Welcome! Everything is fine.

When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 7.1–7.2; for Mon: 7.3–7.4.
- PS07 due Wed Mar 25.
- Exam 2 delayed until ??

Deadline for Outline PS07 to Thy

Last time

Hamming distance $d(\mathbf{x}, \mathbf{y})$ satisfies triangle inequality:

10010011=x
10101101=y dist 5

Triangle ineq: No shortcut by adding dest

$$d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$$

The **nearest neighbor** error-correction method in $\mathcal{C}$ is:

- (Unique nearest codeword) If there is a unique $\mathbf{y}' \in \mathcal{C}$ such that $d(\mathbf{y}, \mathbf{y}')$ is minimal, we correct $\mathbf{y}$ to $\mathbf{y}'$. (Unique nearest neighbor.)

  Need: list of all poss rec'd vectors y and their nearest nbrs
- (Multiple nearest codewords) If there is more than one vector $\mathbf{y}' \in \mathcal{C}$ such that $d(\mathbf{y}, \mathbf{y}') > 0$ is minimized, we state that $\mathbf{y}$ has been detected as an erroneous transmission, but cannot be corrected.

Justification for nearest neighbor: Correction involving fewest number of changes is most likely intended message, since more likely to have fewer errors occurs.

Min weight and error correction

Idea: error-correction comes from large min distance

Theorem

Let $\mathcal{C}$ be a binary linear code with minimum distance d. Then the nearest neighbor method, applied to $\mathcal{C}$, corrects $\lfloor (d-1)/2 \rfloor$ errors and detects $\lfloor d/2 \rfloor$ errors.

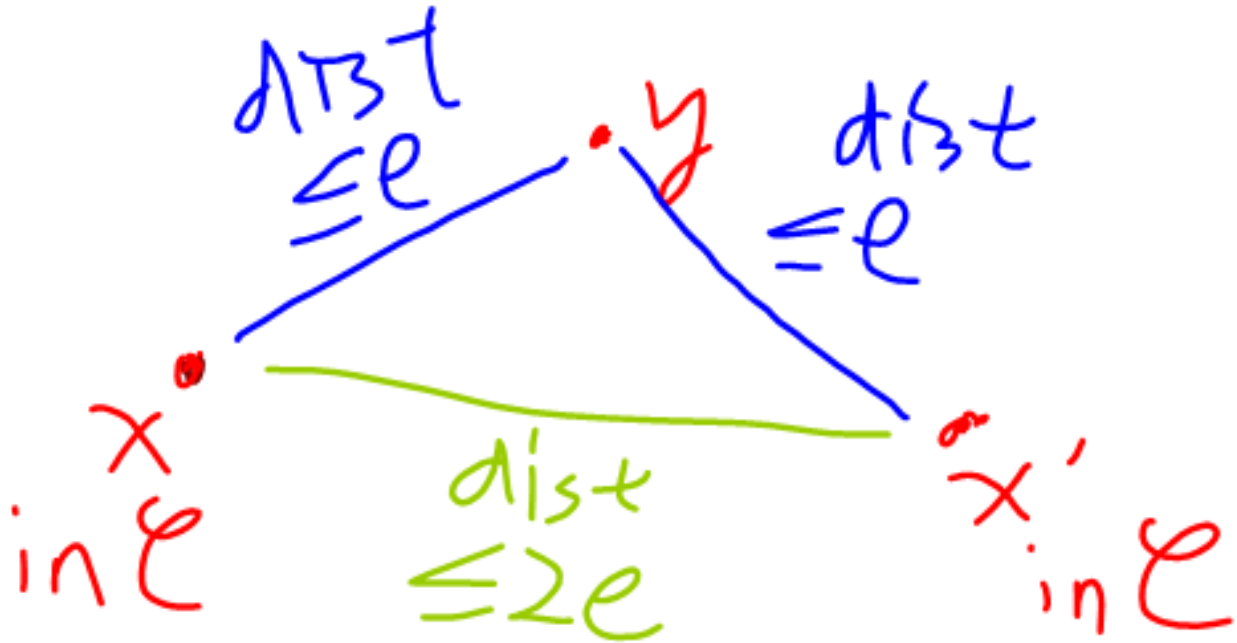
floor means "round down"

Proof:

To say that we can correct up to floor((d-1)/2) errors means that we can correct up to e errors, using nearest neighbor, as long as 2e+1<=d.

So suppose min distance (fewest # of 1s in nonzero vector) is d, and 2e+1 <= d.

If there's some way to find e errors in a transmitted codeword x, that would mean that there's there a possible received message y and two codewords x, x', each of which have distance <= e from y.



So if we had some uncorrectable received vector y, then we would have two codewords x, x' such that d(x,x') <= 2e.
In that case, d(x-x',0) <= 2e, which would mean that there is a nonzero codeword x-x' at distance <= 2e from 0.
But min distance is at least 2e + 1; contradiction.

So it must be the case that each received vector y has at most one neighbor within distance e, so nearest neighbor corrects up to e errors.

Hamming dist bet x and y
is length of shortest path
in Hamming cube bet x and y

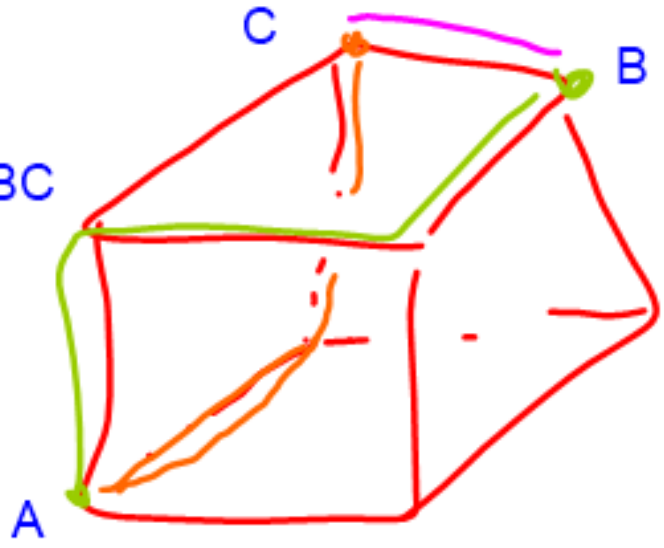
F_2^3, F_2^n is n-cube

Can we think of the triangle in triangle ineq as one face of the cube?

Ans: Any "realistic" picture of a triangle in Hamming cube won't look much like a triangle:

Triangle ABC:

sides of ABC



Hamming 3-cube

Better to have an abstract picture:

Ch. 7: Ideals

And now for something completely different:

(An abstract idea that will lead to most $ concept: finite fields)

Definition R = integers Z or polynomials F[x]; important: F = F_p

Let R be a ring. An **ideal** of R is a subset I of R satisfying the following three axioms:

1. (Zero) The zero element of R is contained in I.
2. (Closed under addition) If $x, y \in I$, then $x + y \in I$.
3. (Closed under R-multiplication) If $x \in I$ and $r \in R$, then $rx \in I$.

Example: Multiples of 3

Prove that/explain why I is an ideal of Z:

Let $I = \{n \in \mathbf{Z} \mid n = 3k \text{ for some } k \in \mathbf{Z}\}$. = {...,-6,-3,0,3,6,9,12,15...}

(Zero)

0=3(0), so 0 is an element of I

(Closed $+$) A. x,y in I. So x=3k, y=3m for some k, m in Z.

Therefore x+y = 3k+3m = 3(k+m).

So x+y = 3 (some integer). Therefore: C. x+y in I

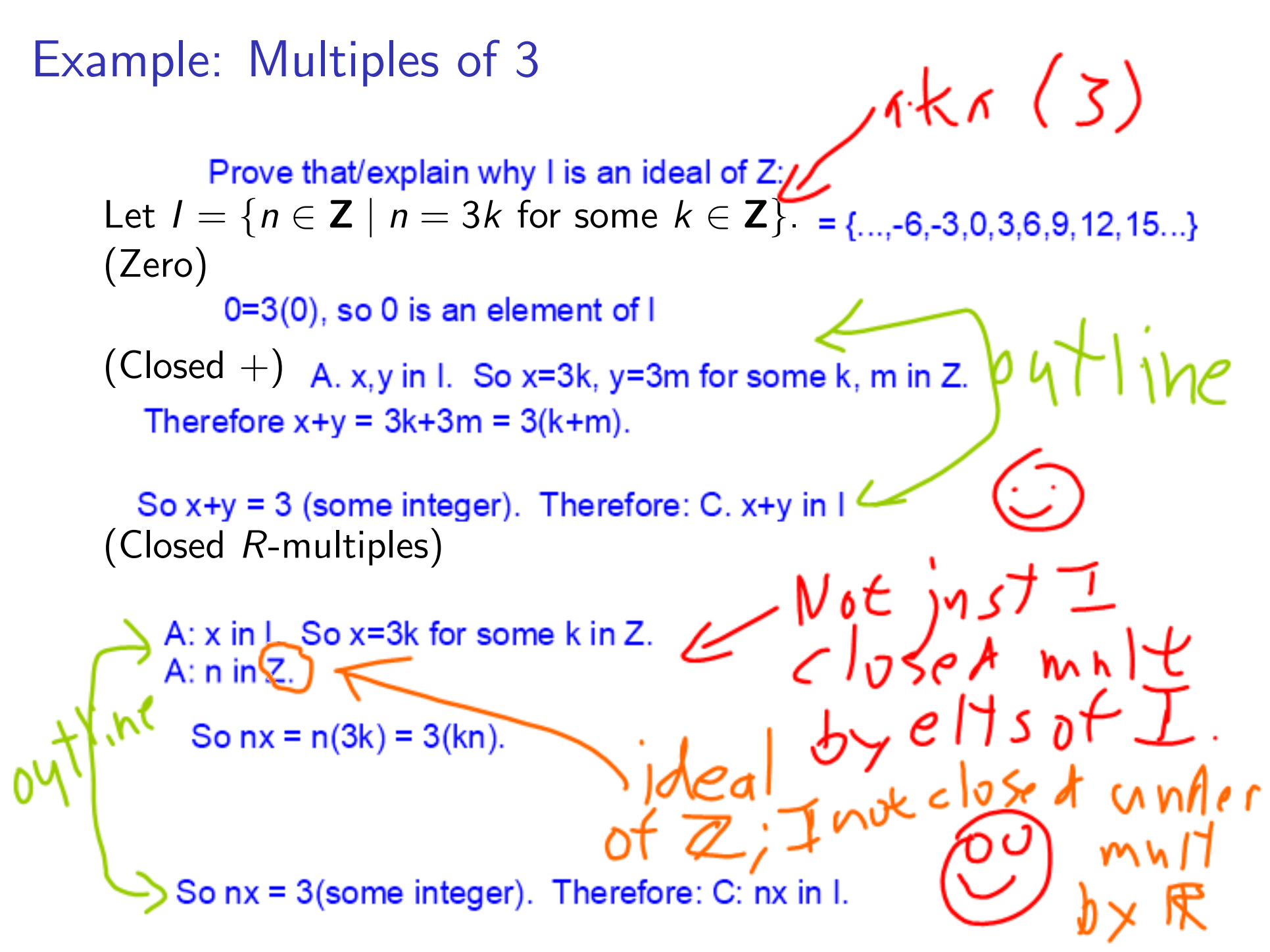
(Closed R-multiples)

A: x in I. So x=3k for some k in Z.

A: n in Z.

So nx = n(3k) = 3(kn).

So nx = 3(some integer). Therefore: C: nx in I.



Example: Multiples of $f(x)$ in $F[x]$

F field

$f(x) \in F[x]$ fixed. F[x]

Let $I = \{a(x)f(x) \in F \mid a(x) \in F[x]\}$. all polynomial multiples of f(x).

WTS: I is an ideal of F[x].

(Zero)

0 = 0 * f(x), so 0 in I.

(Closed $+$) Suppose g(x), h(x) in I. Then g(x)=a(x)f(x), h(x)=b(x)f(x), a,b in F[x].

So g(x)+h(x)=a(x)f(x)+b(x)f(x) = (a(x)+b(x))f(x).
Therefore g+h is a polynomial times f(x). C: g(x)+h(x) in I.

I ideal of F[x]

(Closed R-multiples)

Suppose g(x) in I and c(x) in F[x]. Then by defn of I, g(x)=a(x)f(x) for a in F[x].
Therefore
c(x)g(x) = c(x)a(x)f(x) = (c(x)a(x))f(x).
So c(x)g(x) is a polynomial times f(x). C: c(x)g(x) in I.

Principal ideals and ideals generated by two elements

Same proof works for:

Definition

For a ring R and a fixed $a \in R$, the set

$$(a) = \{ra \mid r \in R\} \tag{1}$$

all R-multiples of a

is called the **principal ideal generated by** a.

Similarly:

Definition

For a ring R and fixed $a, b \in R$, the set

$$(a, b) = \{ra + sb \mid r, s \in R\} \tag{2}$$

all R-linear combinations of a, b; very similar to span

is called the **ideal generated by** a **and** b.

HW: Prove that (a,b) is in fact an ideal of R.

Substitution kernel

For F a field and $a \in F$, the set

$$I_a = \{f(x) \in F[x] \mid f(a) = 0\} \tag{3}$$

is an ideal of $F[x]$ (HW).
Proof uses the fact that:

- The value that you get when you plug a into $f(x) + g(x)$ is $f(a) + g(a)$; and
- The value that you get when you plug a into $f(x)g(x)$ is $f(a)g(a)$.

Quotient rings

Remember early on we didn't quite define Z/(m)?

We can finally actually define $\mathbf{Z}/(m)$!
That is, given an ideal I of ring R, goal is define *quotient ring* R/I.

Definition

Let R be a ring, and let I be an ideal of R. For $r \in R$, we define the **additive coset** $r + I$ to be

$$r + I = \{r + a \mid a \in I\}. \tag{4}$$

If the context is clear, instead of saying "additive coset", we just say **coset**.

Example: $I = (3)$ ={...-9,-6,-3,0,3,6,9,....}

5 $+(3) =$ {...,-4,-1,2,5,8,11,14,....}

On Mon: We'll look at more examples of r + I, for I=(3) in Z.

Q: What is meant by "write down all codewords in H_7"?

A: H_7 is a subspace of F_2^7; specifically, it's the nullspace of a certain matrix. We know how to find a basis for that subspace (Ch. 5); the problem asks you to write out every vector in the subspace.
(Set of all vectors in a subspace = set of all linear combinations of basis.)

(Prob. 6.3.2)

Coset conditions

Theorem

Let R be a ring, let I be an ideal of R, and let $r, s \in R$. Then the following are equivalent (one statement holds if and only the other holds):

1. $r + I = s + I$ *(i.e., the cosets $r + I$ and $s + I$ are the same set).*
2. $r \in s + I$.
3. $r - s \in I$.
4. $r = s + a$ *for some* $a \in I$.

Proof of (1) implies (2):

Coset representatives

Theorem

Let R be a ring, let I be an ideal of R, and let $r, s \in R$. Then the following are equivalent (one statement holds if and only the other holds):

1. $r + I = s + I$ *(i.e., the cosets $r + I$ and $s + I$ are the same set).*
2. $r \in s + I$.
3. $r - s \in I$.
4. $r = s + a$ *for some* $a \in I$.

Definition

Let R be a ring, let I be an ideal of R, and let $r, s \in R$. To say that r is a **representative of the coset** $s + I$ means that $r \in s + I$. Note that any element of a coset can represent it, because r and s are contained in given coset if and only if $r + I = s + I$.

Definition of R/I

Idea: R/I is R setting $I = 0$.

Definition

Let R be a ring and let I be an ideal of R. We define the **quotient ring** R/I as follows.

- **Set:** The elements of R/I are the cosets of I in R.
- **Addition:** For $r + I, s + I \in R/I$, we define

$$(r + I) + (s + I) = (r + s) + I. \tag{5}$$

- **Multiplication:** For $r + I, s + I \in R/I$, we define

$$(r + I)(s + I) = rs + I. \tag{6}$$

The zero element of R/I is $0 + I = I$, and the one element is $1 + I$.

Example: $\mathbf{Z}/(3)$

Elements:

Multiplication table:

R/I is a ring

Elements of R/I are cosets of I in R, and define

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I)(s + I) = rs + I$$

Theorem

It works!

What could go wrong?