Constructions and Performance of Asymmetric Quantum Codes

Martin Rötteler

NEC Laboratories America, Inc.
4 Independence Way, Suite 200
Princeton, NJ 08540, U.S.A.

Conference on Quantum Error Correction
University of Southern California
December 20, 2007

Joint work with Andreas Klappenecker and Pradeep Sarvepalli

Asymmetric Quantum Models – Biased Noise

An interesting observation

- In many physical systems the probabilities for X errors and Z errors are **not equal**. How can this be asymmetry be exploited for the design of efficient quantum codes?
- In particular, the relaxation time T_1 can be much longer than dephasing time T_2.

→ See, e.g., [Ioffe, Mézard 2007], [Evans et al 2007] [Aliferis, Preskill 2007]

→ See also QEC'07 talks by John Preskill and Panos Aliferis

First question: How precisely does $T_1 \gg T_2$ translate into asymmetry in the error probabilities of X and Z errors?

Asymmetric Quantum Models – Biased Noise

An interesting observation

- In many physical systems the probabilities for X errors and Z errors are **not equal**. How can this be asymmetry be exploited for the design of efficient quantum codes?
- In particular, the relaxation time T_1 can be much longer than dephasing time T_2.

→ See, e.g., [Ioffe, Mézard 2007], [Evans et al 2007] [Aliferis, Preskill 2007]

→ See also QEC'07 talks by John Preskill and Panos Aliferis

First question: How precisely does $T_1 \gg T_2$ translate into asymmetry in the error probabilities of X and Z errors?

Asymmetric Quantum Models – Biased Noise

An interesting observation

- In many physical systems the probabilities for X errors and Z errors are **not equal**. How can this be asymmetry be exploited for the design of efficient quantum codes?
- In particular, the relaxation time T_1 can be much longer than dephasing time T_2.

→ See, e.g., [Ioffe, Mézard 2007], [Evans et al 2007] [Aliferis, Preskill 2007]

→ See also QEC'07 talks by John Preskill and Panos Aliferis

First question: How precisely does $T_1 \gg T_2$ translate into asymmetry in the error probabilities of X and Z errors?

Asymmetric Quantum Models – Biased Noise

An interesting observation

- In many physical systems the probabilities for X errors and Z errors are **not equal**. How can this be asymmetry be exploited for the design of efficient quantum codes?
- In particular, the relaxation time T_1 can be much longer than dephasing time T_2.

→ See, e.g., [Ioffe, Mézard 2007], [Evans et al 2007] [Aliferis, Preskill 2007]

→ See also QEC'07 talks by John Preskill and Panos Aliferis

First question: How precisely does $T_1 \gg T_2$ translate into asymmetry in the error probabilities of X and Z errors?

Talk Outline

- A motivating example
- Code constructions:
  - From families of nested CSS codes
  - From quantum LDPC codes
- Performance simulations
- Comparison with related work

Motivating Example

Combined amplitude damping and dephasing

Kraus operators:

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda-\gamma} \end{bmatrix}, A_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}, A_2 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix},$$

where $\sqrt{1-\gamma-\lambda} = e^{-t/T_2}$ and $1-\gamma = e^{-t/T_1}$. Then

$$\begin{aligned} \mathcal{E}(\rho) &= \sum_k A_k \rho A_k^\dagger \\ &= \begin{bmatrix} 1-\rho_{11}e^{-t/T_1} & \rho_{01}e^{-t/T_2} \\ \rho_{10}e^{-t/T_2} & \rho_{11}e^{-t/T_1} \end{bmatrix}. \end{aligned}$$

Questions

- How to relate T_1 and T_2 to p_x, p_y, p_z?
- Perhaps more basic: how to get Pauli channel from this?

Motivating Example

Combined amplitude damping and dephasing

Kraus operators:

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda-\gamma} \end{bmatrix}, A_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}, A_2 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix},$$

where $\sqrt{1-\gamma-\lambda} = e^{-t/T_2}$ and $1-\gamma = e^{-t/T_1}$. Then

$$\begin{aligned} \mathcal{E}(\rho) &= \sum_k A_k \rho A_k^\dagger \\ &= \begin{bmatrix} 1-\rho_{11}e^{-t/T_1} & \rho_{01}e^{-t/T_2} \\ \rho_{10}e^{-t/T_2} & \rho_{11}e^{-t/T_1} \end{bmatrix}. \end{aligned}$$

Questions

- How to relate T_1 and T_2 to p_x, p_y, p_z?
- Perhaps more basic: how to get Pauli channel from this?

Pauli Channels

One qubit

- Depolarizing channel:

$$\rho \mapsto (1-p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$$

- General Pauli channel:

$$\rho \mapsto (1-p_x-p_y-p_z)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$$

Several qubits

- Combinations X, Z, and $Y = XZ$ of bit-flips and phase-flips cover all errors on a single qubit.
- We assume that errors affect qubits independently and are interested in correcting errors of bounded weight.

  $\rightarrow$ See also QEC'07 tutorial by Daniel Gottesman.

Pauli Twirling

Goal: Map an arbitrary channel to a Pauli channel. Recall that a general quantum channel is given by a CPTP map:

$$\mathcal{E} : \rho \mapsto \sum_k A_k \rho A_k^\dagger$$

Alternative representation is as $\rho \mapsto \sum_{k,\ell} \chi_{k,\ell} P_k \rho P_\ell$. Twirling with random Pauli operators maps this to

$$\overline{\mathcal{E}} : \rho \mapsto \sum_k \chi_{k,k} P_k \rho P_k$$

→ See also QEC'07 tutorial by Ray Laflamme.

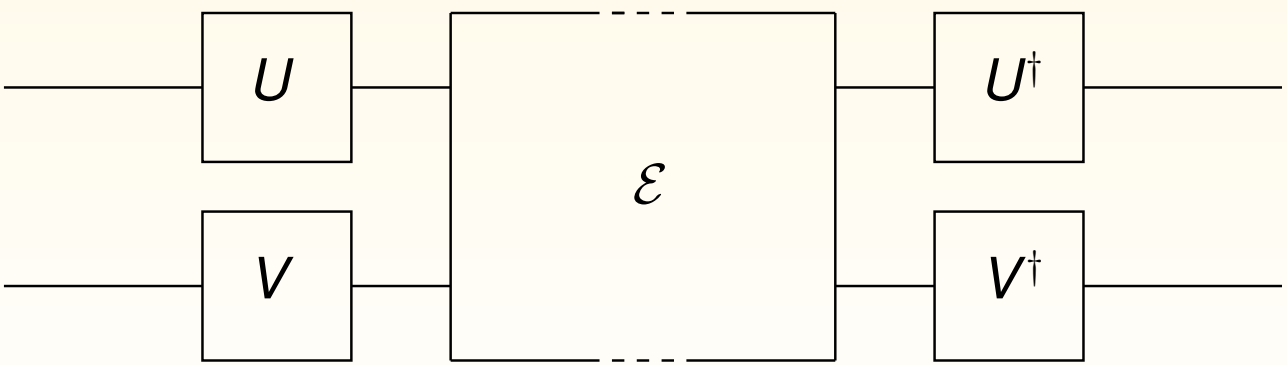
Pauli Twirling

Goal: Map an arbitrary channel to a Pauli channel. Recall that a general quantum channel is given by a CPTP map:

$$\mathcal{E} : \rho \mapsto \sum_k A_k \rho A_k^\dagger$$

Alternative representation is as $\rho \mapsto \sum_{k,\ell} \chi_{k,\ell} P_k \rho P_\ell$. Twirling with random Pauli operators maps this to

$$\overline{\mathcal{E}} : \rho \mapsto \sum_k \chi_{k,k} P_k \rho P_k$$



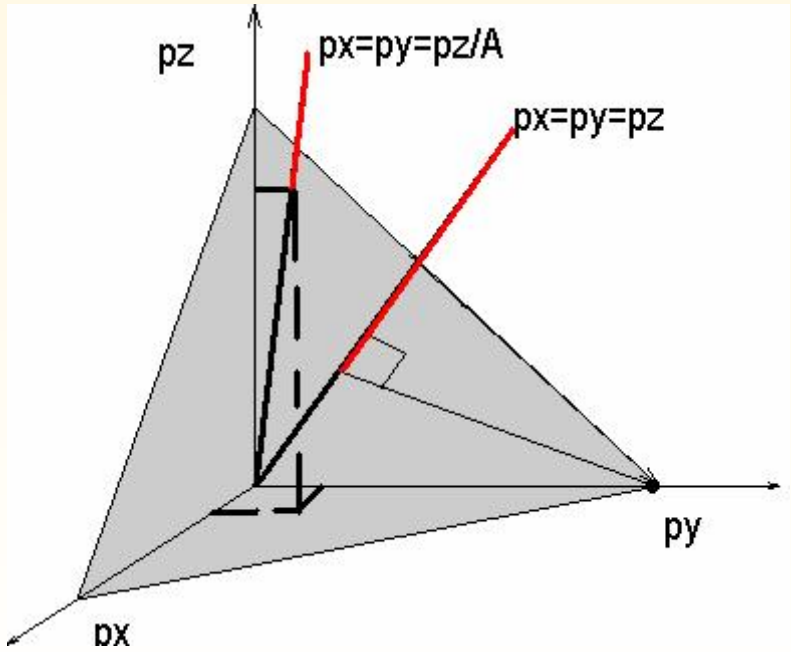
$\rightarrow$ See also QEC'07 tutorial by Ray Laflamme.

Amplitude Damping and Dephasing Redux

Associated Pauli-twirled channel:

$$\overline{\mathcal{E}}(\rho) = (1 - p_x - p_y - p_z)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z.$$

- Here $p_x = p_y = (1-e^{-t/T_1})/4$ and $p_z = 1/2 - p_x - \frac{1}{2}e^{-t/T_2}$.
- The asymmetry ratio is $\frac{p_z}{p_x} = 1 + 2\frac{1-e^{t/T_1(1-T_1/T_2)}}{e^{t/T_1}-1}$
- For $t \ll T_1$ this ratio is $2T_1/T_2 - 1$.



Code constructions

Defining Asymmetric Quantum Codes as CSS codes

CSS Construction

Let $C_x = [n, k_x]_q$, $C_z = [n, k_z]_q$ be codes in $\mathbb{F}_q^n$ with $C_x^\perp \subseteq C_z$.

- Corresponding stabilizer of the CSS code:

$$H = (X|Z) = \left(\begin{array}{c|c} H_x & 0 \\ 0 & H_z \end{array} \right)$$

  where H_x and H_z are parity check matrices of C_X, C_Z.

- This defines $[[n, k_x + k_z - n, d_x/d_z]]_q$ asymmetric quantum code, with $d_x = \mathrm{wt}(C_x \setminus C_z^\perp)$ and $d_z = \mathrm{wt}(C_z \setminus C_x^\perp)$.

Idea: Use CSS construction with C_x much stronger than C_z.
See also [Steane, PRA **54**, 4741 (1996)]

Singleton bound: Any pure asymmetric $[[n, k, d_x/d_z]]_q$ CSS code (more generally, any $\mathbb{F}_q$-linear CSS code) satisfies

$$k \leq n - d_x - d_z + 2.$$

Linear Programming Bounds

Theorem: If an $[[n, k, d_x/d_z]]_2$ asymmetric CSS stabilizer code with $k > 0$ exists, then there exists an integer solution to the problem of maximizing $\sum_{j=1}^{d_z-1} A_j$ subject to the constraints

- $A_0 = A_0^\perp = B_0 = B_0^\perp = 1$ and $A_j, A_j^\perp, B_j, B_j^\perp \geq 0$ $(1 \leq j \leq n)$,
- $\sum_{j=0}^{n} A_j = 2^{k'}, \sum_{j=0}^{n} B_j = 2^{n-k-k'}$, for some $0 < k' < n - k$,
- $A_j^\perp = 1/2^{k'} \sum_{r=0}^{n} K_j(r) A_r$ for all $0 \leq j \leq n$;
- $B_j^\perp = 1/2^{n-k-k'} \sum_{r=0}^{n} K_j(r) B_r$ for all $0 \leq j \leq n$;
- $A_j = B_j^\perp$ for all $0 \leq j < d_x$ and $A_j \leq B_j^\perp$ for all $d_x \leq j \leq n$;
- $B_j = A_j^\perp$ for all $0 \leq j < d_z$ and $B_j \leq A_j^\perp$ for all $d_z \leq j \leq n$;

where $K_j(r)$ denotes the Krawtchouk polynomial

$$K_j(r) = \sum_{s=0}^{j} (-1)^s \binom{r}{s} \binom{n-r}{j-s}.$$

Example: From this follows that a $[[15, 1, 3/7]]$ might exist.

Reed-Muller Codes

A classic code construction

Boolean functions: $f := \{0,1\}^m \to \{0,1\}$, represented in algebraic normal form $f(x_1, \ldots, x_m) = \bigoplus_{v \in \{0,1\}^m} \alpha_v x_1^{v_1} \ldots x_m^{v_m}$. Degree of f is defined as $\max_{\alpha_v \neq 0}(\mathrm{wt}(v))$.

Reed-Muller code: $\mathrm{RM}(\mu, m)$ is generated by truth table of all Boolean functions in m variables of degree $\leq \mu$.

Example: RM(2,3)

$$\begin{pmatrix} 1 \\ x_1 \\ x_2 \\ x_3 \\ x_1x_2 \\ x_1x_3 \\ x_2x_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Asymmetric Quantum Codes From RM Codes

Properties of Reed-Muller codes

- The Reed-Muller code $\mathrm{RM}(r, m)$ of order r in m variables has length 2^m and parameters $[2^m, \sum_{j=0}^{r} \binom{m}{j}, 2^{m-r}]$.
- Fact: $\mathrm{RM}(r, m)^{\perp} = \mathrm{RM}(m - r - 1, m)$.
- Fact: if $r_1 \leq r_2$ then $\mathrm{RM}(r_1, m) \subseteq \mathrm{RM}(r_2, m)$.

Result (see also [Steane, IEEE-IT (1999)]):
There exist $[[2^m, \sum_{j=r_1+1}^{r_2} \binom{m}{j}, 2^{m-r_2}/2^{r_1+1}]]_2$ codes.

Examples:

r_1	r_2	Code $[[n, k, d_x/d_z]]_2$	Rate k/n	Asymmetry d_z/d_x
7	8	$[[1024, 45, 4/256]]_2$	0.044	64
6	8	$[[1024, 165, 4/128]]_2$	0.161	32
5	8	$[[1024, 375, 4/64]]_2$	0.366	16
6	7	$[[1024, 120, 8/128]]_2$	0.117	16

BCH Codes

Definition

- Given $\mathbb{F}_q$ and $n > 0$ such that $\gcd(n, q) = 1$. Let $r = \mathrm{ord}_n(q)$ and let α be a primitive nth root of unity. Then

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^{b} & \alpha^{2b} & \cdots & \alpha^{b(n-1)} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(b+1)(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(b+\delta-2)} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(b+\delta-2)(n-1)} \end{bmatrix}.$$

  is a parity check matrix for a code $\mathrm{BCH}(\delta)$ with $d_{\min} \geq \delta$.

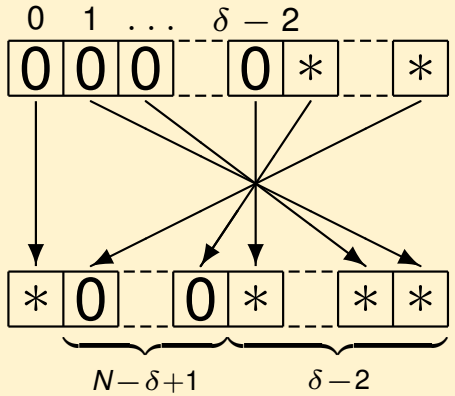
- Its defining set of zeros is $\mathcal{Z} = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2}$, where $C_x = \{xq^i \bmod n \mid i \in \mathbb{Z}, i \geq 0\}$.
- Code is cyclic with generator polynomial $g(x)$ of the form

$$g(x) = \prod_{z \in \mathcal{Z}} (x - \alpha^z).$$

Asymmetric Quantum Codes From BCH Codes

Properties

- Dimension $k \geq n - (\delta - 1)\,\mathrm{ord}_n(q)$.
- Dual code:



- Nested codes: if $n = 2^m - 1$ and $\delta \leq \delta_{\max} = 2^{\lceil m/2 \rceil} - 1$ and δ odd, then $\mathrm{BCH}(\delta)^{\perp} \subseteq \mathrm{BCH}(\delta)$. [Steane, IEEE-IT (1999)], [Aly, Klappenecker, Sarvepalli, IEEE-IT (2007)]

Result

Let $m \geq 2$ and $2 \leq \delta_1 < \delta_2 < \delta_{\max}$, with δ_i odd. Then there exists an $[[2^m - 1, m(\delta_2 - \delta_1)/2, d_x/d_z]]_2$ asymmetric BCH stabilizer code, where $d_x \geq \delta_1$ and $d_z \geq \delta_{\max} + 1$.

Asymmetric BCH Quantum Codes

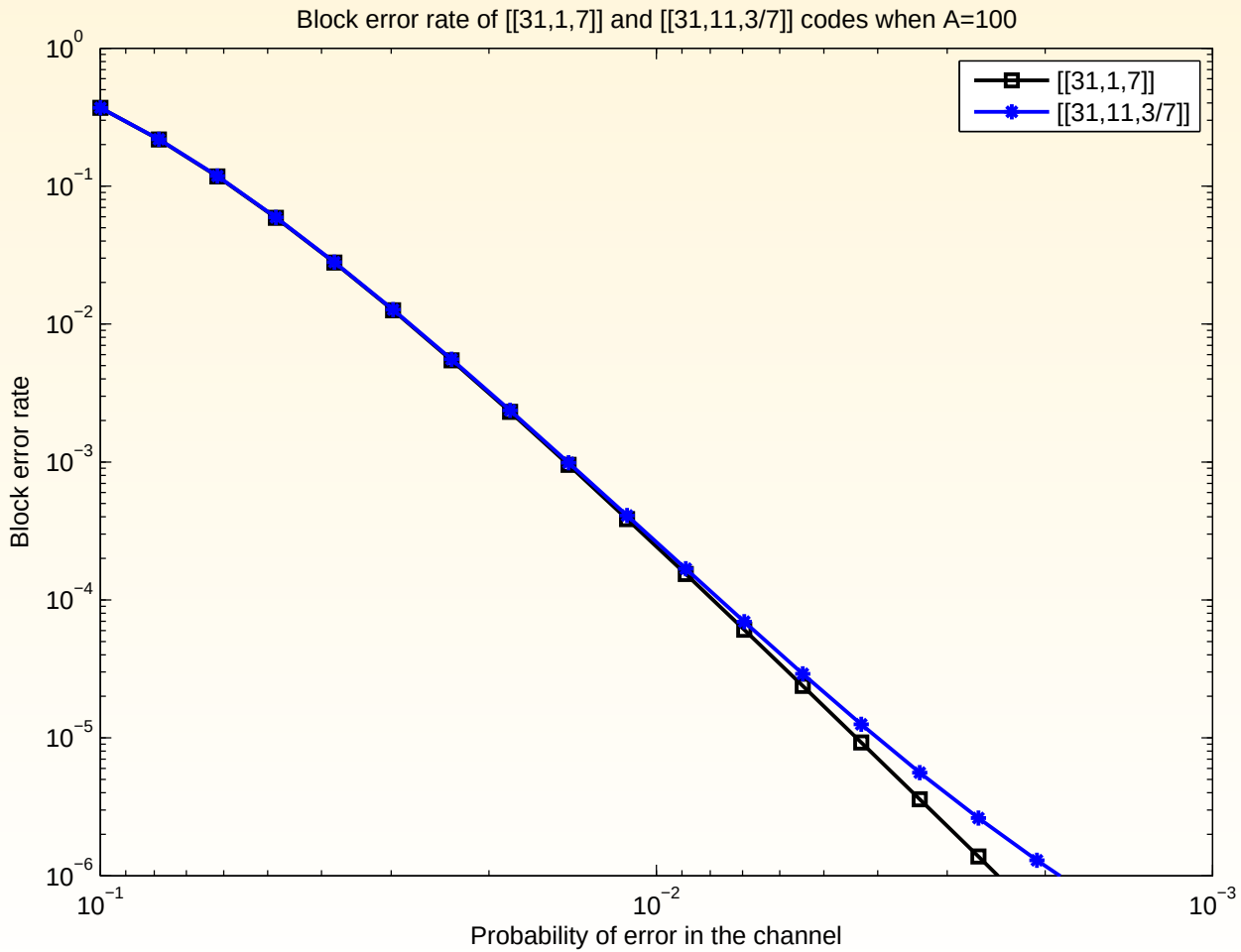
δ_1	δ_2	Code $[[n, k, d_x/d_z]]_2$	Rate k/n	Asymmetry d_z/d_x
29	31	$[[1023, 10, 29/32]]_2$	0.00978	≈ 1
17	31	$[[1023, 70, 17/32]]_2$	0.06843	
15	31	$[[1023, 80, 15/32]]_2$	0.07820	≈ 2
13	31	$[[1023, 90, 13/32]]_2$	0.08798	
11	31	$[[1023, 100, 11/32]]_2$	0.09775	≈ 3
9	31	$[[1023, 110, 9/32]]_2$	0.10753	
7	31	$[[1023, 120, 7/32]]_2$	0.11730	≈ 4
5	31	$[[1023, 130, 5/32]]_2$	0.12708	≈ 6
3	31	$[[1023, 140, 3/32]]_2$	0.13685	≈ 10
27	29	$[[1023, 10, 27/32]]_2$	0.00978	≈ 1
15	29	$[[1023, 60, 15/32]]_2$	0.05865	≈ 2
9	29	$[[1023, 100, 9/32]]_2$	0.09775	≈ 3
7	29	$[[1023, 110, 7/32]]_2$	0.10753	≈ 4
5	29	$[[1023, 120, 5/32]]_2$	0.11730	≈ 6
3	29	$[[1023, 130, 3/32]]_2$	0.12708	≈ 10

Performance simulations

Advantage I: Improvement of Data Rate

Property: Asymmetric codes can achieve a much higher data rate than symmetric codes with similar performance.

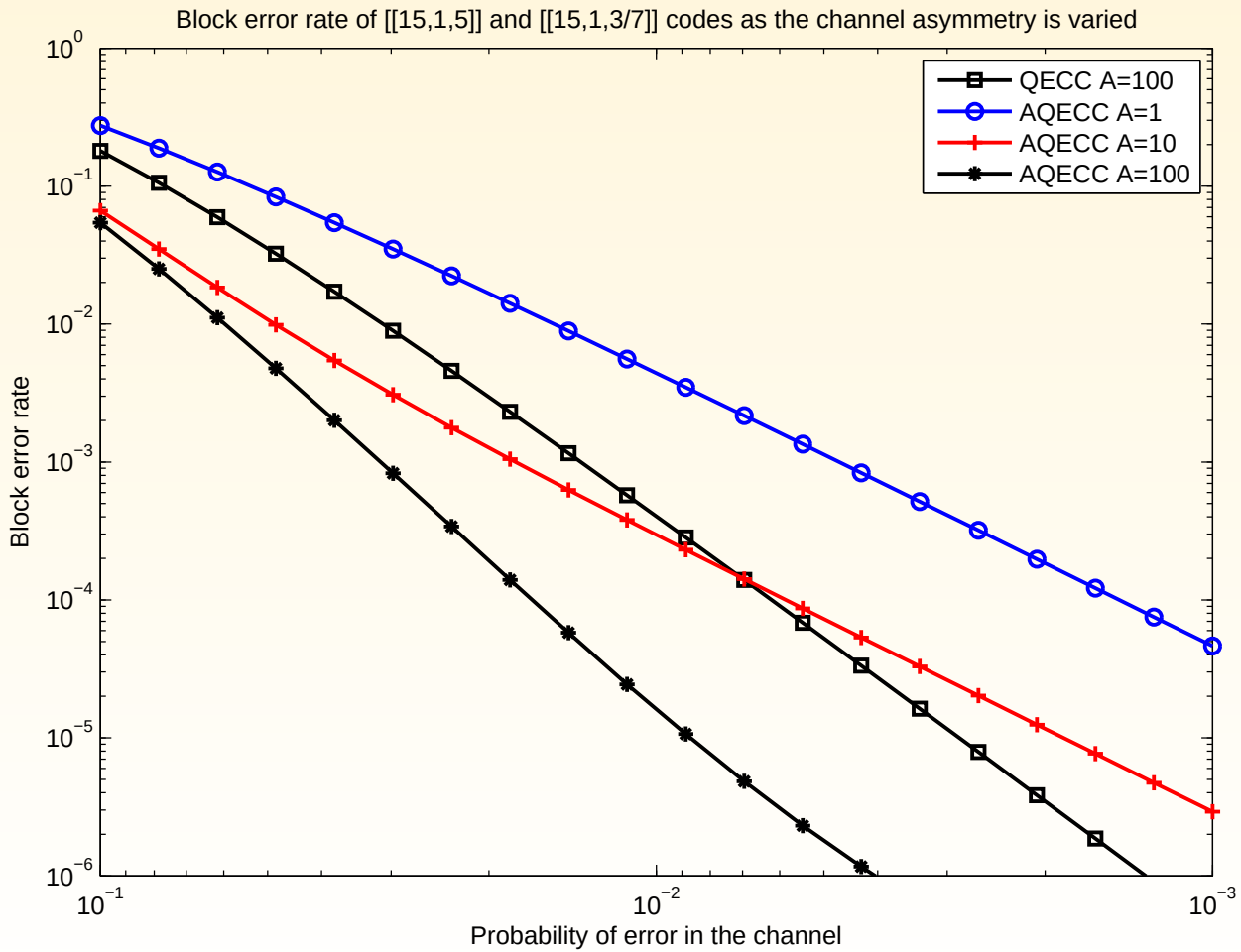
Example: Performances of $[[31, 1, 7]]$ and $[[31, 11, 3/7]]$.



Advantage II: Improvement of Performance

Property: Asymmetric codes perform better on asymmetric channels than symmetric codes with similar data rate.

Example: The performance of $[[15, 1, 3/7]]$.



Quantum LDPC Codes

Quantum LDPC Conundrum

Fact 1

LDPC codes do not perform well if Tanner graph has 4 cycles.

Fact 2

Tanner graph for stabilizer codes necessarily has 4 cycles.

Quantum LDPC Conundrum

Fact 1

LDPC codes do not perform well if Tanner graph has 4 cycles.

Fact 2

Tanner graph for stabilizer codes necessarily has 4 cycles.

Quantum LDPC Conundrum

Fact 1

LDPC codes do not perform well if Tanner graph has 4 cycles.

Fact 2

Tanner graph for stabilizer codes necessarily has 4 cycles.

Quantum LDPC Conundrum

Fact 1

LDPC codes do not perform well if Tanner graph has 4 cycles.

???

Fact 2

Tanner graph for stabilizer codes necessarily has 4 cycles.

Possible Ways Out Of This Dilemma

- Entanglement-enhanced codes
  $\longrightarrow$ See also QEC'07 talk by Todd Brun
- Subsystem codes
  $\longrightarrow$ [A. Klappenecker, MR, P. Sarvepalli] in preparation
- This talk takes yet another approach, the "blissfully ignorant" one. It is based on the fact that some LDPC codes can tolerate **enormous amounts** of 4 cycles without affecting performance.

Other approaches: [MacKey, Mitchison, McFadden '04], [Camera, Ollivier, Tillich '05], [Hagiwara, Imai '07].

Possible Ways Out Of This Dilemma

- Entanglement-enhanced codes
  $\longrightarrow$ See also QEC'07 talk by Todd Brun
- Subsystem codes
  $\longrightarrow$ [A. Klappenecker, MR, P. Sarvepalli] in preparation
- This talk takes yet another approach, the "blissfully ignorant" one. It is based on the fact that some LDPC codes can tolerate **enormous amounts** of 4 cycles without affecting performance.

Other approaches: [MacKey, Mitchison, McFadden '04], [Camera, Ollivier, Tillich '05], [Hagiwara, Imai '07].

LDPC Codes 101

Parity check matrix

As an example take the $[7, 4, 3]$ Hamming code:

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

bit nodes $x_1, x_2, \ldots, x_7$

check nodes C_1, C_2, C_3.

Tanner graph

LDPC Codes 101

Parity check matrix

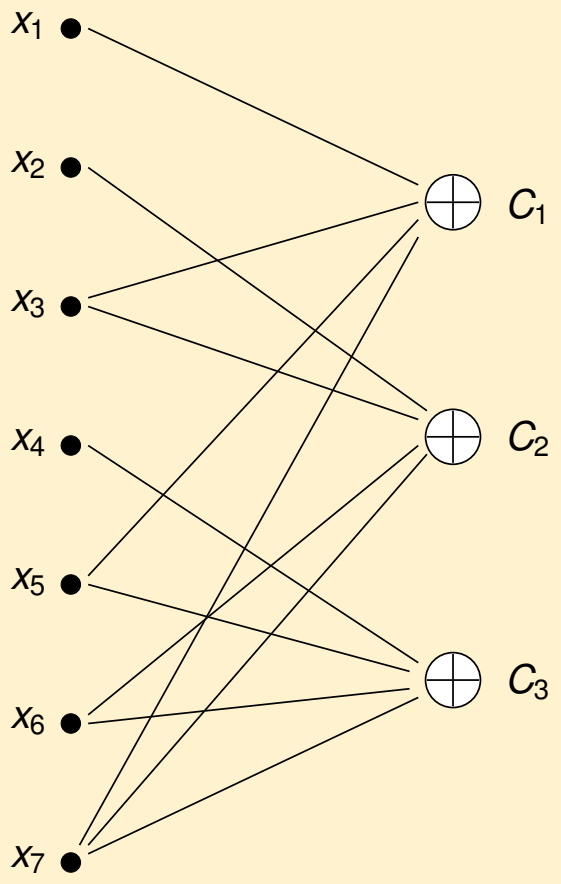
As an example take the $[7, 4, 3]$ Hamming code:

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

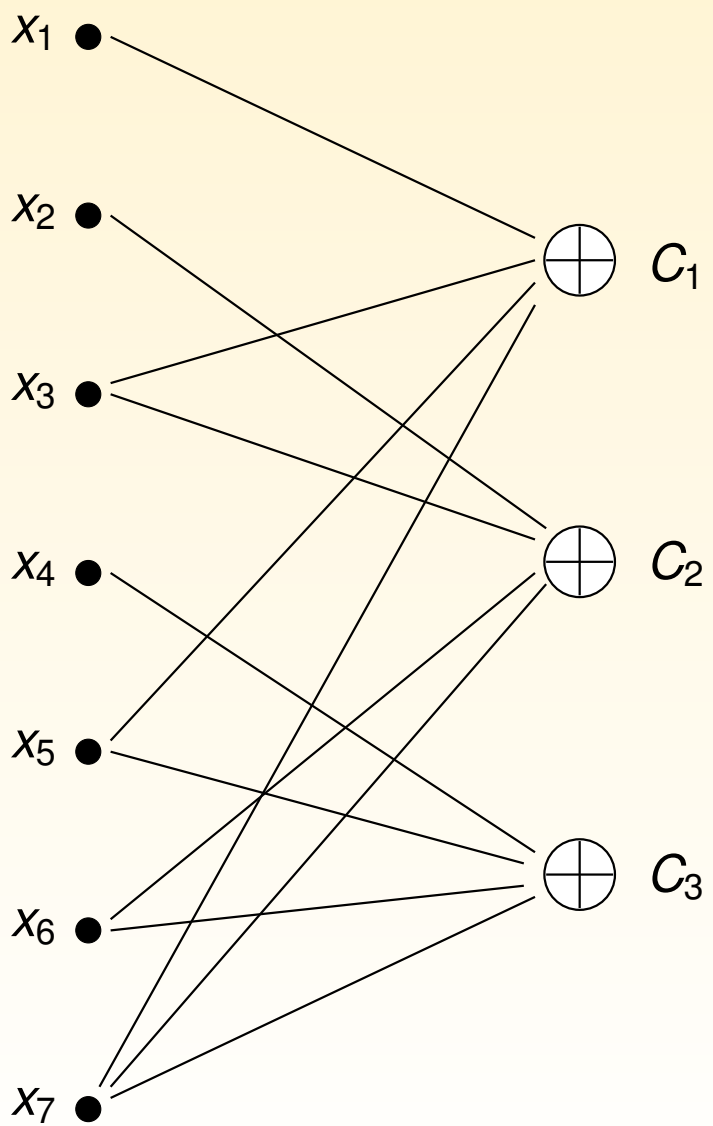
bit nodes $x_1, x_2, \ldots, x_7$

check nodes C_1, C_2, C_3.

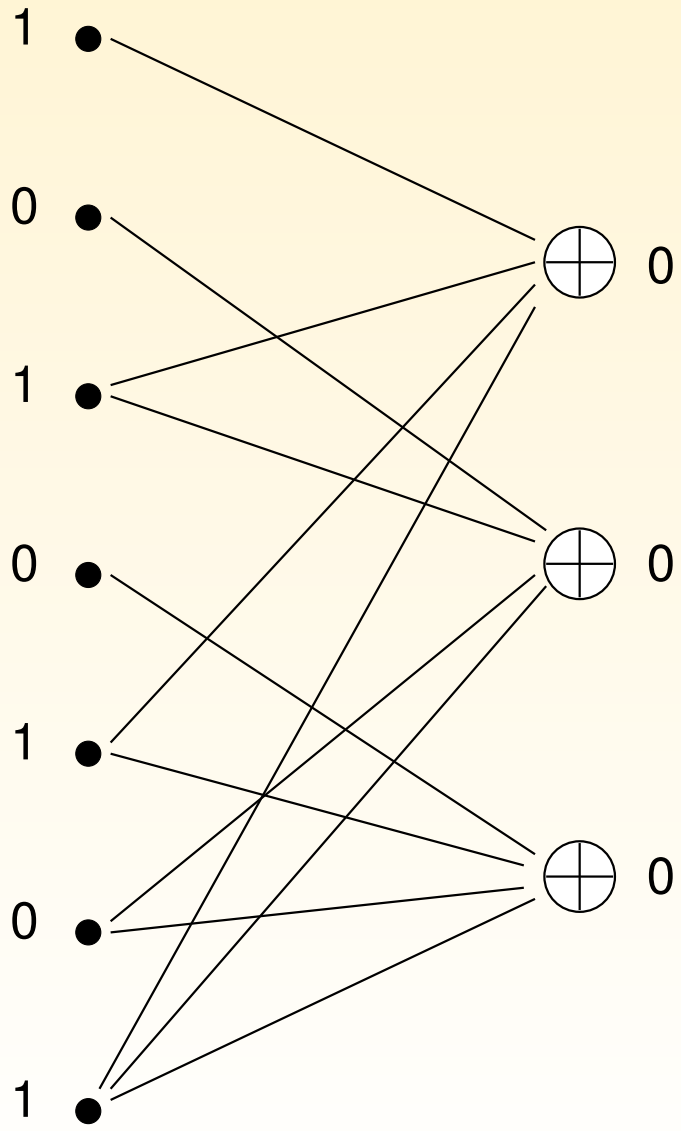
Tanner graph



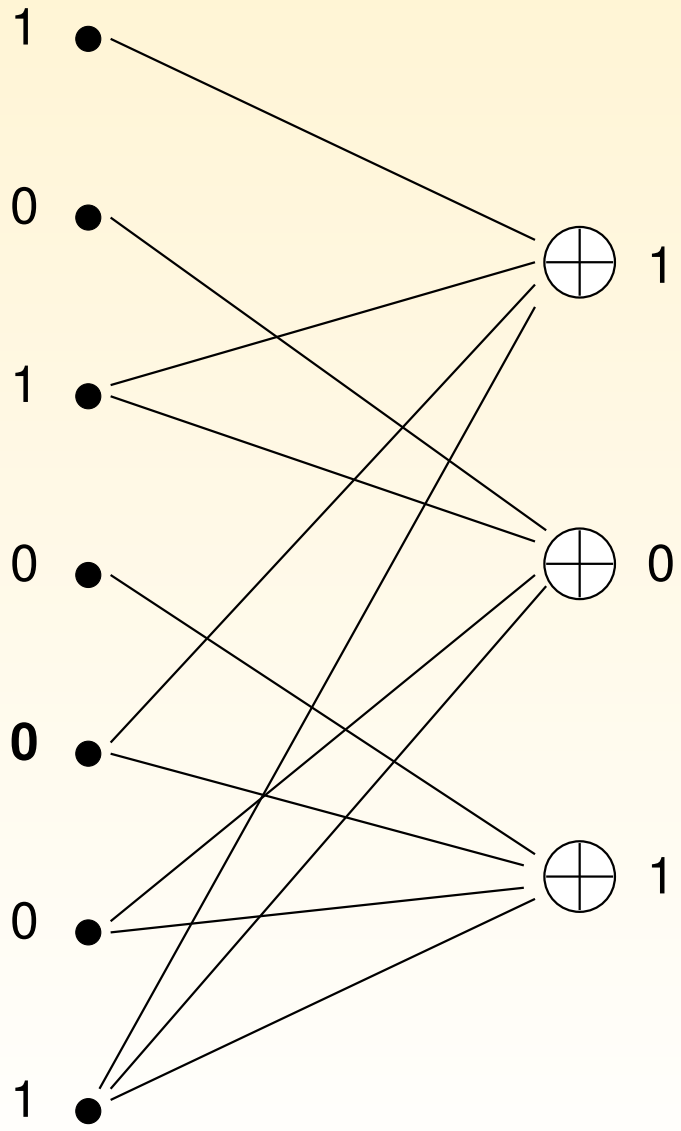
Iterative Decoding



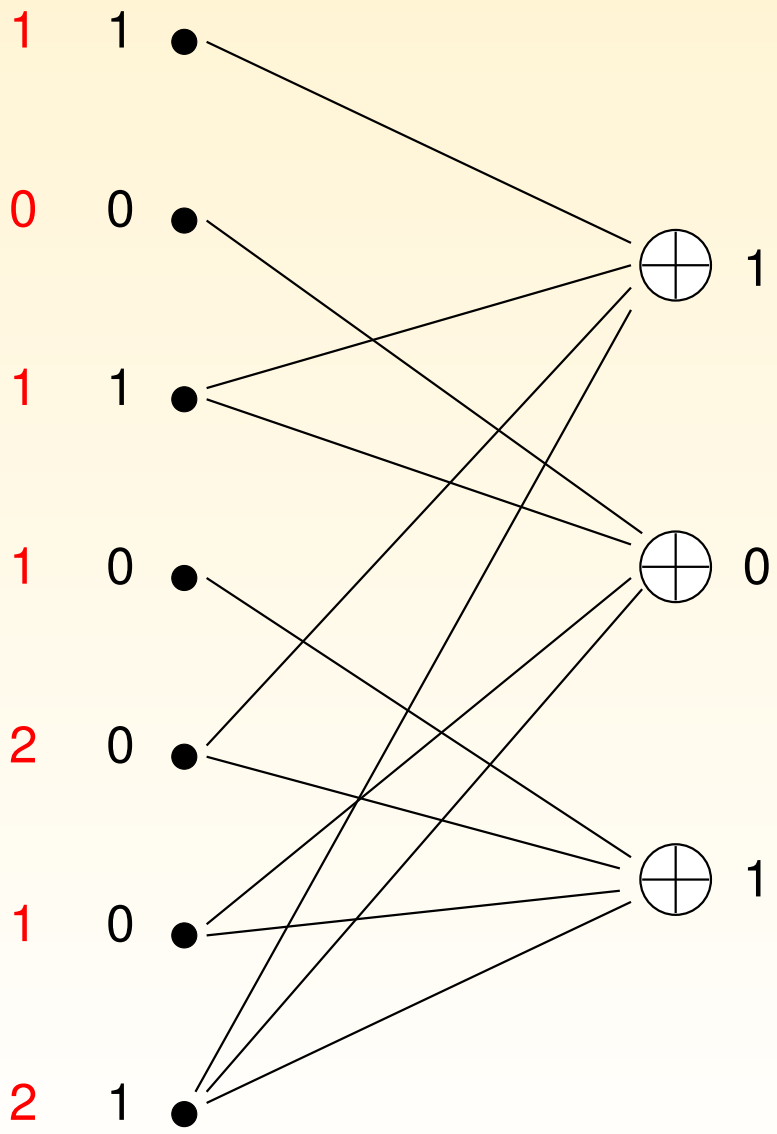
Iterative Decoding – Example BF Algorithm



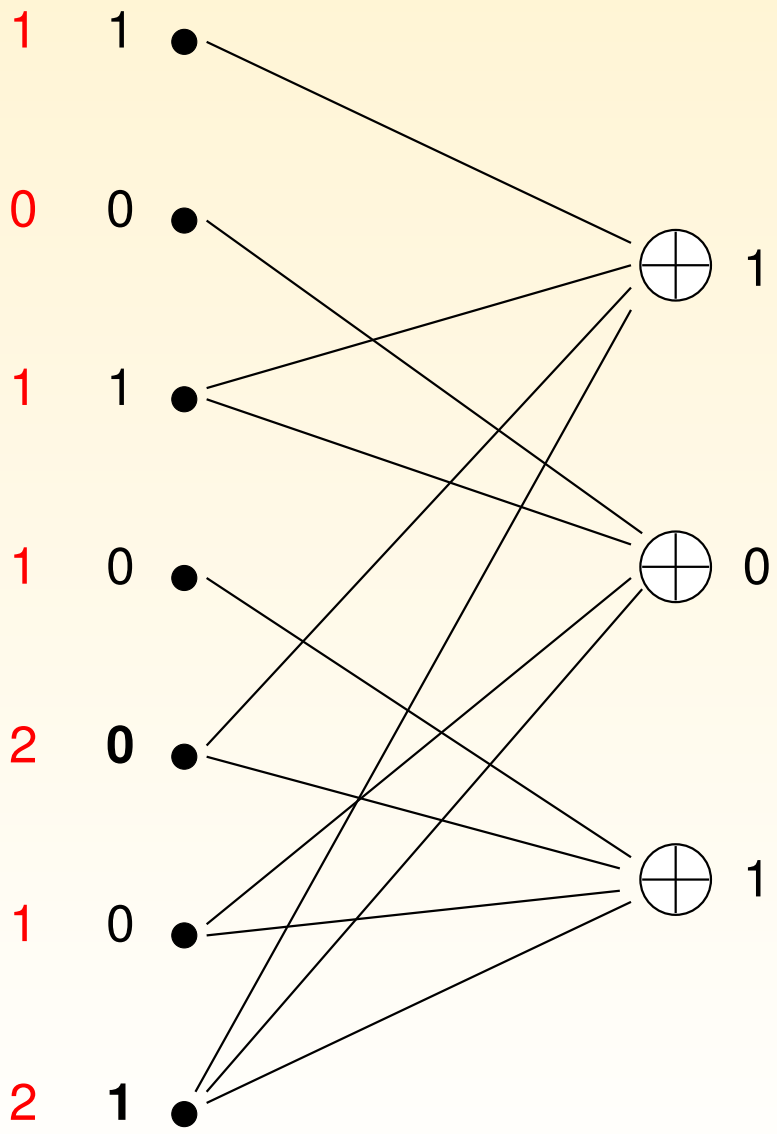
Iterative Decoding – Example BF Algorithm



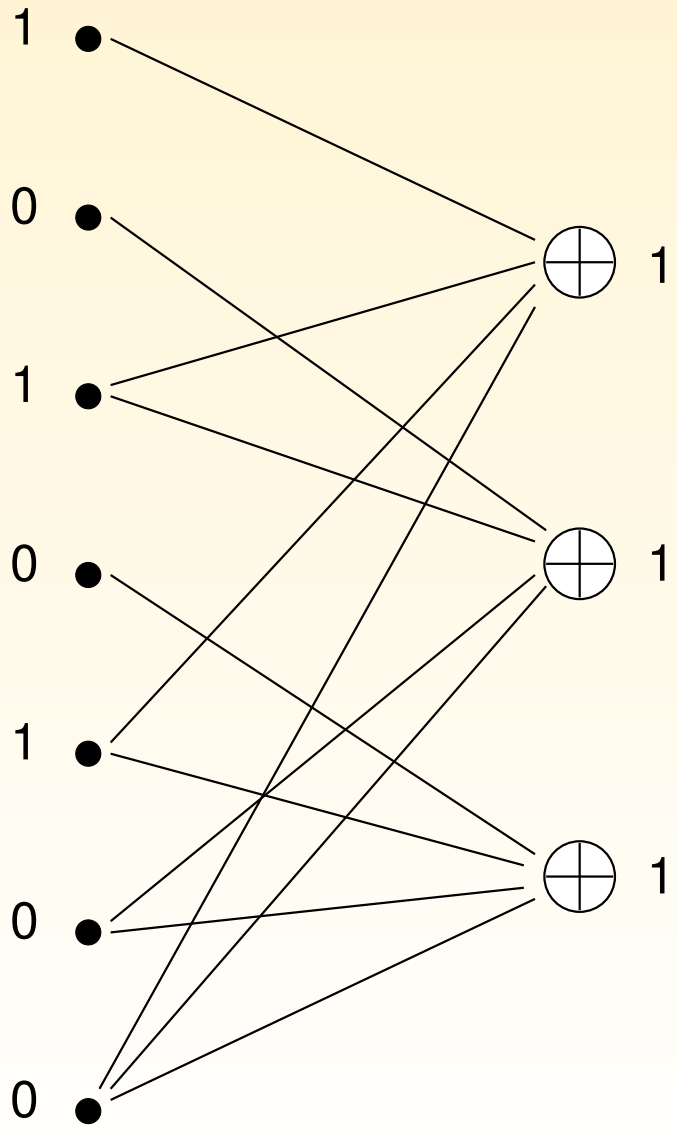
Iterative Decoding – Example BF Algorithm



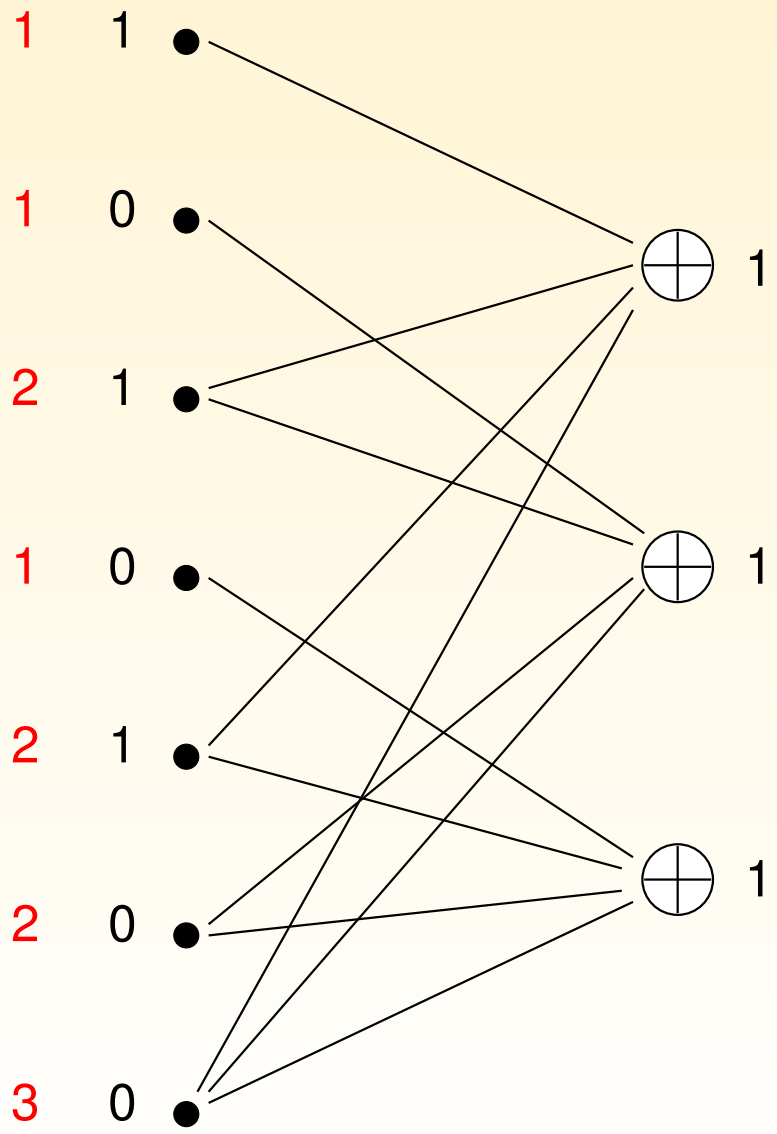
Iterative Decoding – Example BF Algorithm



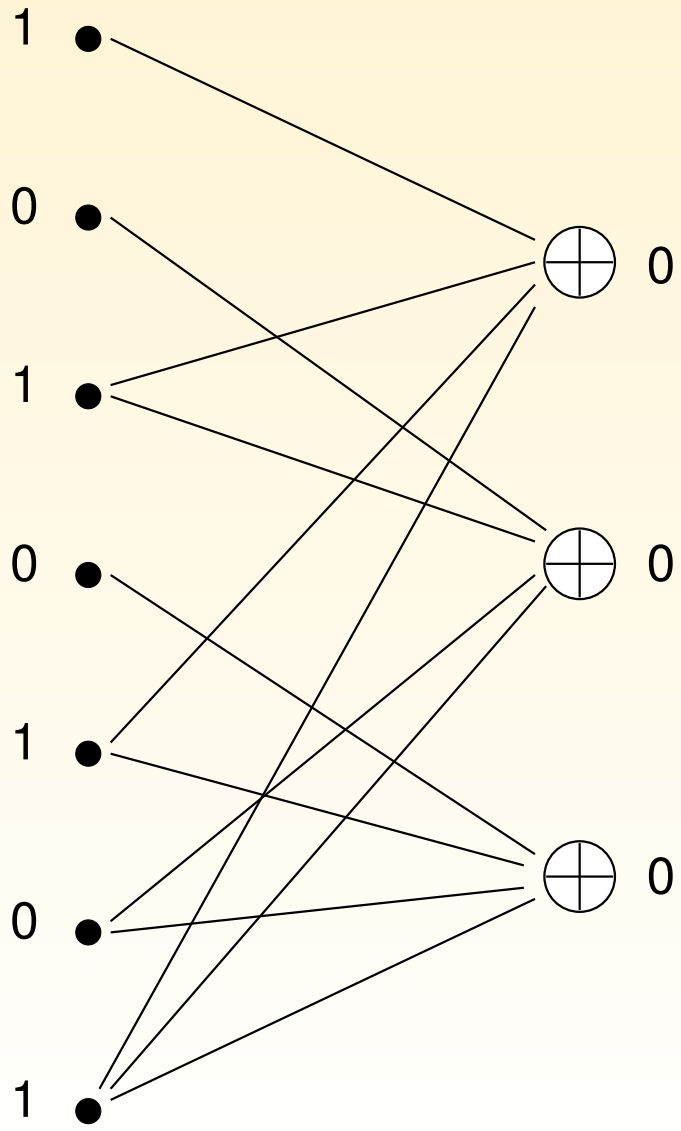
Iterative Decoding – Example BF Algorithm



Iterative Decoding – Example BF Algorithm

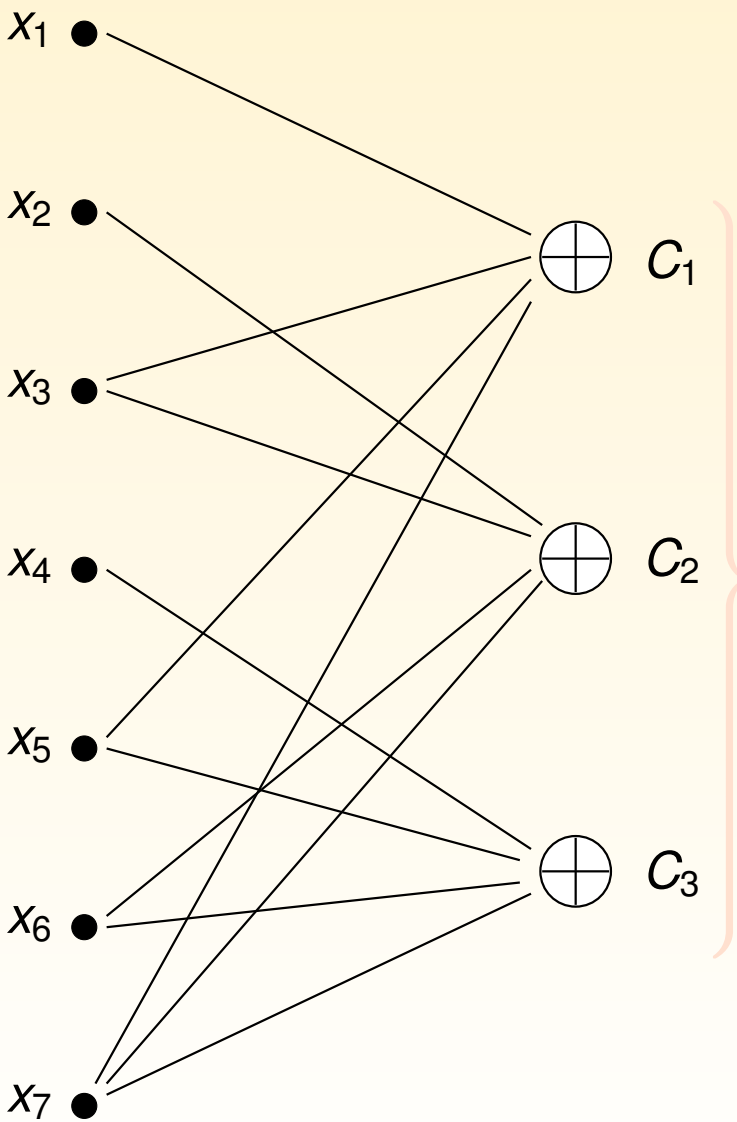


Iterative Decoding – Example BF Algorithm



Iterative Decoding: The Quantum Case

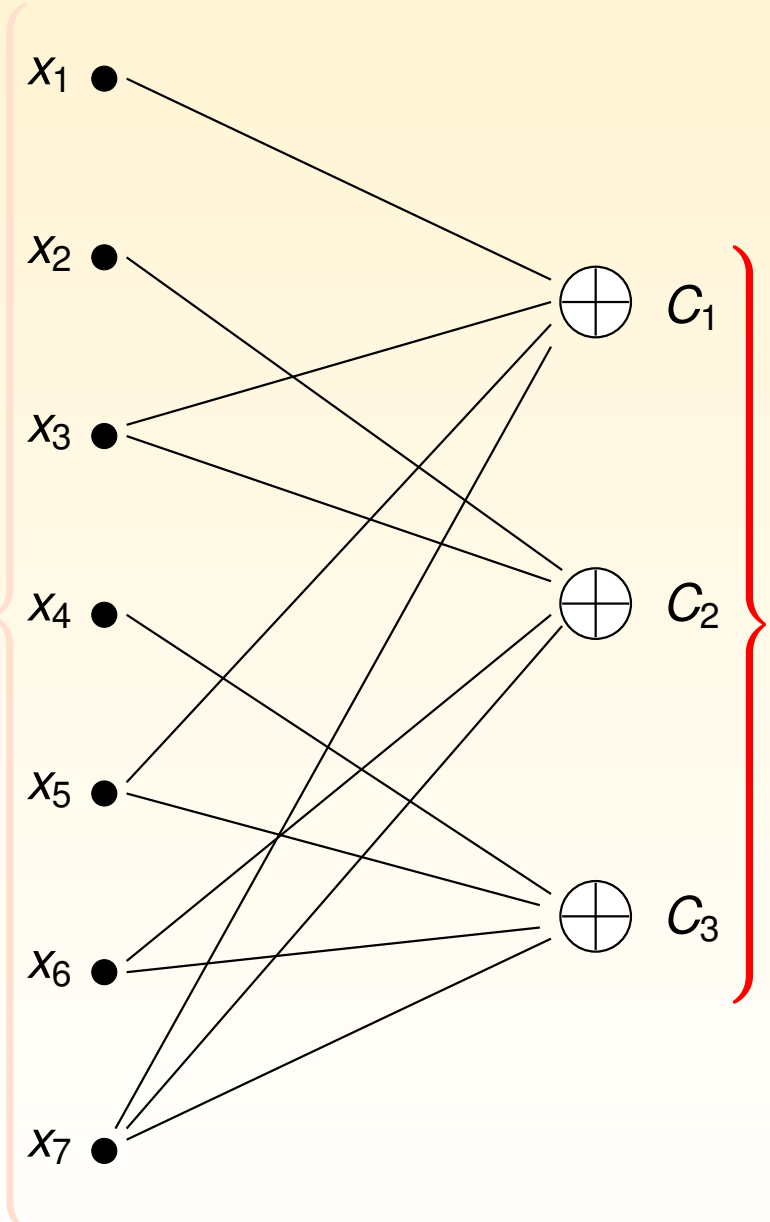
All zeros goes here



Syndrome goes here

Iterative Decoding: The Quantum Case

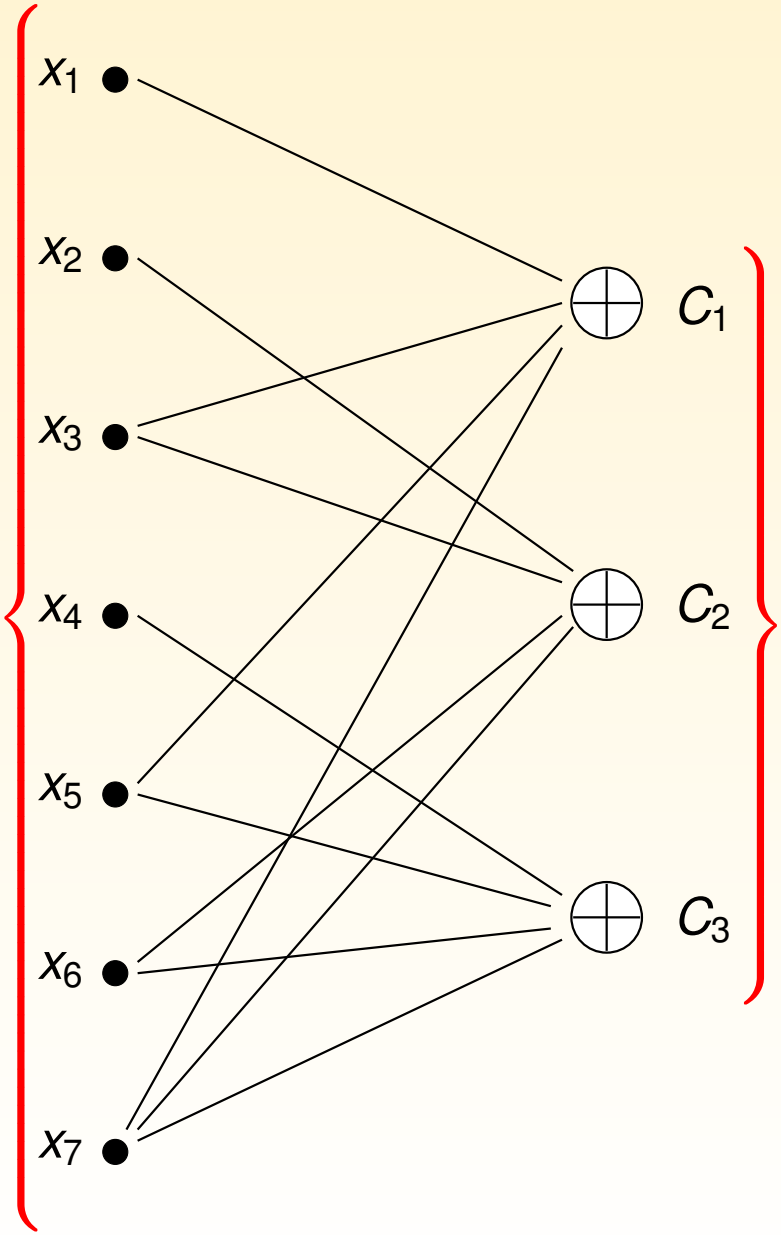
All zeros goes here



Syndrome goes here

Iterative Decoding: The Quantum Case

All zeros goes here



Syndrome goes here

Finite Geometry LDPC Codes

Finite Geometries – Axioms

Finite geometry is a collection of points and lines such that

- Every line has ρ points
- Every point is on γ lines
- Any two lines intersect only at one or no points
- Any two points are connected by only one line

Finite Geometries – Realizations

There are (at least) two geometries that satisfy these axioms.

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

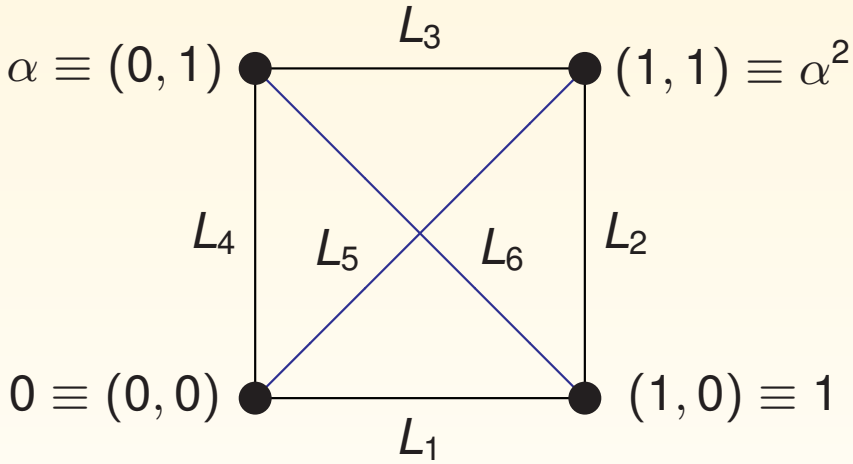
Finite Geometries – A Simple Example

- Identify $\mathbb{F}_2^2$ with the elements $\{0, 1, \alpha, \alpha^2\}$ of $\mathbb{F}_4$, i. e., $\{(0,0), (1,0), (0,1), (1,1)\}$
- Lines $= \{\{0,1\}, \{0,\alpha\}, \{0,\alpha^2\}, \{1,\alpha\}, \{1,\alpha^2\}, \{\alpha,\alpha^2\}\}$

Assign incidence vector to lines

For instance L_1 corresponds to

Points	0	1	α	α^2
Line	1	1	0	0

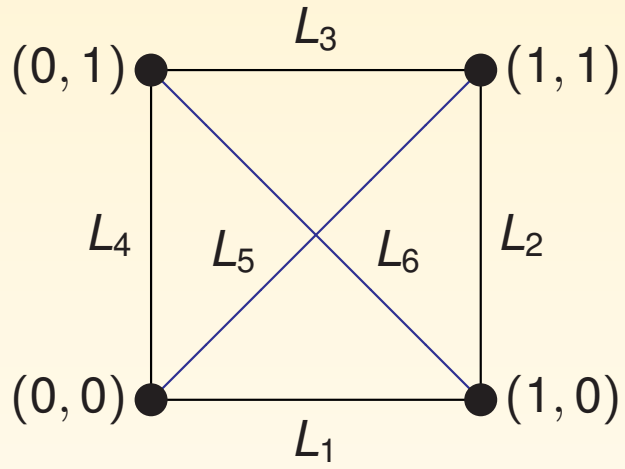


- More generally, this can be applied to $\mathbb{F}_{p^s}^m$ and leads to a finite Euclidean geometry $\mathrm{EG}(m, p^s)$.

Finite Geometry LDPC Codes

Now, list all the incidence vectors for all the lines:

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



- Gives the $[4,1,4]$ code
- Note the redundancy in the parity checks

Define $C_{\mathrm{EG}}^{(1)}(m,s,p)$ code as null space of the incidence vectors of the lines in $\mathrm{EG}(m,p^s)$.

Parameters of Finite Geometry LDPC Codes

- The associated parity check matrices have precisely ρ many 1s in each row and γ many 1s in each column
- Somewhat involved expressions are known for the dimension k of these codes
- Excluding the origin gives cyclic codes
- Including the origin gives extended cyclic codes

Cyclic

n	$p^{ms} - 1$
ρ	p^s
γ	$\frac{p^{ms}-1}{p^s-1} - 1$
d	$\geq \gamma + 1$
k	$\ldots$

Extended

n	p^{ms}
ρ	p^s
γ	$\frac{p^{ms}-1}{p^s-1}$
d	$\geq \gamma + 1$
k	$\ldots$

Generalizing This Simple Idea

Hyperplanes and general FG codes

- We consider now lines to be bit nodes and planes to be check nodes. Or more generally hyperplanes (flats) of different dimensions.
- Start with the Euclidean geometry $\mathrm{EG}(m, p^s)$. Consider all the flats of dimension μ_1 and μ_2, where $\mu_2 > \mu_1$.
- The incidence vector of a μ_2 flat is an n-tuple with ith component 1 if and only if ith μ_1-flat is contained in it
- The incidence vectors of all μ_2-flats gives the parity check matrix of a $C_{\mathrm{EG}}^{(1)}(m, \mu_2, \mu_1, s, p)$ code
- If $\mu_2 - \mu_1 > 1$, then these codes have many 4-cycles, yet they do not show any error floor.

Cyclic $C_{\mathrm{EG}}^{(1)}(3, 2, 0, 3, 2)$ code $[511, 448]$ has > 3.6 million 4-cycles, yet no error floors for BER around 10^{-6}

Generalizing This Simple Idea

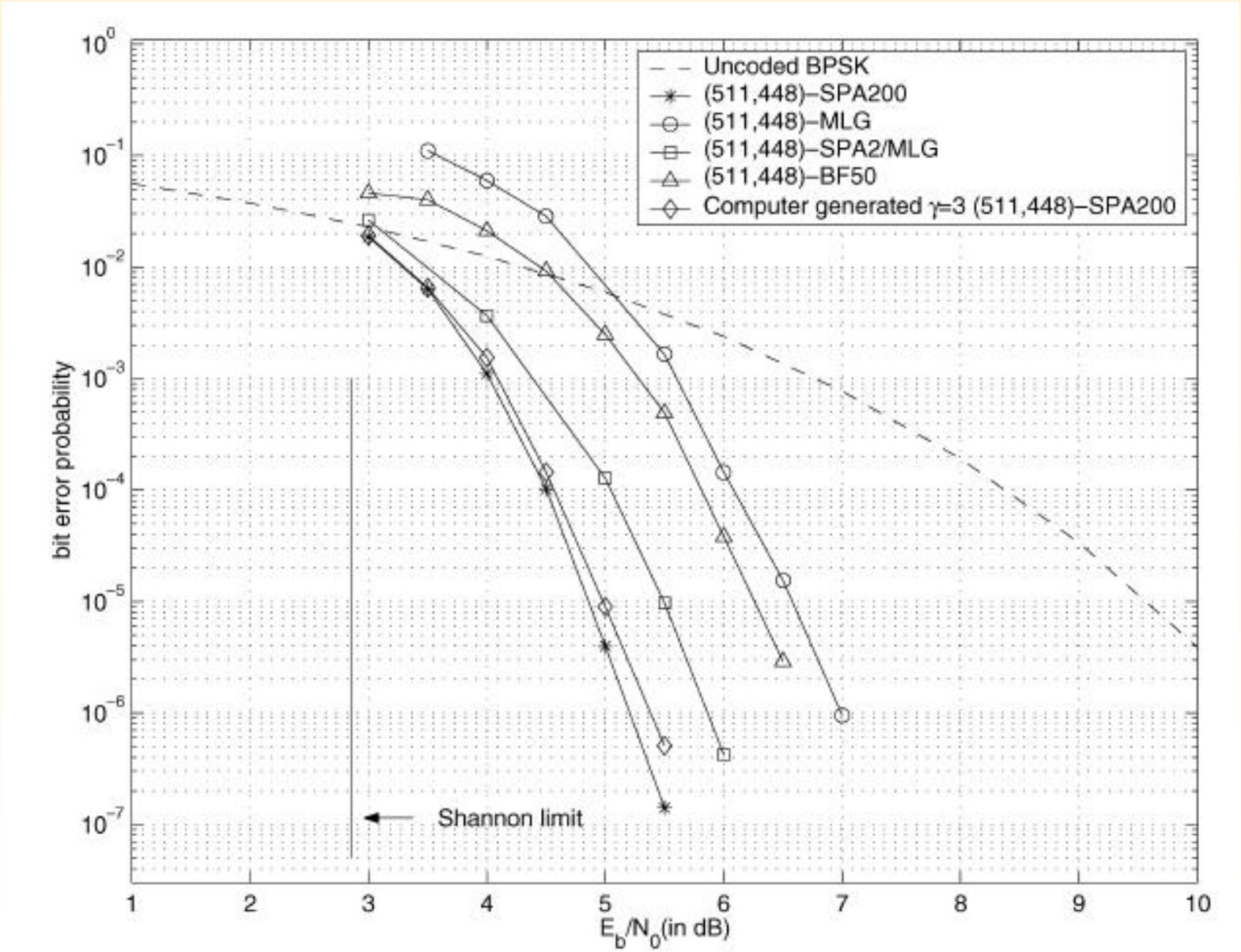
Hyperplanes and general FG codes

- We consider now lines to be bit nodes and planes to be check nodes. Or more generally hyperplanes (flats) of different dimensions.
- Start with the Euclidean geometry $\mathrm{EG}(m, p^s)$. Consider all the flats of dimension μ_1 and μ_2, where $\mu_2 > \mu_1$.
- The incidence vector of a μ_2 flat is an n-tuple with ith component 1 if and only if ith μ_1-flat is contained in it
- The incidence vectors of all μ_2-flats gives the parity check matrix of a $C_{\mathrm{EG}}^{(1)}(m, \mu_2, \mu_1, s, p)$ code
- If $\mu_2 - \mu_1 > 1$, then these codes have many 4-cycles, yet they do not show any error floor.

Cyclic $C_{\mathrm{EG}}^{(1)}(3, 2, 0, 3, 2)$ code $[511, 448]$ has $>$ 3.6 million 4-cycles, yet no error floors for BER around 10^{-6}

Classical Performance in Presence of Many 4 Cycles

Example: $C_{\mathrm{EG}}^{(1)}(3,2,0,3,2) = [511, 448]$



Finally: Quantum LDPC codes

Connection to Generalized Reed-Muller Codes

- We consider the special case $\mu_1 = 0$, *i.e.*, $C^{(1)}_{\mathrm{EG},c}(m, \mu, 0, s, p)$ codes. These are cyclic.
- Recall that the subfield subcode of $C \subseteq \mathbb{F}_{q^s}^n$ is given by $C|_{\mathbb{F}_q} = \{\text{All codewords of } C \text{ such that they are in } \mathbb{F}_q^n\}$.
- It turns out that the dual $C^{(1)}_{\mathrm{EG},c}(m, \mu_2, 0, s, p)^\perp$ is the subfield subcode of a generalized Reed-Muller code.
- Is is possible to embed this generalized Reed-Muller code into a BCH code.

Theorem: Let $C = C^{(1)}_{\mathrm{EG},c}(2, 1, 0, s, 2)$ and $\delta = 2t + 1 \leq 2^s - 1$. Then an $[[2^{2s} - 1, 2^{2s} - 3^s - s(\delta - 1), \delta/2^s + 1]]_2$ exists.

Compare with [Ioffe/Mézard]: they start with BCH code, pick low weight codewords to define sparse parity checks. We start with LDPC code and search for a BCH code containing its dual.

Finally: Quantum LDPC codes

Connection to Generalized Reed-Muller Codes

- We consider the special case $\mu_1 = 0$, *i.e.*, $C^{(1)}_{\mathrm{EG},c}(m, \mu, 0, s, p)$ codes. These are cyclic.
- Recall that the subfield subcode of $C \subseteq \mathbb{F}_{q^s}^n$ is given by $C|_{\mathbb{F}_q} = \{\text{All codewords of } C \text{ such that they are in } \mathbb{F}_q^n\}$.
- It turns out that the dual $C^{(1)}_{\mathrm{EG},c}(m, \mu_2, 0, s, p)^\perp$ is the subfield subcode of a generalized Reed-Muller code.
- Is is possible to embed this generalized Reed-Muller code into a BCH code.

Theorem: Let $C = C^{(1)}_{\mathrm{EG},c}(2, 1, 0, s, 2)$ and $\delta = 2t + 1 \leq 2^s - 1$. Then an $[[2^{2s} - 1, 2^{2s} - 3^s - s(\delta - 1), \delta/2^s + 1]]_2$ exists.

Compare with [Ioffe/Mézard]: they start with BCH code, pick low weight codewords to define sparse parity checks. We start with LDPC code and search for a BCH code containing its dual.

Finally: Quantum LDPC codes

Connection to Generalized Reed-Muller Codes

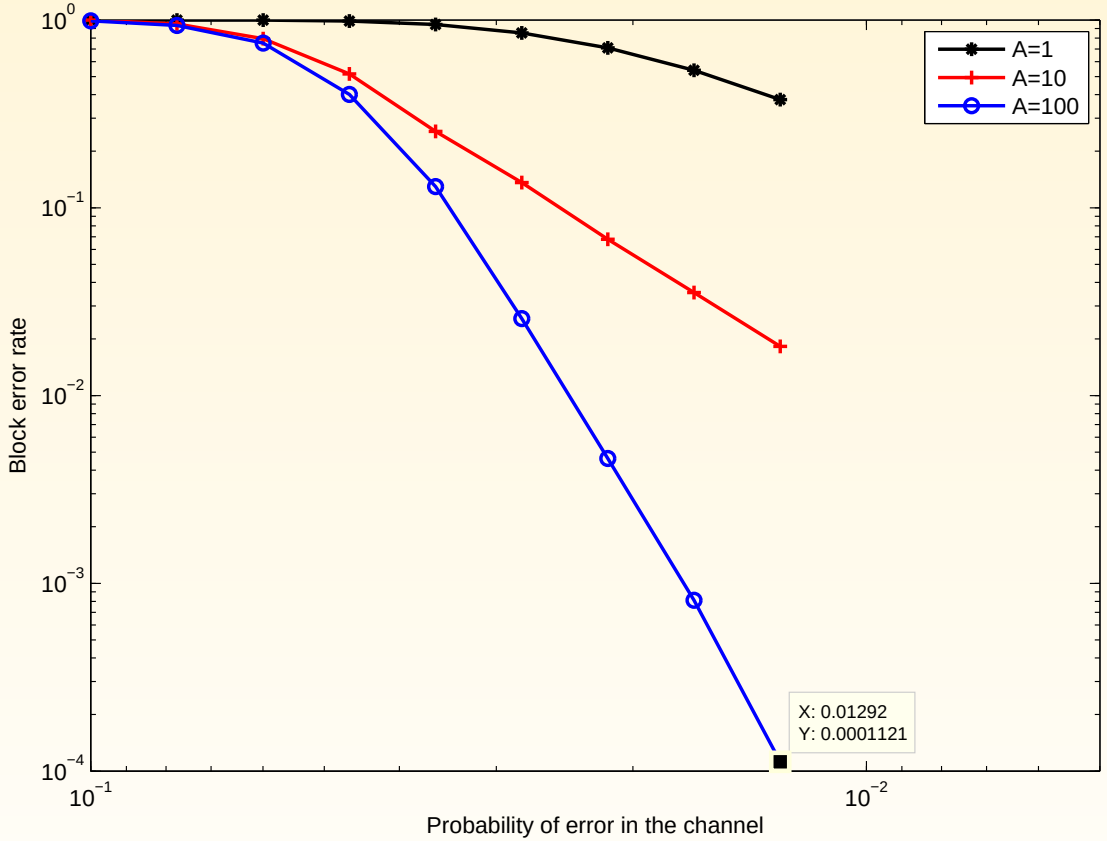
- We consider the special case $\mu_1 = 0$, *i.e.*, $C^{(1)}_{\mathrm{EG},c}(m, \mu, 0, s, p)$ codes. These are cyclic.
- Recall that the subfield subcode of $C \subseteq \mathbb{F}_{q^s}^n$ is given by $C|_{\mathbb{F}_q} = \{\text{All codewords of } C \text{ such that they are in } \mathbb{F}_q^n\}$.
- It turns out that the dual $C^{(1)}_{\mathrm{EG},c}(m, \mu_2, 0, s, p)^\perp$ is the subfield subcode of a generalized Reed-Muller code.
- Is is possible to embed this generalized Reed-Muller code into a BCH code.

Theorem: Let $C = C^{(1)}_{\mathrm{EG},c}(2, 1, 0, s, 2)$ and $\delta = 2t + 1 \leq 2^s - 1$. Then an $[[2^{2s} - 1, 2^{2s} - 3^s - s(\delta - 1), \delta/2^s + 1]]_2$ exists.

Compare with [Ioffe/Mézard]: they start with BCH code, pick low weight codewords to define sparse parity checks. We start with LDPC code and search for a BCH code containing its dual.

Quantum LDPC Codes: Performance

Example: Performance of a $[[255, 159, 5/17]]$ quantum LDPC code for $A = 1, 10, 100$. Maximum no. of iterations set to 50.



- Hard decision bit flipping algorithm [Gallager], [Kou et al]
- Many other ways of message passing: MLG, BF, weighted BF, APP, BP.

Summary

Wrap up:

- Asymmetric error models / biased noise
- Constructions of asymmetric codes from nested codes
- Construction of asymmetric quantum LDPC codes
- Performance simulations

Take home:

- The constructed codes are good for memory
- Achieve higher rate while similar performance
- Achieve better performance while similar rate
- Don’t know yet if they are also useful for FTQC

Comparison With Related Work

- [Rahn, Doherty, Mabuchi, PRA **66**, 032304 (2002)] studied performance of block codes such as [[5,1,3]] or [[7,1,3]] over arbitrary (not necessarily symmetric) Pauli channels.
- [Ioffe, Mézard, PRA **75**, 032345 (2007)] closest to our work regarding methods. Use LDPC codes with irregular degree profiles. Harder to analyze but performance seems ok.
- [Aliferis, Preskill, quant-ph/0710.1301] use concatenation of repetition code with any other code to get asymmetric codes for biased noise. Universal QC possible!
- [Fletcher, Shor, Win, quant-ph/0708.3658] devise adaptive QECC recovery strategies. Can find optimal recovery strategies, works very well for asymmetric channels that arise from amplitude damping channels.
- [Evans, Stephens, Cole, Hollenberg, quant-ph/0709.3875] use symmetric CSS codes with asymmetric error correction strategy, higher frequency of syndrome measurements for the X-only generators.

Comparison With Related Work

- [Rahn, Doherty, Mabuchi, PRA **66**, 032304 (2002)] studied performance of block codes such as [[5,1,3]] or [[7,1,3]] over arbitrary (not necessarily symmetric) Pauli channels.
- [Ioffe, Mézard, PRA **75**, 032345 (2007)] closest to our work regarding methods. Use LDPC codes with irregular degree profiles. Harder to analyze but performance seems ok.
- [Aliferis, Preskill, quant-ph/0710.1301] use concatenation of repetition code with any other code to get asymmetric codes for biased noise. Universal QC possible!
- [Fletcher, Shor, Win, quant-ph/0708.3658] devise adaptive QECC recovery strategies. Can find optimal recovery strategies, works very well for asymmetric channels that arise from amplitude damping channels.
- [Evans, Stephens, Cole, Hollenberg, quant-ph/0709.3875] use symmetric CSS codes with asymmetric error correction strategy, higher frequency of syndrome measurements for the X-only generators.

Comparison With Related Work

- [Rahn, Doherty, Mabuchi, PRA **66**, 032304 (2002)] studied performance of block codes such as [[5,1,3]] or [[7,1,3]] over arbitrary (not necessarily symmetric) Pauli channels.
- [Ioffe, Mézard, PRA **75**, 032345 (2007)] closest to our work regarding methods. Use LDPC codes with irregular degree profiles. Harder to analyze but performance seems ok.
- [Aliferis, Preskill, quant-ph/0710.1301] use concatenation of repetition code with any other code to get asymmetric codes for biased noise. Universal QC possible!
- [Fletcher, Shor, Win, quant-ph/0708.3658] devise adaptive QECC recovery strategies. Can find optimal recovery strategies, works very well for asymmetric channels that arise from amplitude damping channels.
- [Evans, Stephens, Cole, Hollenberg, quant-ph/0709.3875] use symmetric CSS codes with asymmetric error correction strategy, higher frequency of syndrome measurements for the X-only generators.

Comparison With Related Work

- [Rahn, Doherty, Mabuchi, PRA **66**, 032304 (2002)] studied performance of block codes such as [[5,1,3]] or [[7,1,3]] over arbitrary (not necessarily symmetric) Pauli channels.
- [Ioffe, Mézard, PRA **75**, 032345 (2007)] closest to our work regarding methods. Use LDPC codes with irregular degree profiles. Harder to analyze but performance seems ok.
- [Aliferis, Preskill, quant-ph/0710.1301] use concatenation of repetition code with any other code to get asymmetric codes for biased noise. Universal QC possible!
- [Fletcher, Shor, Win, quant-ph/0708.3658] devise adaptive QECC recovery strategies. Can find optimal recovery strategies, works very well for asymmetric channels that arise from amplitude damping channels.
- [Evans, Stephens, Cole, Hollenberg, quant-ph/0709.3875] use symmetric CSS codes with asymmetric error correction strategy, higher frequency of syndrome measurements for the X-only generators.

Comparison With Related Work

- [Rahn, Doherty, Mabuchi, PRA **66**, 032304 (2002)] studied performance of block codes such as [[5,1,3]] or [[7,1,3]] over arbitrary (not necessarily symmetric) Pauli channels.
- [Ioffe, Mézard, PRA **75**, 032345 (2007)] closest to our work regarding methods. Use LDPC codes with irregular degree profiles. Harder to analyze but performance seems ok.
- [Aliferis, Preskill, quant-ph/0710.1301] use concatenation of repetition code with any other code to get asymmetric codes for biased noise. Universal QC possible!
- [Fletcher, Shor, Win, quant-ph/0708.3658] devise adaptive QECC recovery strategies. Can find optimal recovery strategies, works very well for asymmetric channels that arise from amplitude damping channels.
- [Evans, Stephens, Cole, Hollenberg, quant-ph/0709.3875] use symmetric CSS codes with asymmetric error correction strategy, higher frequency of syndrome measurements for the X-only generators.