15 Apr 2026
Ph/CS 219

Circulant matrices and polynomial ring

Shift symmetry: Each row (or column) obtain by shifting previous by one place

$$C = \begin{pmatrix} c_0 & c_2 & c_1 \\ c_1 & c_0 & c_2 \\ c_2 & c_1 & c_0 \end{pmatrix} \qquad C^T = \begin{pmatrix} c_0 & c_1 & c_2 \\ c_2 & c_0 & c_1 \\ c_1 & c_2 & c_0 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad X^T = X^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$C = c_0 X^0 + c_1 X^1 + c_2 X^2 \qquad C^T = c_0 (X^{-1})^0 + c_1 (X^{-1})^1 + c_2 (X^{-1})^2$$

Matrix completely determined by first row or column

$X^a X^b = X^{a+b}$ rule for multiplying shifts or monomials. Commutative!

$n \times n$ matrix $\Rightarrow X^n = 1$

over check matrices have entries $\in \{0, 1\}$

$\Rightarrow$ ring of polynomials $\mathbb{F}_2[x] = \mathbb{F}_2[x, x^{-1}]$ where $x^n = 1$

$\mathbb{F}_2[x]/(x^n - 1)$ Finite ring: We can multiply + add

---

We can also represent action of circulant matrix on vector as multiplication of polynomials. Now x is a "dummy variable" – not a shift

$$v = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \end{pmatrix} = v_0 + v_1 X + v_2 X^2 \Rightarrow Xv = v_2 + v_0 X + v_1 X^2 = \begin{pmatrix} v_2 \\ v_0 \\ v_1 \end{pmatrix}$$

$$X^{-1} v = v_1 + v_2 X + v_0 X^2 = \begin{pmatrix} v_1 \\ v_2 \\ v_0 \end{pmatrix}$$

15 Apr 2026

I can write a parity check matrix with shift symmetry as $H = f(x)$

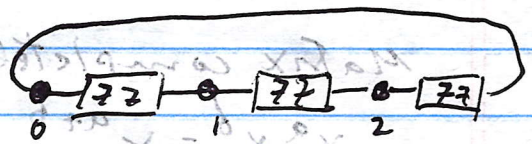
$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots$$

$(c_0, c_1, c_2, \ldots)$ has two interpretations:
A single parity check (vector) or full matrix (obtained by cyclic shifts).

$x^T = x^{-1} \Rightarrow f(x)^T = f(x^{-1})$ Interpreting $f(x)$ as a matrix.

Example: Repetition Code

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



(checks are redundant (only 2 are linearly independent))

If $H = f(x)$ and $v = g(x)$, then $Hv = 0 \iff f(x)g(x) = 0$

$(1+x)(g(x)) = 0$ Solutions are $g(x) = 0 \Rightarrow v = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

$g(x) = 1 + x + x^2 \Rightarrow v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

For CSS codes
X and Z checks commute: $H_X H_Z^T = 0$ the rows of H_X ⊥ to rows of H_Z

$H_Z H_X^T = 0$

~~$(1+x)g(x^{-1}) = 0$~~

~~$\Rightarrow g(x) = (1+x+x^2)$~~

Take a single X and Z check (one row of H_X, H_Z) should be orthogonal when shifted by any amount. $H_X = f(x)$ $H_Z = g(x) \Rightarrow$

$$H_X H_Z^T = f(x) g(x)^T = f(x) g(x^{-1}) = 0$$

15 Apr 2026
Ph/CS 219

$$f(x)\,g(x^{-1}) = \left(\sum_a c_a x^a\right)\left(\sum_b d_b x^{-b}\right) = \sum_c h_c x^c$$

$$h_c = \sum_{a-b=c} c_a d_b = \#\text{ of collisions when shifted by } c$$

We can have more than one cyclic symmetry and more than one qubit register:

Toric code $\quad s(x,y) = \begin{pmatrix} 1+y & 1+x \\ 1+x^{-1} & 1+y^{-1} \end{pmatrix} \begin{matrix} \in H_X \\ \in H_Z \end{matrix}$

(↑ register 1, ↑ register 2)

$L \times M$ toric $\Rightarrow \quad x^L = I = y^M$

Ring is $\quad \mathbb{F}_2[x,y]/(x^L-1,\ y^M-1)$

Register 1 is vertical edges
Register 2 is horizontal edges

Logical operator: Think of X-type Pauli as a vector of 0s and 1s
Commutes with Z type checks. This means the first row of H_Z and all shifts of it annihilate the X-type vector

$$H = f(x) = \sum_a f_a x^a = \begin{pmatrix} f_0 & f_2 & f_1 \\ f_1 & f_0 & f_2 \\ f_2 & f_1 & f_0 \end{pmatrix} \Rightarrow H_{ij} = f_{j-i}$$

$$v(x) = \sum_b v_b x^b$$

$$(Hv)_i = \sum_j H_{ij} v_j = \sum_j f_{j-i} v_j$$

Condition derived earlier

$$h(x^{-1})\,v(x) = 0$$

15 Apr 2026

For rep code: $(1+x^{-1})\,c(x) = 1+x+x^2+\cdots+x^{n}$

$\bar{x} = x \to x$

same for the toric code

2 logical (f, g) where $(1+y^{-1})f + (1+x^{-1})g = 0$

$(0, \sum x^a)$ or $(\sum_a y^a, 0)$

More general $\begin{pmatrix} A(x,y) & B(x,y) \\ B(x,y)^T & A(x,y)^T \end{pmatrix}$ $\leftarrow H_X$, $\leftarrow H_Z$

register 1 ↑ register 2

checks commute $H_X H_Z^T$

$AB + BA = 0$

(circulant polynomials commute - polynomials in x and y)

Bravyi et al 2308.07915

Bivariate bicycle codes

↑ 2 shifts ↖ 2 registers

If A function of x only and B of y only, a hypergraph product

If polynomials have finite order as n grows, a local code

Higher order polynomials → longer distance checks → opportunity to improve $[[n, k, d]]$

Example: Gross code $[[144, 12, 12]]$

cf rotated surface code: $[[144, 1, 12]]$

Lecture 6

15 Apr 2026

PHICS 719

$A(x,y) = x^3 + y + y^2$

$B(x,y) = y^3 + x + x^2$

$x^{12} = 1 = y^6$

Can lay out on torus but with some long connections

Relabel qubits $A' = y^{-1}A = y^{-1}x^3 + 1 + y$

$B' = x^{-1}B = x^{-1}y^3 + 1 + x$

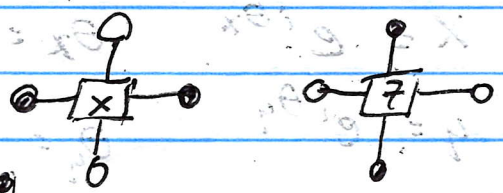
Two registers are 2 12×6 lattices

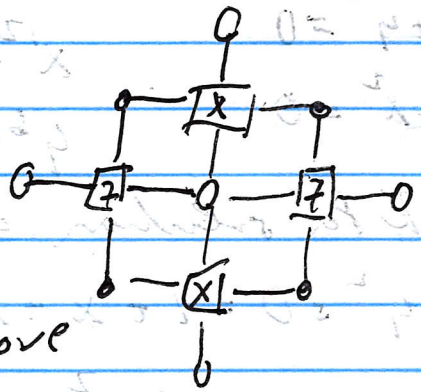
All checks are weight 6

Four Paulis are neighbors of check, as for toric code

Two Paulis are farther from check qubits

Toric





x, y shift each sublattice (colored + uncolored)

uncolored is first register and colored is second

In addition, 2 move qubits in check.

X check includes 1st (uncolored) 3 steps right + 2 down

and 2nd (colored) 3 steps up + 1 left

Z check 1st: 3 down + 1 right

2nd: 3 left + 1 up.

15 Apr 2026

How to determine k = # X logicals
= # Z logicals

We have $n = 144$ qubits, 72 X checks, 72 Z checks
But the checks are not independent

X logicals $\xrightarrow{\text{satisfies checks}}$ $Z_X = \dfrac{\ker(H_Z)}{\text{Im}(H_X^T)}$ $\xrightarrow{\text{in stab.}}$ $k = \dim\ker(H_Z) - \dim(\text{rank } H_X^T)$

Redundancy will increase the kernel + diminish the rank.

Translation invariance means, find solutions to $A = B = 0$ using discrete Fourier transform (use reciprocal lattice)

Now the shifts become phases $x = e^{i\theta_x}$ $\theta_x = \frac{2\pi}{L_x} k$

$y = e^{i\theta_y}$ $\theta_y = \frac{2\pi}{L_y} \ell$

$A = x^3 + y + y^2 = 0$
$B = y^3 + x + x^2 = 0$

$x^{12} - 1 = 0 = (x^3 - 1)^4$ $\quad x^3 = y^3 = 1$
$y^6 - 1 = 0 = (y^3 - 1)^2$

We can look for solutions with $x^3 = 1 = y^3$

$\Rightarrow 1 + y + y^2 = 0 = 1 + x + x^2$

Solutions are ω and ω^2 $\quad \omega = e^{2\pi i/3}$ $\quad \omega = e^{4\pi i/3}$

4 values solve $\quad = -\frac{1}{2} + i\sqrt{3}/2$ $\quad = -\frac{1}{2} - i\sqrt{3}/2$

(ω, ω) (ω, ω^2) (ω^2, ω) (ω^2, ω^2)

But (ω, ω^2) and (ω^2, ω) are doubly degenerate,
so 6 solutions and $k = 12$

Again: 2 registers

A is $r_1 \times n_1$ B is $r_2 \times n_2$

A, B act on distinct registers in H_x and H_z

$$H_x = (A \otimes I_{n_2},\ I_{r_1} \otimes B^T)$$

$$H_z = (I_{n_1} \otimes B^{mT},\ A^T \otimes I_{r_2})$$

Toric code:
A grid of vertical edges
A grid of horizontal edges

# of qubits $n_1 n_2 + r_1 r_2$ (Length of rows in X and Z checks)

How many constraints (# of rows)

$r_1 n_2$ (H_x) and $n_1 r_2$ (H_z)

$$K \geq n_1 n_2 + r_1 r_2 - r_1 n_2 - n_1 r_2$$

$$= (n_1 - r_1)(n_2 - r_1) \sim K_1 K_2$$

Key point is $H_x H_z^T = AB^T + AB^T = 0$

We've arranged # of collisions to always be even

$$d = \min(d_A, d_B, d_{A^T}, d_{B^T})$$

E.g. codeword annihilated by A annihilated by $A \otimes I$, etc

We want codes A, B, A^T, B^T to have high rate and distance

$K_1, d_1 = \Omega(n_1)$ $K_2, d_2 = \Omega(n_2)$ LDPC codes

Rate $\sim \frac{K_1 K_2}{n_1 n_2} = \Omega(1)$ But distance $\sim n_1, n_2 \sim \sqrt{n}$

= "the square root barrier"

15 Apr 2026

Another way to see 2 logicals per solution
$A=B=0 \Rightarrow Af+Bg=0$ for $(f,0)$ and $(0,g)$

Homework: Use inverse F.T. to reconstruct logicals as Pauli's

$d=12 \Rightarrow$ Need to show no nontrivial logical of lower weight

BB code is one way to generalize toric code
Hypergraph product code is another (HGP code)

Toric is HGP of two rep codes
We can take HGP of any two classical linear codes. (Don't need to be shift invariant)
= the "two register" picture

We use a code + its transpose code (distinct from its dual).
C has parity check H and C^T has parity check H^T

Example of rep code $H = 1+x$ and $H^T = 1+x^{-1}$ (same code). Important that H has redundancy

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad H^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$ same checks

But $H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \Rightarrow H^T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$ No solutions