Title: Two Approaches to Sparse Graph Quantum Codes

Date: May 02, 2008 11:30 AM

URL: http://pirsa.org/08050026

Abstract: Constructing good quantum LDPC codes remains an important problem in quantum coding theory. We contribute to the ongoing discussion on this topic by proposing two approaches to constructing quantum LDPC codes. In the first, we rely on an algebraic method that uses a redundant description of the parity check matrix to overcome the problem of 4-cycles in the Tanner graph that degrade the performance of iterative decoding. In the second we use the fact that subsystem coding can simplify the decoding process. We show that if there exist classical LDPC codes with large error exponents, then we can construct degenerate subsystem LDPC codes with the stabilizer generators having low weight.

Two Approaches to Sparse Graph Quantum Codes

Pradeep Kiran Sarvepalli

Department of Computer Science
Texas A&M University

Joint work with Andreas Klappenecker and Martin Rötteler

Quantum Information and Graph Theory: Emerging Connections
Perimeter Institute for Theoretical Physics
May 2, 2008

Motivation

Protect (quantum) information using "efficient" codes.

We evaluate a code with respect to:

- Overall error rate
- Rate of the code
- Complexity of error correction

Motivation

Protect (quantum) information using "efficient" codes.

We evaluate a code with respect to:

- Overall error rate
- Rate of the code
- Complexity of error correction

Classical sparse graph codes i.e. low density parity check (LDPC) codes achieve

- Error rates arbitrarily close to zero
- Rates that approach arbitrarily close to capacity
- Linear complexity of decoding

Motivation

Protect (quantum) information using "efficient" codes.

We evaluate a code with respect to:

- Overall error rate
- Rate of the code
- Complexity of error correction

Classical sparse graph codes i.e. low density parity check (LDPC) codes achieve

- Error rates arbitrarily close to zero
- Rates that approach arbitrarily close to capacity
- Linear complexity of decoding

How can we build quantum codes with similar performance?

Preliminaries – Stabilizer Codes

A stabilizer code is a joint eigenspace of an abelian subgroup S of the Pauli group $\mathcal{P}_n$ on n qubits.

$$\mathcal{P}_n = \{i^c E_1 \otimes E_2 \otimes \cdots \otimes E_n\}; \quad E_i \in \{I, X, Y, Z\}.$$

The subgroup is called the stabilizer of the code.

An $[[n, k, d]]$ quantum code

- encodes k qubits into n qubits
- is a 2^k-dimensional subspace in $\mathbb{C}^{2^n}$
- is capable of detecting all errors on $d-1$ or fewer qubits.

A stabilizer code can be constructed from a classical code that contains its dual.

Preliminaries – Stabilizer Codes

We form the stabilizer code by taking a classical code $C \supseteq C^{\perp}$ and forming the stabilizer (matrix) as

$$S = \left[\begin{array}{c|c} H & 0 \\ 0 & H \end{array}\right], \quad HH^t = 0.$$

where H is the parity check matrix of C.

Quantum Codes from Bipartite Graphs

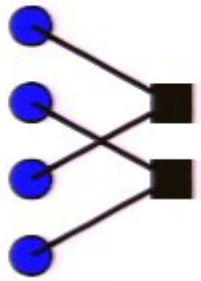
Classical codes are often associated to bipartite graphs (also called Tanner graphs).

In view of the CSS construction, we can also define the stabilizer (codes) by bipartite graphs.

Parity check matrix

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

Tanner graph



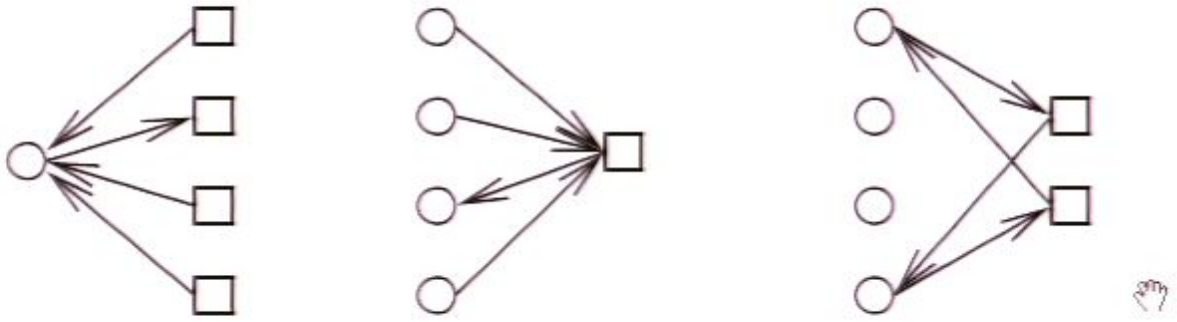
Stabilizer

$$\begin{bmatrix} X & & X & \\ & X & & X \\ Z & & Z & \\ & Z & & Z \end{bmatrix}$$

Message Passing Decoding on Graphs

The decoding problem: Estimate the error e, given the syndrome He^t.

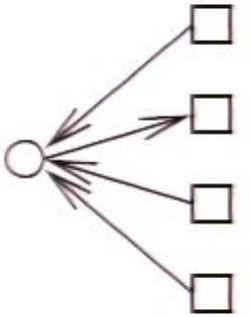
Messages are sent from qubits to syndrome nodes and vice versa in each iteration.



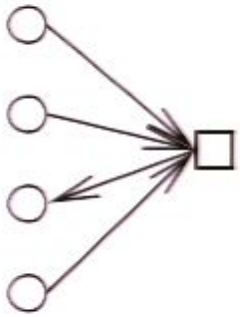
Left to right messages Right to left messages A 4−cycle

Assumption: Messages are independent $\Rightarrow$ Graph has large girth.

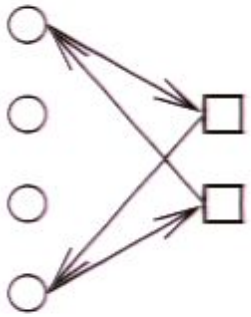
Message Passing Decoding on Graphs



Left to right messages

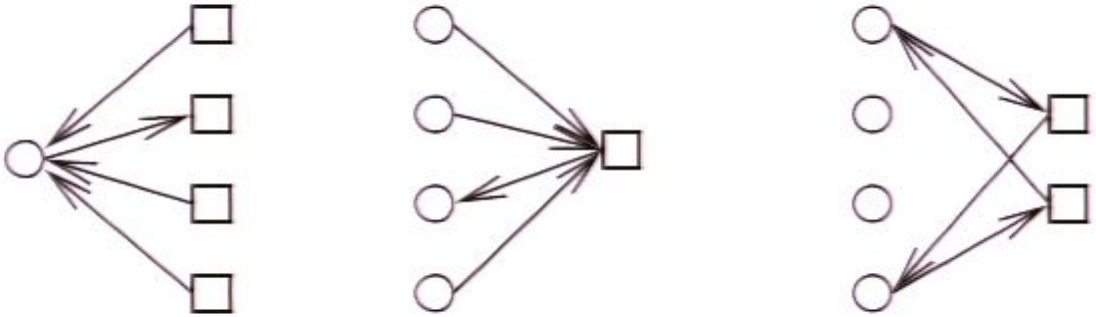


Right to left messages



A 4−cycle

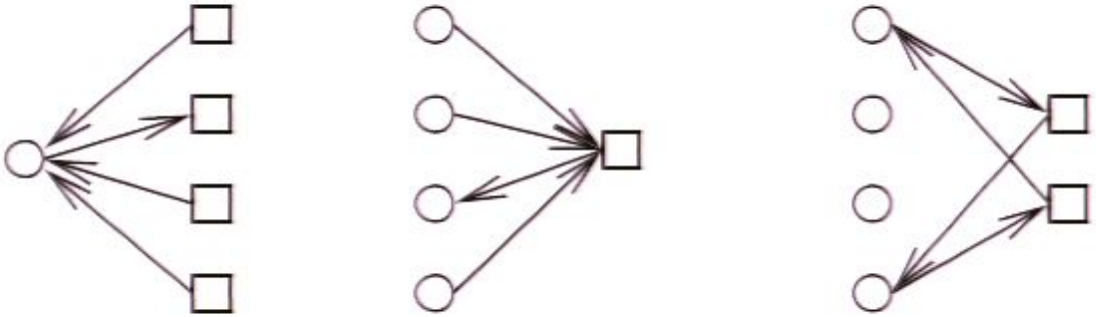
Message Passing Decoding on Graphs



Left to right messages Right to left messages A 4−cycle

If a stabilizer code is nontrivial, then the graph must have many 4-cycles.

Message Passing Decoding on Graphs



Left to right messages Right to left messages A 4−cycle

If a stabilizer code is nontrivial, then the graph must have many 4-cycles.

A possible solution: Redundant decoding on graphs.

Finite Geometries

We will construct LDPC codes from finite geometries. (Kou, Lin and Fossorier; Tang et al.)

A finite collection of n points and J lines obeying the following axioms

1) Every line has ρ points
2) Every point is on γ lines
3) Any two lines intersect only at one or no points
4) Any two points are connected by only one line

There are two geometries that satisfy these axioms.

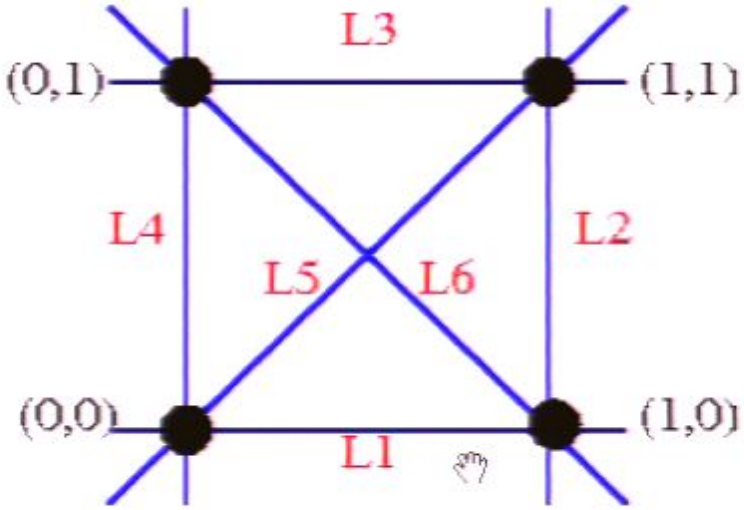
- Euclidean geometry $\mathrm{EG}(m, p^s)$ with points in $\mathbb{F}_{p^s}^m$
- Projective geometry $\mathrm{PG}(m, p^s)$ with points in $\mathbb{F}_{p^s}^{(m+1)}$

Incidence Graphs from Finite Geometries

Consider the points in $\mathbb{F}_2^2 \cong \mathbb{F}_4$ *i.e.*, $\{(0,0);(1,0);(0,1);(1,1)\}$

$\{0, 1, \alpha, \alpha^2\}$

$$\text{Lines} = \{(0,1);(0,\alpha);(0,\alpha^2);(1,\alpha);(1,\alpha^2);(\alpha,\alpha^2)\}$$



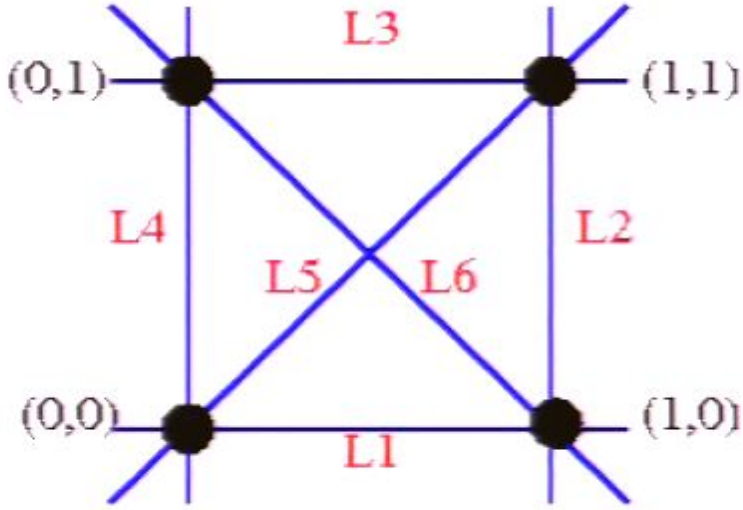
Incidence vector for L_1

Points	0	1	α	α^2
Line	1	1	0	0

More generally any $\mathbb{F}_{p^s}^m$ leads to a finite Euclidean geometry

Finite Geometry LDPC Codes

$$H_{\mathrm{EG}}^{(1)} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$



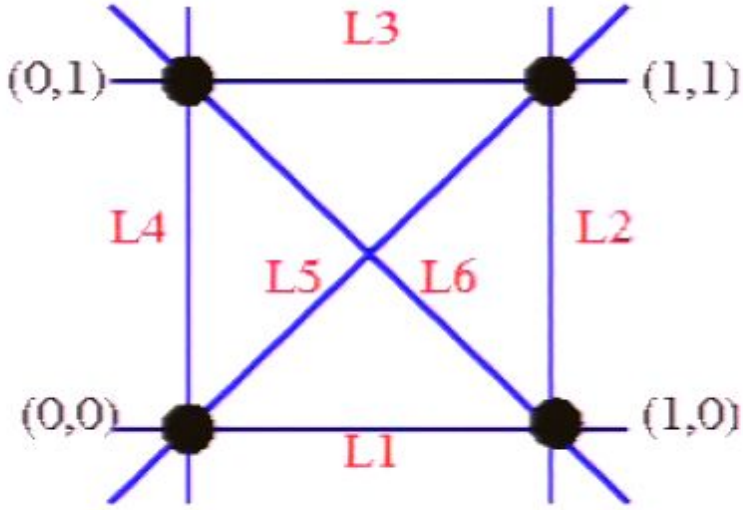
Gives the $[4.1.4]$ code

Note the redundancy in the parity checks

Extended Type-I $C_{\mathrm{EG}}^{(1)}(m.s.p)$ code is the null space of the incidence vectors of the lines in $\mathrm{EG}(m, p^s)$.

Finite Geometry LDPC Codes

$$H_{\mathrm{EG}}^{(1)} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$



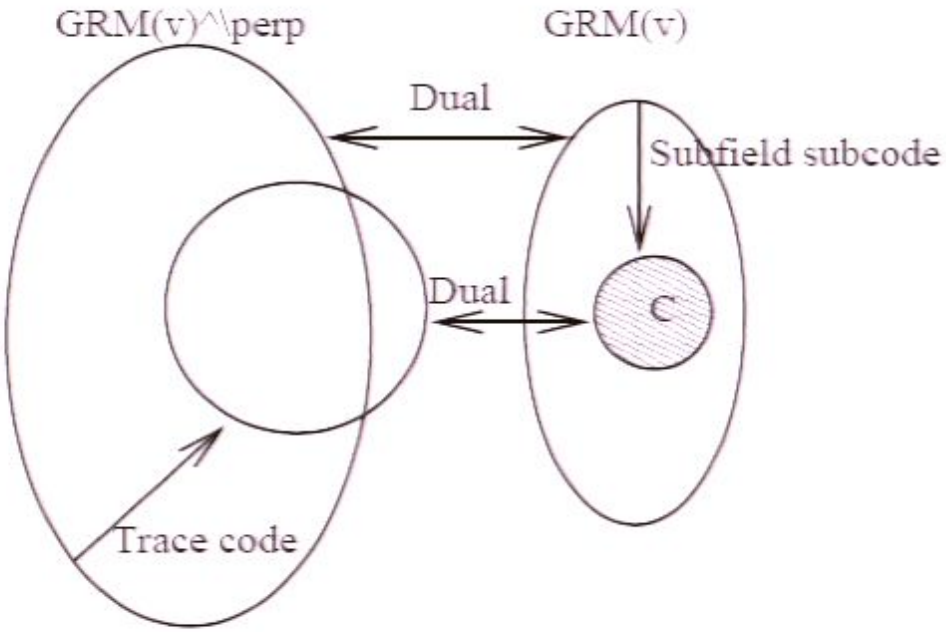
Gives the [4. 1. 4] code

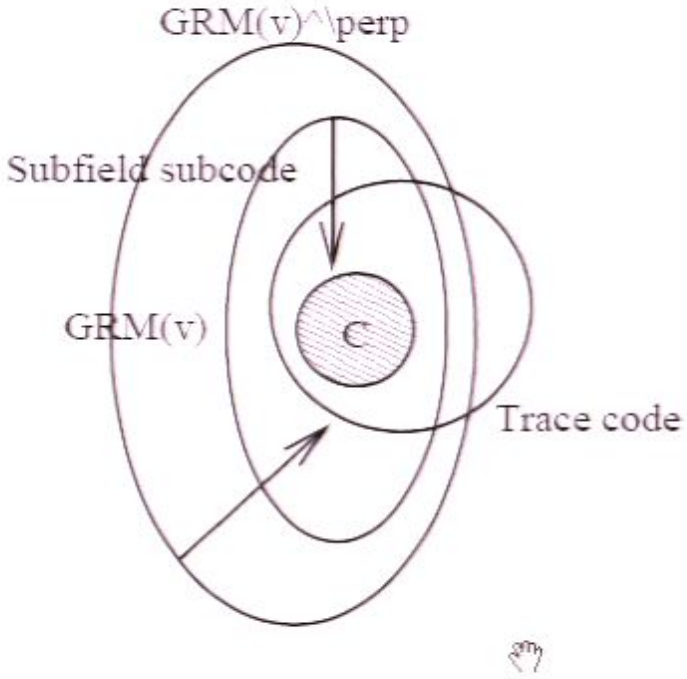
Note the redundancy in the parity checks

Extended Type-I $C_{\mathrm{EG}}^{(1)}(m, s, p)$ code is the null space of the incidence vectors of the lines in $\mathrm{EG}(m, p^s)$.

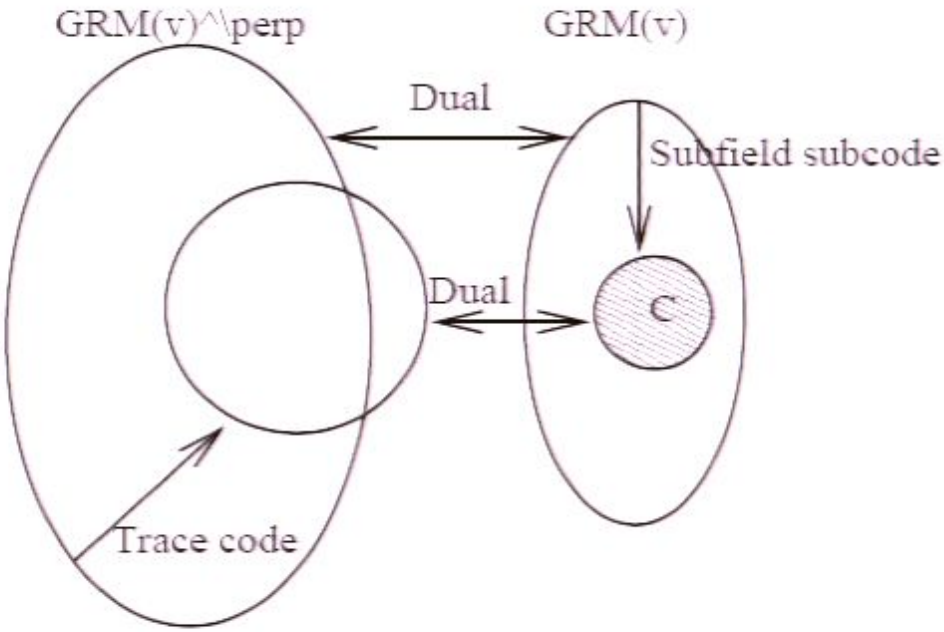
To construct stabilizer codes from finite geometries we need to look at more general incidence structures. (Tang et al.)

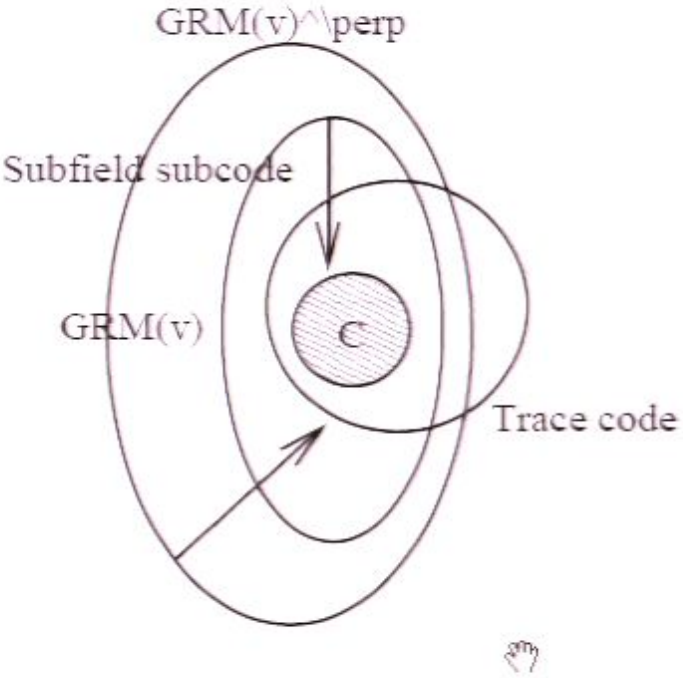
Finite Geometry Quantum LDPC Codes





Finite Geometry Quantum LDPC Codes





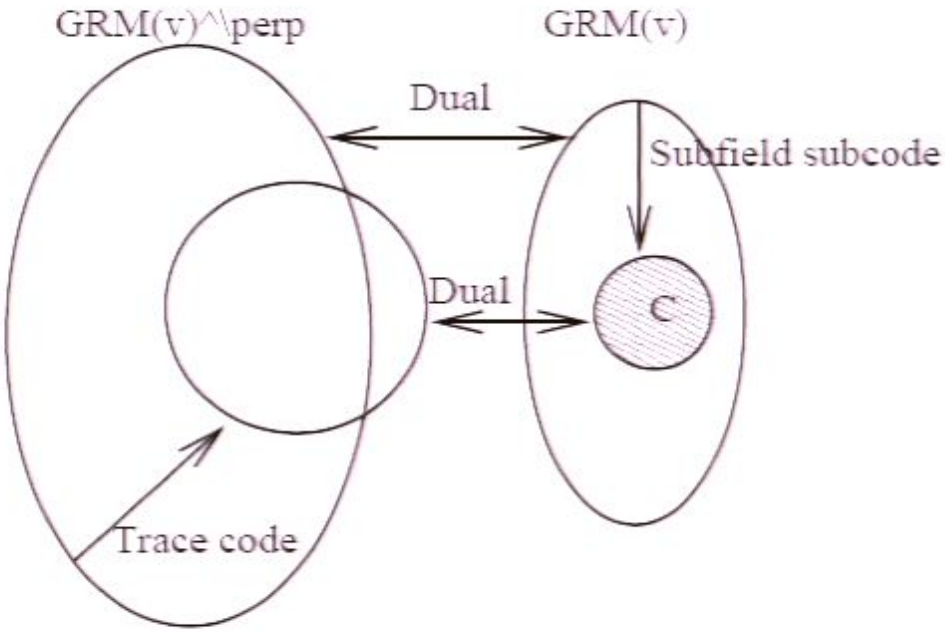
If $\lceil m/2 + (q-1)/2 \rceil \leq \mu \leq m$, then there exists an $[[2^{ms}, 2k - n, \geq d]]$ quantum LDPC code where $k = \dim C_{\mathrm{EG}}(m, \mu, s, 2)$ and $d = \mathrm{wt}(C_{\mathrm{EG}}(m, \mu, s, 2))$.

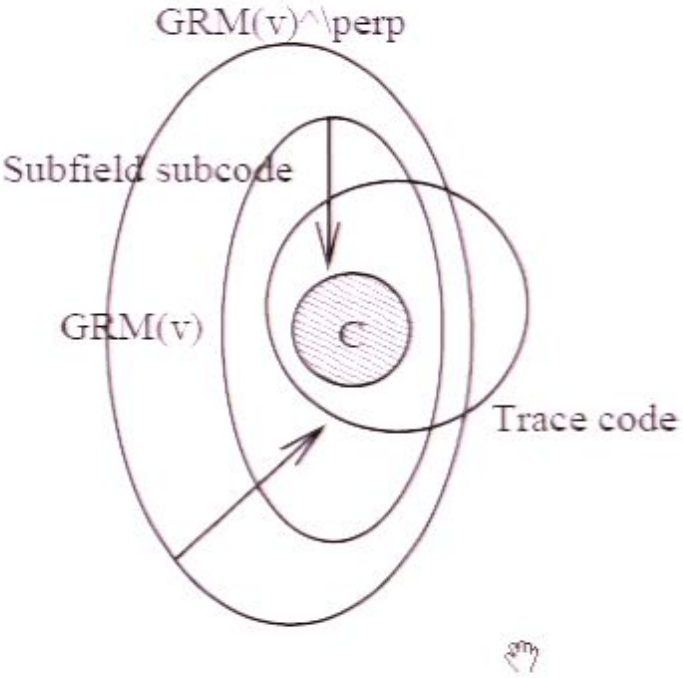
A $[[512, 384, \geq 10]]$ quantum LDPC code

Chose the Euclidean geometry over $\mathbb{F}_{2^3}^3$ and form the incidence structures from planes and points.

This geometry has 512 points and 584 planes. More importantly, it defines a $[512. 448. \geq 10]$ code $C \supseteq C^{\perp}$. We can construct a $[[512. 384. \geq 10]]$ quantum code.

Finite Geometry Quantum LDPC Codes





If $\lceil m/2 + (q-1)/2 \rceil \leq \mu \leq m$, then there exists an $[[2^{ms}, 2k - n, \geq d]]$ quantum LDPC code where $k = \dim C_{\mathrm{EG}}(m, \mu, s, 2)$ and $d = \mathrm{wt}(C_{\mathrm{EG}}(m, \mu, s, 2))$.

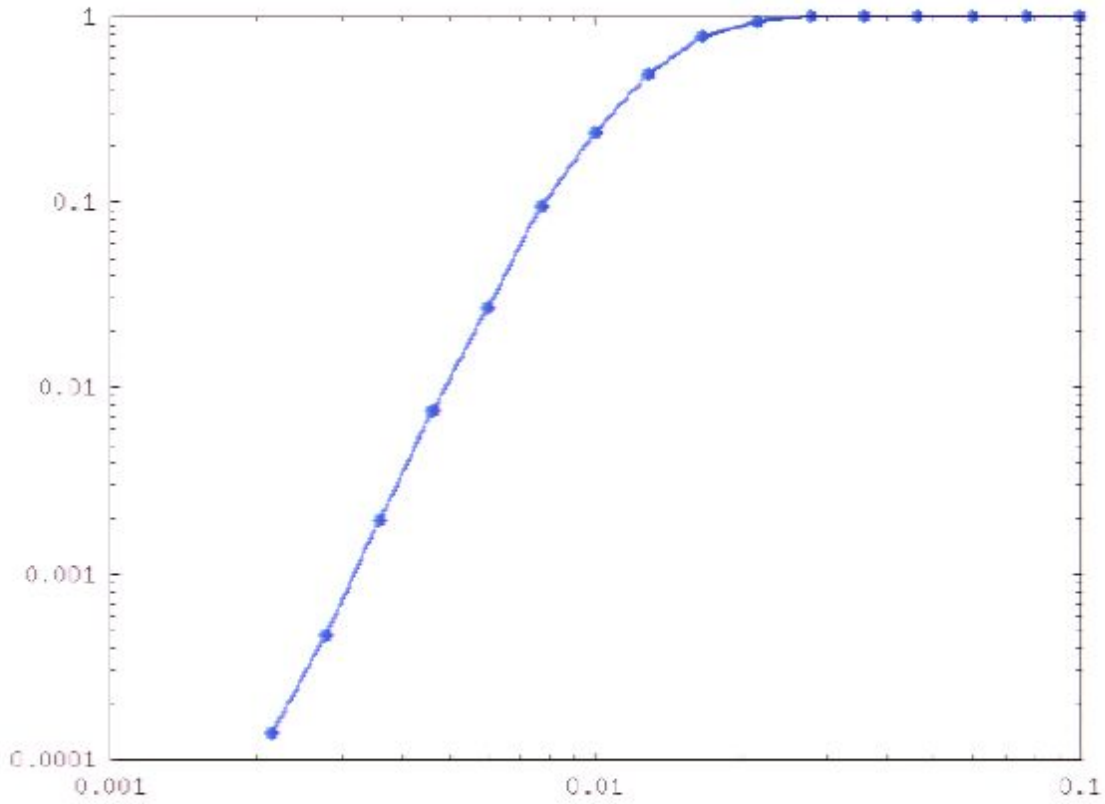
A $[[512, 384, \geq 10]]$ quantum LDPC code

Chose the Euclidean geometry over $\mathbb{F}_{2^3}^3$ and form the incidence structures from planes and points.

This geometry has 512 points and 584 planes. More importantly, it defines a $[512. 448. \geq 10]$ code $C \supseteq C^{\perp}$. We can construct a $[[512. 384. \geq 10]]$ quantum code.

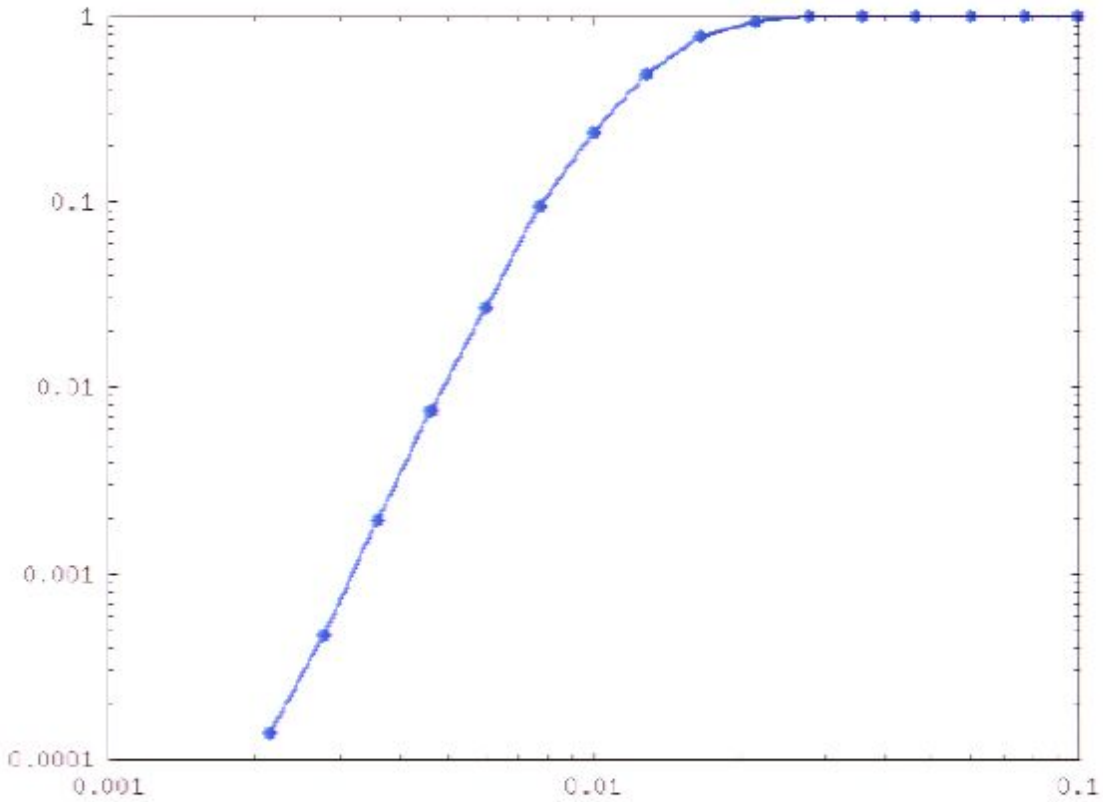
Performance of $[[512, 384, \geq 10]]$ quantum LDPC code

Block error rate vs Probability of error in channel



Performance of $[[512, 384, \geq 10]]$ quantum LDPC code

Block error rate vs Probability of error in channel



This code has > 3 million 4-cycles! and iterative decoding still works!!

The Summing Up

These codes typically give high rates.

The degree of the nodes depends on the length of the code and is of the order $p^{ms/2}$. The complexity of decoding is $O(n^{3/2})$.

4-cycles need not be catastrophic in the design of quantum LDPC codes.

Subsystem Codes

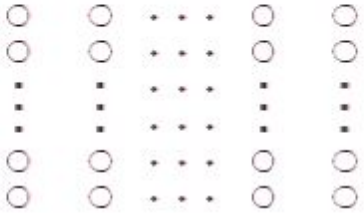
Subsystem codes promise to simplify error recovery schemes by providing additional degrees of freedom. The system Hilbert space is decomposed as $\mathcal{H} = A \otimes B \oplus C^{\perp}$, (Kribs *et al*).

If $\dim A = 2^k$; $\dim B = 2^r$ and A can detect all errors on $d-1$ or less qubits, then we say that it is an $[[n, k, r, d]]$ subsystem code.

The errors that act nontrivially on A form a subgroup called the gauge group G. The stabilizer acts trivially on $A \otimes B$.

Subsystem Codes – Construction

Using concatenation of two codes one to correct the phase errors and the other to correct the bit flip errors we can construct subsystem codes.

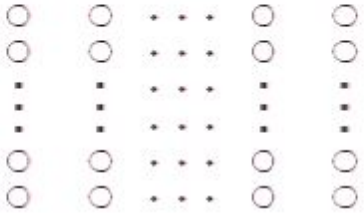


$$\mathcal{G} = \left[\begin{array}{c|c} I \otimes H & \\ & H \otimes I \end{array} \right]; S = \left[\begin{array}{c|c} G \otimes H & \\ & H \otimes G \end{array} \right].$$

(Bacon-Casaccino) Given an $[n, k, d]$ classical code there exists an $[[n^2, k^2, (n-k)^2, d]]$ subsystem code.

Subsystem Codes – Construction

Using concatenation of two codes one to correct the phase errors and the other to correct the bit flip errors we can construct subsystem codes.



$$\mathcal{G} = \left[\begin{array}{c|c} I \otimes H & \\ & H \otimes I \end{array} \right]; S = \left[\begin{array}{c|c} G \otimes H & \\ & H \otimes G \end{array} \right].$$

(Bacon-Casaccino) Given an $[n, k, d]$ classical code there exists an $[[n^2, k^2, (n-k)^2, d]]$ subsystem code.

These codes are asymptotically bad as $d/n^2 \to 0$. But ...

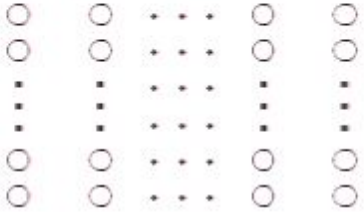
Steps to Subsystem LDPC Codes

If we shift our focus from distance, then we can get codes whose error rates go to zero asymptotically.

- Reducing error support using the gauge group
- Splitting the errors
- Syndrome measurement by parts
- Codes with nontrivial error exponents

Subsystem Codes – Construction

Using concatenation of two codes one to correct the phase errors and the other to correct the bit flip errors we can construct subsystem codes.



$$\mathcal{G} = \left[\begin{array}{c|c} I \otimes H & \\ & H \otimes I \end{array} \right]; S = \left[\begin{array}{c|c} G \otimes H & \\ & H \otimes G \end{array} \right].$$

(Bacon-Casaccino) Given an $[n, k, d]$ classical code there exists an $[[n^2, k^2, (n-k)^2, d]]$ subsystem code.

These codes are asymptotically bad as $d/n^2 \to 0$. But ...

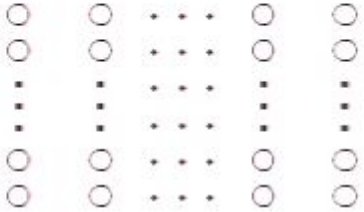
Steps to Subsystem LDPC Codes

If we shift our focus from distance, then we can get codes whose error rates go to zero asymptotically.

- Reducing error support using the gauge group
- Splitting the errors
- Syndrome measurement by parts
- Codes with nontrivial error exponents

Subsystem Codes – Construction

Using concatenation of two codes one to correct the phase errors and the other to correct the bit flip errors we can construct subsystem codes.



$$\mathcal{G} = \left[\begin{array}{c|c} I \otimes H & \\ & H \otimes I \end{array} \right]; S = \left[\begin{array}{c|c} G \otimes H & \\ & H \otimes G \end{array} \right].$$

(Bacon-Casaccino) Given an $[n, k, d]$ classical code there exists an $[[n^2, k^2, (n-k)^2, d]]$ subsystem code.

These codes are asymptotically bad as $d/n^2 \to 0$. But ...

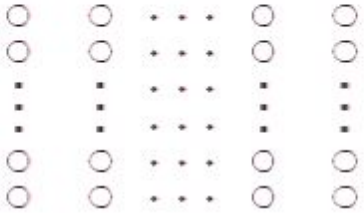
Steps to Subsystem LDPC Codes

If we shift our focus from distance, then we can get codes whose error rates go to zero asymptotically.

- Reducing error support using the gauge group
- Splitting the errors
- Syndrome measurement by parts
- Codes with nontrivial error exponents

Subsystem Codes – Construction

Using concatenation of two codes one to correct the phase errors and the other to correct the bit flip errors we can construct subsystem codes.



$$\mathcal{G} = \left[\begin{array}{c|c} I \otimes H & \\ & H \otimes I \end{array} \right]; S = \left[\begin{array}{c|c} G \otimes H & \\ & H \otimes G \end{array} \right].$$

(Bacon-Casaccino) Given an $[n, k, d]$ classical code there exists an $[[n^2, k^2, (n-k)^2, d]]$ subsystem code.

These codes are asymptotically bad as $d/n^2 \to 0$. But ...

Steps to Subsystem LDPC Codes

If we shift our focus from distance, then we can get codes whose error rates go to zero asymptotically.

- Reducing error support using the gauge group
- Splitting the errors
- Syndrome measurement by parts
- Codes with nontrivial error exponents

Reducing the Error Support Using the Gauge Group

Instead of n rows (columns), we need only look at k rows (columns).

$$I \otimes H = \begin{bmatrix} H & 0 & \dots & 0 & 0 \\ 0 & H & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & H & 0 \\ 0 & 0 & \dots & 0 & H \end{bmatrix}.$$

$$H = \begin{bmatrix} p_{1.1} & \dots & \dots & p_{1.k} & 1 & 0 & \dots & 0 \\ p_{2.1} & \dots & \dots & p_{2.k} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_{n-k.1} & \dots & \dots & p_{n-k.k} & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Use the ith row of H to move an error on the ith column onto the first k columns.

Splitting an Error into k Smaller Errors

$$H = [\ P \quad I_{n-k}\ ]; \quad G = [\ I_k \quad P^t\ ]; \quad P = (p_{i,j})_{(n-k)\times k}.$$

$$G \otimes H = \begin{bmatrix} H & 0 & \dots & 0 & p_{1,1}H & \dots & \dots & p_{1,n-k}H \\ 0 & H & \dots & \dots & p_{1,2}H & \dots & \dots & p_{2,n-k}H \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & H & p_{1,k}H & \dots & \dots & p_{k,n-k}H \end{bmatrix}.$$

An error in the first row can be decoded independently of other rows using the classical LDPC code!

Complexity of decoding is $O(kD)$, where D decoding complexity of the classical LDPC code. This is still $O(n^2)$, linear in the length of the code.

Syndrome Measurement by Parts

$$G \otimes H = \begin{bmatrix} H & 0 & \dots & 0 & p_{1,1}H & \dots & \dots & p_{1,n-k}H \\ 0 & H & \dots & \dots & p_{1,2}H & \dots & \dots & p_{2,n-k}H \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & H & p_{1,k}H & \dots & \dots & p_{k,n-k}H \end{bmatrix}.$$

$$I \otimes H = \begin{bmatrix} H & 0 & \dots & 0 & 0 \\ 0 & H & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & H & 0 \\ 0 & 0 & \dots & 0 & H \end{bmatrix}.$$

We can compute the syndrome corresponding to each stabilizer generator by measuring the gauge generators and combining them classically.

Syndrome Measurement by Parts – An Example

Aliferis and Cross first used this idea for the Bacon-Shor code. The stabilizer for the Bacon Shor code is

$$\left[\begin{array}{ccc|ccc|ccc} X & X & X & X & X & X & I & I & I \\ I & I & I & X & X & X & X & X & X \\ Z & Z & I & Z & Z & I & Z & Z & I \\ I & Z & Z & I & Z & Z & I & Z & Z \end{array}\right].$$

To measure $Z \otimes Z \otimes I \otimes Z \otimes Z \otimes I \otimes Z \otimes Z \otimes I$ we could measure Z_1Z_2, Z_4Z_5 and Z_7Z_8 separately and compute the syndrome corresponding to $Z \otimes Z \otimes I \otimes Z \otimes Z \otimes I \otimes Z \otimes Z \otimes I$.

Existence of Asymptotically Good Codes

Error rate: $P_{e.q} \leq 2kP_{e.c}(2p/3)$,

where p the probability of error on a depolarizing channel, and $P_{e.c}(2p/3)$ is the error rate of the classical code on a binary symmetric channel with crossover probability of $2p/3$.

If we have an asymptotically good classical code with nonzero error exponent, *i.e.*, $P_{e.c} \leq e^{-nE+o(n)}$ and $E > 0$, then the error rate of the subsystem LDPC code is $P_{e.q} \leq e^{-nE+o(n)+c\ln n}$. Asymptotically, the code is good.

Existence of Asymptotically Good Codes

Do such codes exist? We do not know the error exponents of LDPC codes, but expander codes (which can be viewed as LDPC codes) have positive error exponents. They can be used to construct a class of asymptotically good quantum expander codes.

In fact any code with a positive error exponent in this case will lead to quantum codes which are asymptotically good.

It would be interesting to find other classes of codes with positive error exponents

Summary

We proposed two methods to construct quantum LDPC codes

- The effects of 4-cycles can be offset by redundant parity checks.
- Gauge group can be exploited to get LDPC codes whose syndrome measurements are still of constant complexity.
- Shifting the focus from distance to error rate can still lead to codes that are asymptotically good.

The Summing Up

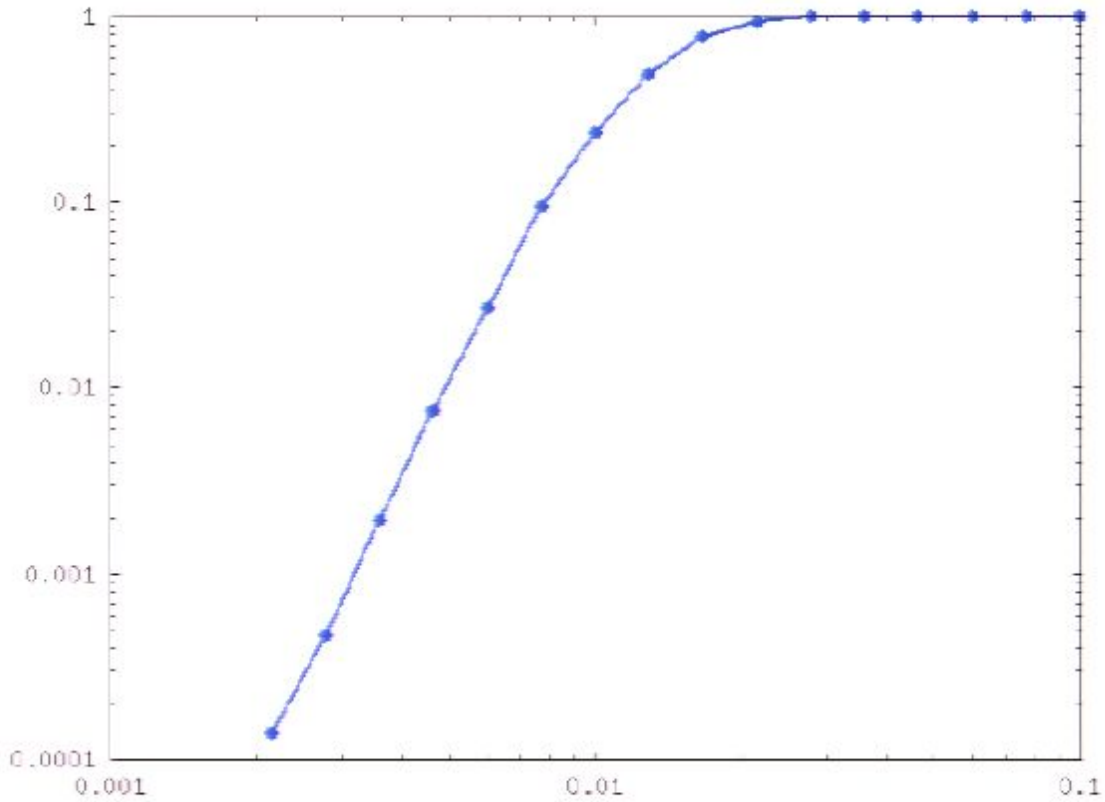
These codes typically give high rates.

The degree of the nodes depends on the length of the code and is of the order $p^{ms/2}$. The complexity of decoding is $O(n^{3/2})$.

4-cycles need not be catastrophic in the design of quantum LDPC codes.

Performance of $[[512, 384, \geq 10]]$ quantum LDPC code

Block error rate vs Probability of error in channel



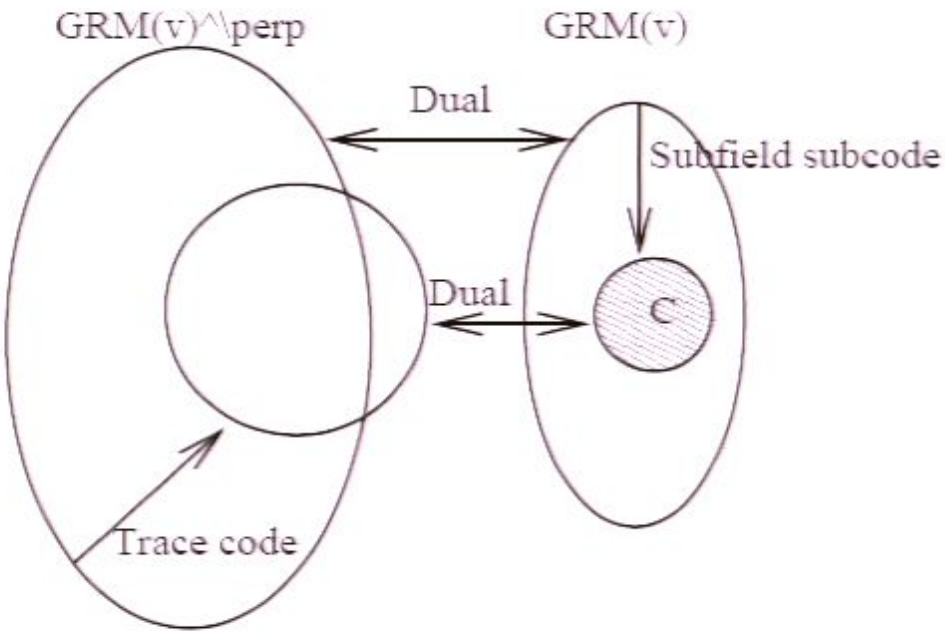
This code has > 3 million 4-cycles! and iterative decoding still works!!

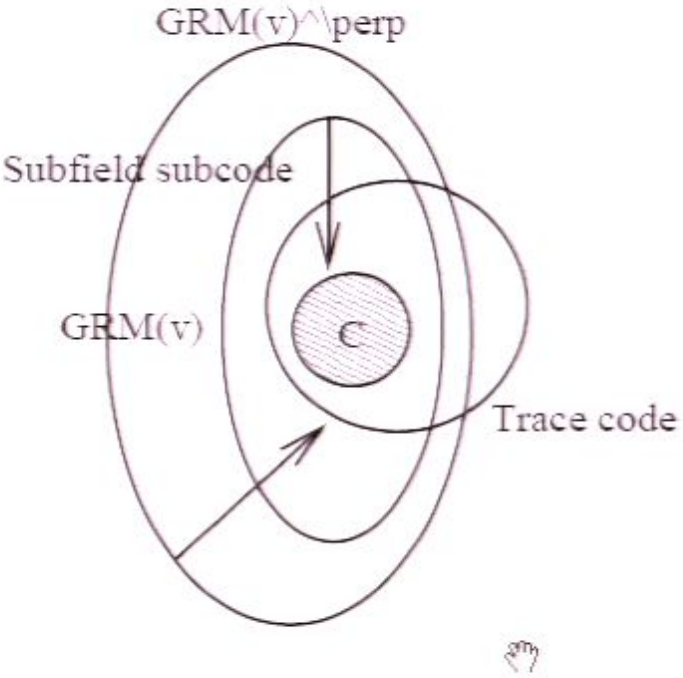
A $[[512, 384, \geq 10]]$ quantum LDPC code

Chose the Euclidean geometry over $\mathbb{F}_{2^3}^3$ and form the incidence structures from planes and points.

This geometry has 512 points and 584 planes. More importantly, it defines a $[512.448, \geq 10]$ code $C \supseteq C^{\perp}$. We can construct a $[[512.384, \geq 10]]$ quantum code.

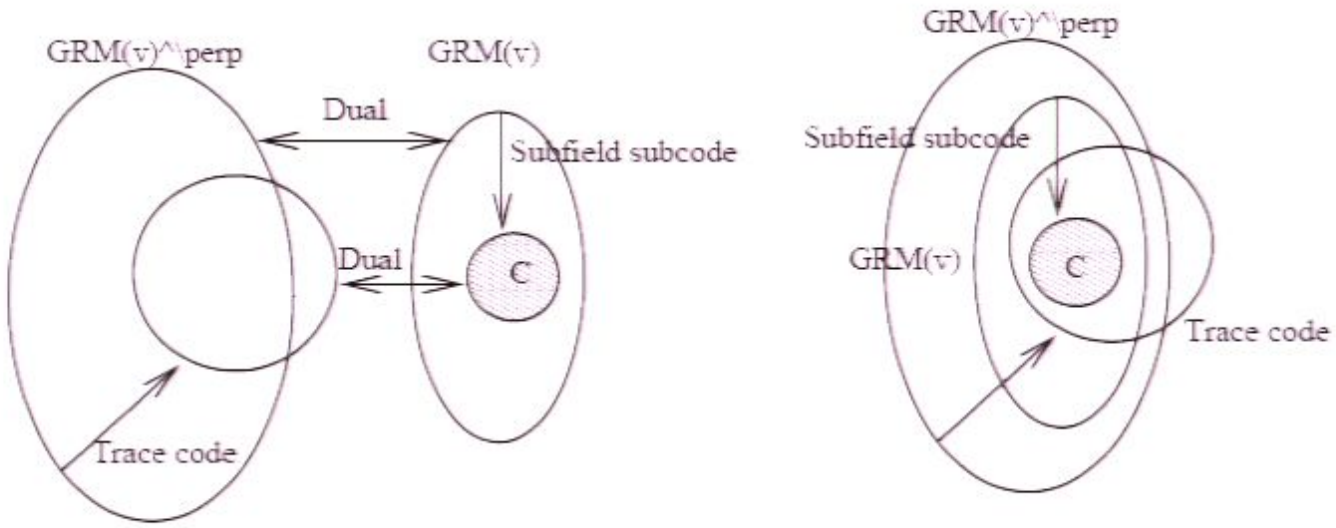
Finite Geometry Quantum LDPC Codes





If $\lceil m/2 + (q-1)/2 \rceil \leq \mu \leq m$, then there exists an $[[2^{ms}, 2k - n, \geq d]]$ quantum LDPC code where $k = \dim C_{\mathrm{EG}}(m, \mu, s, 2)$ and $d = \mathrm{wt}(C_{\mathrm{EG}}(m, \mu, s, 2))$.

Finite Geometry Quantum LDPC Codes



If $\lceil m/2 + (q-1)/2 \rceil \leq \mu \leq m$, then there exists an $[[2^{ms}, 2k - n, \geq d]]$ quantum LDPC code where $k = \dim C_{EG}(m, \mu, s, 2)$ and $d = \mathrm{wt}(C_{EG}(m, \mu, s, 2))$.