Admin: Final exam is Thursday, Dec. 12, 2-4pm
You are allowed to use one page of notes.
Course evaluations are online.
Section today going over review problems.
Office hours

Topics since the midterm

- Singular-value decomposition
- Spectral decomposition
- Least squares: $\min \| Ax - b \|$
  - either using normal equations
  - or the pseudoinverse
- Special matrices
  - Diagonalizable
  - Normal
  - Unitary, orthogonal (and isometries)
  - Symmetric, Hermitian
  - Positive semi-definite, positive definite
  - Stochastic
- Applications:
  - Solving recurrences and differential equations
  - Linear regression
  - Principal component analysis ← low-rank approx. of matrices
  - PageRank ← Markov chains
  - Quantum physics ← unitary & Hermitian matrices
  - Spectral graph analysis ← tensor products, commuting matrices

• Condition number,
  - stability of linear systems of equations
• Power method for finding eigenvectors
  - Spectral gap
LET'S PLAY A GAME!
Tell me which vertices to click.
Goal: Color the graph red.

Formalizing the game:
Observe: 1. Clicking a vertex twice cancels it out.
2. The order in which you click the vertices doesn't matter.
⇒ All that matters is the subset of vertices you click.
⇒ Problem: Is there a subset of vertices to click that will make everything red?
will make everything red?

Solve

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
0 \\
0 \\
0 \\
0 \\
0 \\
0
\end{pmatrix}
\mod 2
\]

for \(x_i \in \{0, 1\}\)

How? Use Gaussian elimination (mod 2)!

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 1 to row 9

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 9 to rows 2, 4, 5, 6, 7

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 5 to rows 2, 3, 4

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 4 to rows 2, 7

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 7 to rows 2, 3, 4, 5, 6

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 3 to rows 2, 4, 5, 6, 7

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 3 & 4 & 5 & 6 & 7 & 1 \\
3 & 4 & 5 & 6 & 7 & 1 & 2 \\
4 & 5 & 6 & 7 & 1 & 2 & 3 \\
5 & 6 & 7 & 1 & 2 & 3 & 4 \\
6 & 7 & 1 & 2 & 3 & 4 & 5 \\
7 & 1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{pmatrix}
\]

add row 2 to row 3 \(\Rightarrow x_6 = 0\)

add row 3 to rows 4, 5, 6, 7
Done! \( \bar{x} = (1, 1, 1, 0, 0, 0, 0, 0, 0) \) works!

Conclusion: As well as real and complex numbers, \( \mathbb{R} \) and \( \mathbb{C} \), linear algebra works over the integers mod 2.

**Concept:**

- Vector space  
- Subspace  
- Linear independence, bases  
- Gaussian elimination  

Works over finite fields? 

<table>
<thead>
<tr>
<th>Concept</th>
<th>Works over finite fields?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vector space</td>
<td>✓</td>
</tr>
<tr>
<td>Subspace</td>
<td>✓</td>
</tr>
<tr>
<td>Linear independence, bases</td>
<td>✓</td>
</tr>
<tr>
<td>Gaussian elimination</td>
<td>✓</td>
</tr>
</tbody>
</table>


Gaussian elimination
LU decomposition
Orthogonality
Rank-Nullity Theorem
Angles
Norms
Isometries, unitaries,...
Singular-value decomposition
Spectral decomposition

In general, a field supports addition and subtraction, multiplication and division (except for division by 0), and multiplication's inverse operation.

Examples:
\( \mathbb{R}, \mathbb{C}, \mathbb{Z}/3, \mathbb{Z}/1, \mathbb{Z}/2^3 \)

How to divide by 2?
It should be the inverse of multiplying by 2

\[
\text{Observe: } x \cdot 2 \cdot 2 = x \cdot 4 = x \mod 3
\]

\[
\Rightarrow 2'' = 2
\]

\( \mathbb{Z}/2, \mathbb{Z}/2^3 \)
No! For no \( x \) is \( 2x = 1 \mod 4 \)

\[
\Rightarrow 2'' \text{ does not exist } \mod 4
\]

(Alternatively, \( 1 \cdot 2 = 2 \mod 4 \)
\( 3 \cdot 2 = 2 \mod 4 \)
So multiplication by 2 cannot be undone/inverted)

Fact: *For any prime \( p \), the integers \( \mod p \) form a field.*

*For any prime \( p \) and \( k=1,2,3,... \), there is a field of size \( p^k \).

(But for \( k \geq 2 \), the field is not the integers \( \mod p^k \))
• These are the only finite fields.

For today: Let's focus on the field \( \mathbb{F}_2 \). Subspaces of \( \mathbb{F}_2 \)

**Examples:**

1. \( \{ (0, 0, 0, 0), (1, 1, ..., 1) \} \)
   - closed under addition?
   - closed under multiplication by 0 and 1?

2. \( \text{Span}\left\{ \begin{pmatrix} 0, 0, 0, 1 \\ 1, 1, 0, 0 \end{pmatrix}, \begin{pmatrix} 1, 0, 1, 1 \\ 1, 0, 1, 1 \end{pmatrix} \right\} \)

**Claim:** This is a four-dimensional subspace, i.e., the four vectors in the spanning set are linearly independent.

**Proof:** \( \begin{pmatrix} 0, 0, 0, 1 \\ 1, 1, 0, 0 \\ 1, 0, 0, 1 \\ 1, 0, 1, 0 \end{pmatrix} \) are linearly indep. because each has a 1 in a position that the other two can't cancel out.

The last vector, \( \begin{pmatrix} 1, 1, 1, 1, 1 \\ 1, 1, 1, 1, 1 \end{pmatrix} \), is linearly indep. of the first three, because it has a 1 in all 3 of the positions marked above, so it could only equal the sum of the first 3, and it isn't.

Alternatively, it has odd weight, while any combination of the first 3 vectors has an even number of 1s.

Alternatively, we want to show that this matrix has a trivial nullspace: (so there are no linear dependencies between its columns, and its rank is 4)

\[
G = \begin{pmatrix}
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1
\end{pmatrix}
\]

Solving \( G \begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = 0 \) \( \Rightarrow x_3 + x_4 = 0 \) \( \Rightarrow x_3 = x_4 \)
$$\begin{pmatrix}
1 & 0 & 0 \\
1 & 0 & 1 \\
1 & 1 & 0
\end{pmatrix}$$

Solving \( G(x_4) \) →
\( x_3 + x_4 = 0 \) \( \Rightarrow x_3 = x_4 \)
\( x_2 + x_4 = 0 \) \( \Rightarrow x_2 = x_4 \)
\( x_1 + x_4 = 0 \) \( \Rightarrow x_1 = x_4 \)

and (1) doesn’t work. \( \checkmark \)

**Problem:** How big is a \( k \)-dimensional subspace of \( \mathbb{F}_{13}^n \)?

**Answer:**

The answer “has to” be \( 2^k \), since \( |\mathbb{F}_{13}^k| = 2^k \).

To prove it, let \( v_1, v_2, \ldots, v_k \) be a basis for the subspace, and start listing elements:

\[
\begin{align*}
0 &= 0^n \\
v_1 \\
v_2 \\
v_3 \\
v_1 + v_2 \\
v_1 + v_3 \\
v_1 + v_2 + v_3 \\
\vdots
\end{align*}
\]

these are all different!

again, all different, or there would be a linear dependency

... \( \checkmark \)

**Problem:** How many \( k \)-dimensional subspaces of \( \mathbb{F}_{13}^n \) are there?

**Answer:**

\[
\begin{align*}
\# \text{k-dim subspaces of } \mathbb{F}_{13}^n &= \frac{\# \text{ways to pick } k \text{ linearly independent vectors from } \mathbb{F}_{13}^n}{\# \text{ways to pick } k \text{ linearly independent vectors from } \mathbb{F}_{13}^k} \\
\# \text{ways to pick } k \text{ basis vectors from } \mathbb{F}_{13}^n &= (2^n - 1) \times (2^n - 2) \times (2^n - 4) \times \cdots \\
&\quad \uparrow \\
&\quad v_1 \neq 0^n \\
&\quad v_2 \notin \{0, v_1\} \\
&\quad v_3 \notin \text{Span}\{v_1, v_2\} \\
&\quad \vdots \\
&\quad v_k \notin \text{Span}\{v_1, v_2, \ldots, v_{k-1}\} \\
\Rightarrow \# \text{k-dim subspaces of } \mathbb{F}_{13}^n &= \frac{(2^n - 2^k)}{\prod_{i=0}^{k-1} (2^n - 2^i)}
\end{align*}
\]
Linear error-correcting codes

Definition: The Hamming distance between \( x \) and \( y \) in \( \{0,1\}^n \) is the number of coordinates in which they differ.

The Hamming weight of \( x \in \{0,1\}^n \) is \( \|x\| = \) the number of nonzero coordinates.

Thus
\[
d_H(x, y) = |x + y|
\]
since \( x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \)
\[
\begin{align*}
0 & \text{ if } x_i = y_i, & \ldots \\
1 & \text{ if } x_i \neq y_i
\end{align*}
\]

Definition: A binary, error-correcting code is a subset of \( \{0,1\}^n \).

The code's distance is the minimum Hamming distance between any two distinct elements.

Example: \( C = \{(0,0,\ldots,0), (1,1,\ldots,1)\} \subseteq \{0,1\}^n \) has distance \( n \).

Definition: A binary, error-correcting, linear code is a subspace of \( \{0,1\}^n \).

Notation: \([n, k, d]\) code
\[
\begin{align*}
\text{n bits} & \quad \text{dim-k subspace} \\
\text{distance} d & \quad 2^k \text{ codewords} \\
& \quad k \text{ encoded bits}
\end{align*}
\]

Example: 7-bit Hamming code
To encode 4 bits into 7, multiply by
\[
\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}
\]
To encode, each \( x \) is multiplied by

\[
G = \begin{pmatrix}
\varepsilon_x & \varepsilon_1 & \cdots & \varepsilon_n \\
1 & x_1 & \cdots & x_n \\
\varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_n
\end{pmatrix}
\]

\[
G(x) = x_1 \varepsilon_1 + x_2 \varepsilon_2 + \cdots + x_n \varepsilon_n \\
\in \text{Span}\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n\}
\]

**Claim:** For a linear code, the code's distance is \( \min_{x \in \text{code}} |x| \)

**Proof:** code distance is \( \min_{x, y \in \text{code}} d_M(x, y) \)

\[
|\begin{pmatrix} x \\ y \end{pmatrix}| \\
|\begin{pmatrix} x + y \end{pmatrix}|
\]

But the code is linear, so \( x + y \) is in the code, too \( \square \)

**Code duality**

For any subspace \( V \),

\[
V^\perp = \{ w | w \perp v \text{ for all } v \in V \}
\]

is another subspace.

(And \( (V^\perp)^\perp = V \))

For a code \( C \) with generator matrix \( G_{n \times k} \),

\[
C = R(G), \quad N(G) = \text{span}\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k\}
\]

so columns are linearly independent

\[ C^\perp = N(G^\perp) \text{ has dimension } n-k \text{ (by rank-nullity).} \]

**Example:** \( n \)-bit repetition code

\[
G = \begin{pmatrix}
1 \\
1 \\
\vdots \\
1
\end{pmatrix}_{n \times 1}
\]

\[ N(G^\perp) \text{ has dimension } n-1, \]

generated by

\[
P = \begin{pmatrix}
1 & 1 & 0 & 0 & \cdots & 0 \\
1 & 0 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & 0 & 0 & & 1
\end{pmatrix}
\]

Rows of \( P \perp \) columns of \( G \)
Example: 7-bit Hamming code

\[
\begin{array}{ccccccc}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 \\
\end{array}
\]

Claim: This code has distance $\geq 3$ (it is a $[7,1,3]$ code)

Proof:

1. The distance is $\geq 3$:
   - Why?
   - Let $x \in \mathbb{R}(G)$ be a codeword.
   - $Px = 0$
   - $\Rightarrow P(x+y) = Py$ for any error $y \in \{0,1\}^n$

   Observe: If $|y| \leq 1$, then it is uniquely identified by $Py$.

   Since $P0 = 0$ and $P1 = 1$ in binary!

   $\Rightarrow$ Given $y$, promised to be within distance 1 of some codeword, you can recover the codeword by flipping the $(Pz)'th$ bit.

   $\Rightarrow$ Any pair of codewords must be $\geq 3$ apart.

2. The distance is $\leq 3$:
   - Why?

If the distance is $\geq 3$, then the balls of
If the distance is \(3\), then the balls of Hamming radius \(1\) around the codewords must all be disjoint.

This accounts for \(2^k \cdot (1 + \binom{k}{1}) = 16 \cdot 8 = 2^7\)

points in \(0, 1^7\) \(\Rightarrow\) no room for any more! \(\square\)

Remark: This argument holds for any linear code, and is known as the “Hamming Bound.”

The \([7, 1, 3]\) Hamming code is called “perfect” because the Hamming balls fill \(0, 1^7\) completely, with no gaps between them.