Lecture 5 ①
13 Apr 2026
Ph/CS 219

Codes from circulant matrices

Last time, limitations of local stabilizer codes.
BPT bound $kd^2 = O(n)$ in 2D saturated by Toric.
2D local stab codes have string operators ⟹ constant energy barrier ⟹ not self-correcting.

What about (CSS) codes that are not local?
We now know such codes can be explicitly constructed w. k, d much better than for local codes.

We'll develop some tools:
① Chain complexes, boundary operators, homology
② Polynomial formalism for codes with translation sym. = "quasi-cyclic" ("quasi" because circulant parity check for subblocks).

Rings, Modules, Ideals, Group algebras, Commutative algebra

Examples: Repetition code, Toric code

Rep code = 1D Ising (on a cycle) – PBC.
n checks of which $n-1$ are independent
$Z_1 Z_2, Z_2 Z_3, \cdots, Z_n Z_1$.
E.g. $n=4$ cyclic shift

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

X: $1 \to 2 \to 3 \to 4 \to 1$
X^{-1}: $4 \to 3 \to 2 \to 1 \to 4$
$X^4 = I$

13 Apr 2026

The rep code parity check is $H = 1+X$

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

or think of X as a dummy variable

$1+X$ as a polynomial

$$(1+X)\sum_{a=0}^{n-1} c_a X^a = \sum_a c_a (X^a + X^{a+1}) = \sum_a (c_a + c_{a-1}) X^a$$

Now the $\{X^a\}$ coef in $f(X)$ represent column vectors (length n, $X^n = 1$, $c_a \in \{0,1\}$

Think of X as generator of $\mathbb{Z}_n$

Elements are $\{X^a, a = 0, 1, \dots, n-1\}$

$\sum_a c_a X^a$ & $c_a \in \{0,1\}$ is element of group algebra over $\mathbb{F}_2$

$\mathbb{F}_2[X, X^{-1}]$ is group algebra, $X^n = 1$.

Laurent polynomials in X, X^{-1}

For CSS codes we want to know whether X and Z stab generators commute

X type $f(X) = \sum_a c_a X^a$ $\quad c_a = 1$ where X acts

Z type $g(X) = \sum_b d_b X^b$ $\quad c_a = 1$ where Z acts

$$f(X^{-1}) g(X) = \sum_{a,b} c_a d_b X^{b-a} = \sum_c h_c X^c$$

$$h_c = \sum_{b-a=c} c_a d_b$$

h_c counts # of collisions (mod 2) when shifted by c.

3 Apr 2026
ph/cs 219

Because of cyclic symmetry,

If $f(x)$ is X-type generator, so is $x^b f(x)$

Example — we need all shifted X type to commute with all shifted Z type

Logical X operator of rep code:

$$(1+x) f(x) = 0 \Rightarrow f(x) = (1 + x + x^2 + \cdots x^{n-1})$$

i.e. $\bar{X} = (XX \cdots X)$.

What if $H_X = (1+x)$ and $H_Z = (1+x)$?

Then $f(x^{-1}) g(x) = (1+x^{-1})(1+x) = x + x^{-1}$

E.g. $ZZI - I$
$IXX - I$ when shifted by one place left or right ZZ and XX anticommute.

Toric Code: Now there are 2 cyclic symmetries shift horizontally (x), shift vertically (y)
And there are two registers (I can interpret as horizontal & vertical edges)

Two registers: 2 qubits per unit cell.

unit cell is minimal subgraph that generates a tiling of plane when translated.
(applying $X^a y^b$).

There are LM unit cells and $2LM$ qubits
where $X^L = I = y^M$

13 Apr 2026

First register is vertical edges, 2nd is horizontal

$$H_X = (1+y,\ 1+x)$$

$$H_Z = (1+x^{-1},\ 1+y^{-1}) \Rightarrow H_Z^T = (1+x,\ 1+y)$$

Do they commute? $(1+y)(1+x) + (1+x)(1+y) = 0$ ✓

- this is "bivariate bicycle code" (?)
  Two cycles because two registers
  Bivariate because two shifts: x and y.

Generalize several ways

$$H_X = (A(x,y) \mid B(x,y))$$

$$H_Z = (B^T(x,y) \mid A^T(x,y))$$

$$H_X H_Z^T = AB + BA = 0$$

circulant matrices commute. (because poly mult does!)

A special case: A, B are univariate

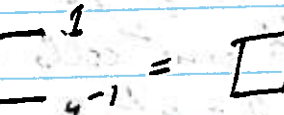
$$H_X = (A(y) \mid B(x))$$

$$H_Z = (B^T(x) \mid A^T(y))$$

These are hypergraph product codes that have cyclic symmetries

Why is this the toric code?

$H_X =$  and  = "star" operator

$H_Z =$  and  = plaquette operator

13 Apr 2026
Ph/CS 219

Logical operators!

Z logical is (f, g) where $(1+y)f + (1+x)g = 0$

Two solutions: $Z_H = (0, \sum_a x^a)$, $Z_V = (\sum_a y^a, 0)$
vertical + horizontal string operators

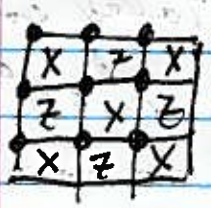
X logical is (f, g) where $(1+x^{-1})f + (1+y^{-1})g$

Two solutions: $X_H = (\sum_a x^a, 0)$ $X_V = (0, \sum y^a)$

Do Z_H and X_V commute? $\sum_{a,b} x^a y^b$

Same for Z_V and X_H
No matter how we shift them relative to one another, they still anticommute!

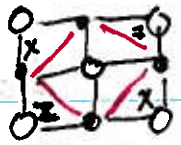
An example with one register:
The rotated surface code. (Checkerboard)



Qubits on sites, X, Z checks on plaquettes
$H_X = H_Z = 1 + x + y + xy = (1+x)(1+y)$

Both $\sum x^a$ and $\sum y^a$ are logical (annihilated by $1+x$, $1+y$ respectively)

But Do Z and X checks commute
$(1+x^{-1})(1+x)(1+y^{-1})(1+y) = (x+x^{-1})(y+y^{-1})$
Don't commute when rotated both V and H

Actually the unit cell is  

have one two plaquettes per unit cell

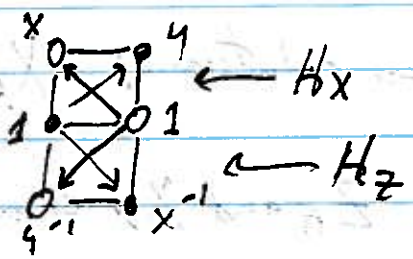
The two registers are two checkerboards of vertices

x and y are primitive lattice translations

- $H_X = (1+y)(1+x)$ 

$H_Z = (1+x^{-1})(1+y^{-1})$



The codes have same polynomial presentation, yet $n = d^2$ for rotated and $n = 2d^2$ for unrotated.

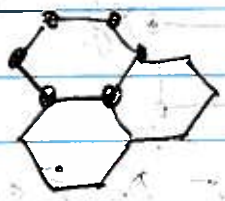
Unrotated: 2 $d \times d$ registers, hence $n = 2d^2$

Rotated: Now there are $d^2/2$ unit cells and two qubits per cell $\Rightarrow$ $n = d^2$.

Another way to say this: For rotated code, x and y are 45° rotated. We have $x^d = y^d = 1$

Unit cell has area = 2 vs area = 1 for unrotated, yet area of torus is the same.

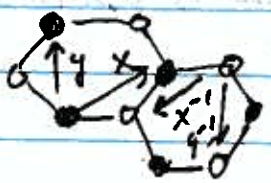
Color code on a honeycomb



The checks are $X^{\hexagon}$ and $Z^{\hexagon}$ on each hexagon. We can formulate using either 2 or 3 registers

13 Apr 2026
Ph/CS 719

Two coloring of vertices ⇒ two registers



$H_X = H_Z = (1 + x + y,\ 1 + x^{-1} + y^{-1})$

check commutation

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

Can map to 2 copies of toric code on 4 registers (homework)

So far codes are local. Only small powers of x and y. Allowing longer powers can make codes more efficient

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

– cf 12×12 toric $[[144, 2, 12]]$
(or just $K = 1$ for surface code)

$H_X = (A \mid B)$ Now $A(x,y) = x^3 + y + y^2$

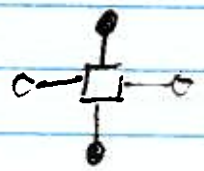
$H_Z = (B^T \mid A^T)$ $B(x,y) = y^3 + x + x^2$

Recall $A' = y^{-1} A = y^{-2} x^3 + 1 + y$

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

$x^{12} = 1 = y^6$ ⇒ Two registers, each w/ 72 qubits

check has weight 6



4 neighbors as in toric code

And two longer connections

Either 3 steps hor and 1 vertical,
or 3 steps vert and 1 horizontal.

13 Apr 2026

Aside: Circulant matrices and polynomials.
Circulant means all columns obtained from the first by cyclic permutations

$$C = \begin{pmatrix} c_0 & c_{n-1} & & \\ c_1 & c_0 & \ddots & \\ c_2 & c_1 & \ddots & c_{n-1} \\ \vdots & & \ddots & c_0 \\ c_{n-1} & & & \end{pmatrix} = c_0 I + c_1 X + c_2 X^2 + \cdots + c_{n-1} X^{n-1}$$

Or -- for transpose

$$C^T = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_n & c_0 & c_1 & c_2 & \cdots \\ c_{n-1} & c_n & c_0 & c_1 & \cdots \end{pmatrix} = \sum_a c_a (X^{-1})^a$$

C^T

Hence $C \cdot D = \left(\sum_a c_a X^a\right)\left(\sum_b d_b X^b\right)$ = Products of polynomials

Polynomials live in ring $\mathbb{F}_2[X]/(X^n - 1)$

We consider $\mathbb{F}_2[x,y]/(X^L - 1, y^M - 1)$

- its parity check is invariant under 2 independent shift symmetries.

Again the matrices can be expanded in powers $\{X^a y^b\}$ and matrix multiplication is same as polynomial multiplications.