order of a Latin square where $q = n + 1$ for some prime q . Let $\mathbf{H}(\rho, \lambda)$ be a parity check matrix of a LDPC code over \mathbb{F}_2 with column weight ρ and row weight λ . Then, there exists a quantum LDPC code with parameters $[[\lambda n, \lambda n - 2n\rho, \geq \rho]]_2$.

Any Smart Idea to derive Self-orthogonal LDPC

- Finite and Projective Geometry Codes.
- Other Combinatorial Objects: graphs.

Math Dept.,
TAMU,
11/04/2007

Overview

Example
- Stabilizer

LDPC

Latin Square

LDPC& Latin

Quantum
LDPC

Overview

Example
- Stabilizer

LDPC

Latin Square

LDPC& Latin

**Quantum
LDPC**

Thank You

Math Dept.,
TAMU,
11/04/2007

Questions !!!

Thank you

Overview

Example
- Stabilizer

LDPC

Latin Square

LDPC& Latin

Quantum
LDPC

Overview

Example
- Stabilizer

LDPC

Latin Square

LDPC& Latin

**Quantum
LDPC**

Overview

Example
- Stabilizer

LDPC

Latin Square

LDPC& Latin

**Quantum
LDPC**