Discovery learning in an interdisciplinary course on finite fields and applications

Christopher O'Neill

San Diego State University

cdoneill@sdsu.edu

Taught with Lily Silverstein

August 4, 2018

UC Davis, Math 148: “Discrete Math”

Topics: finite fields, block designs, error-correcting codes

UC Davis, Math 148: “Discrete Math”

Topics: finite fields, block designs, error-correcting codes

Students: 45% Math, 40% CS, 15% other
highly varied math backgrounds

UC Davis, Math 148: “Discrete Math”

Topics: finite fields, block designs, error-correcting codes

Students: 45% Math, 40% CS, 15% other
highly varied math backgrounds

Course structure: half lecture days
half discovery learning (“discussion”) days

Overview of block designs

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	6	11	16	21
2	7	12	17	22
3	8	13	18	23
4	9	14	19	24
5	10	15	20	25

1	7	13	19	25
2	8	14	20	21
3	9	15	16	22
4	10	11	17	23
5	6	12	18	24

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

1	9	12	20	23
2	10	13	16	24
3	6	14	17	25
4	7	15	18	21
5	8	11	19	22

1	10	14	18	22
2	6	15	19	23
3	7	11	20	24
4	8	12	16	25
5	9	13	17	21

Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5	1	6	11	16	21	1	7	13	19	25
6	7	8	9	10	2	7	12	17	22	2	8	14	20	21
11	12	13	14	15	3	8	13	18	23	3	9	15	16	22
16	17	18	19	20	4	9	14	19	24	4	10	11	17	23
21	22	23	24	25	5	10	15	20	25	5	6	12	18	24

1	8	15	17	24	1	9	12	20	23	1	10	14	18	22
2	9	11	18	25	2	10	13	16	24	2	6	15	19	23
3	10	12	19	21	3	6	14	17	25	3	7	11	20	24
4	6	13	20	22	4	7	15	18	21	4	8	12	16	25
5	7	14	16	23	5	8	11	19	22	5	9	13	17	21

Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5	1	6	11	16	21	1	7	13	19	25
6	7	8	9	10	2	7	12	17	22	2	8	14	20	21
11	12	13	14	15	3	8	13	18	23	3	9	15	16	22
16	17	18	19	20	4	9	14	19	24	4	10	11	17	23
21	22	23	24	25	5	10	15	20	25	5	6	12	18	24

1	8	15	17	24	1	9	12	20	23	1	10	14	18	22
2	9	11	18	25	2	10	13	16	24	2	6	15	19	23
3	10	12	19	21	3	6	14	17	25	3	7	11	20	24
4	6	13	20	22	4	7	15	18	21	4	8	12	16	25
5	7	14	16	23	5	8	11	19	22	5	9	13	17	21

No wasted space!

Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

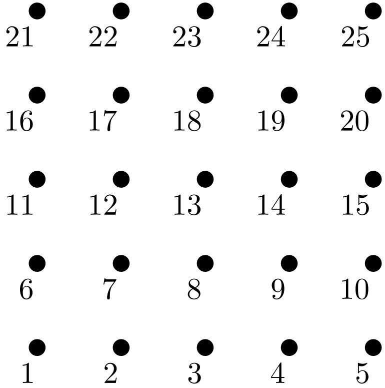
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



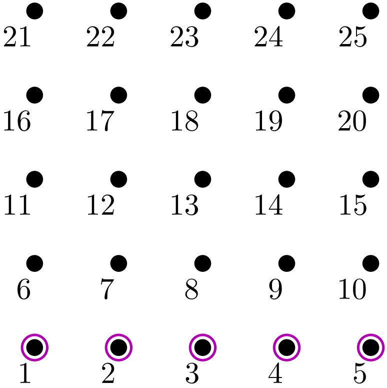
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



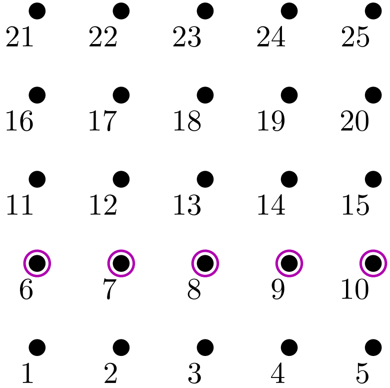
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



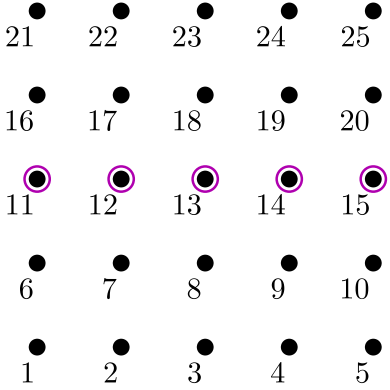
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:

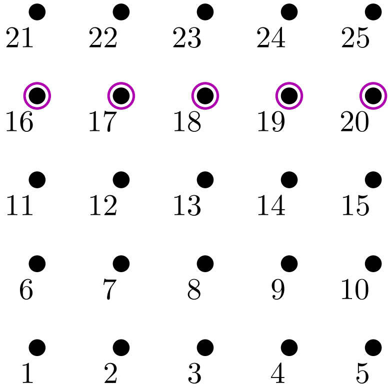


Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



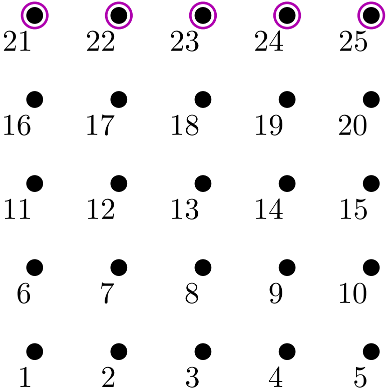
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



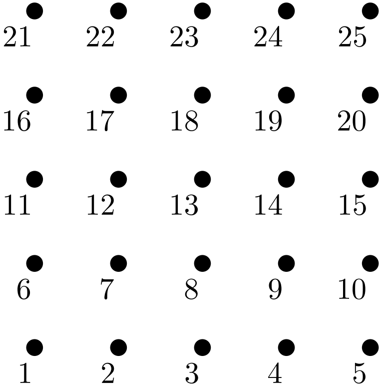
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



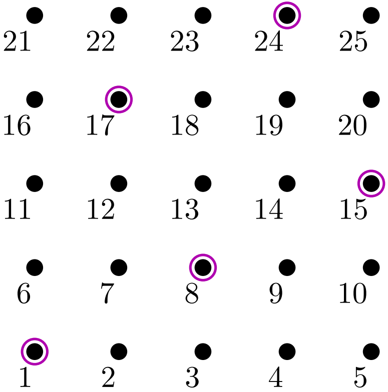
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



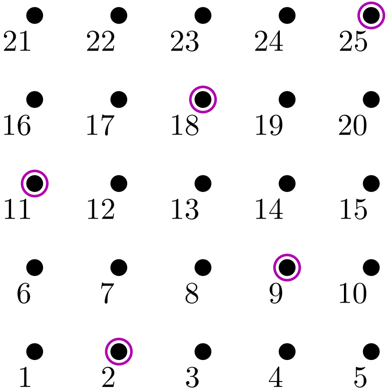
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



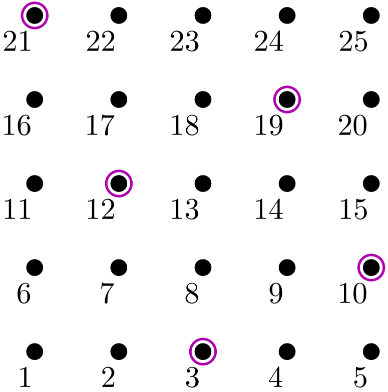
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



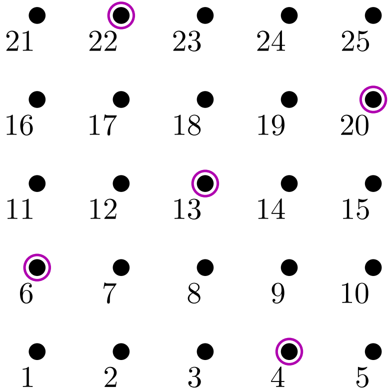
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



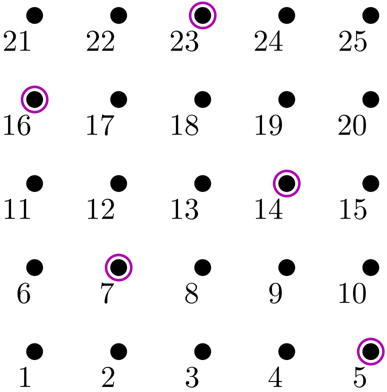
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



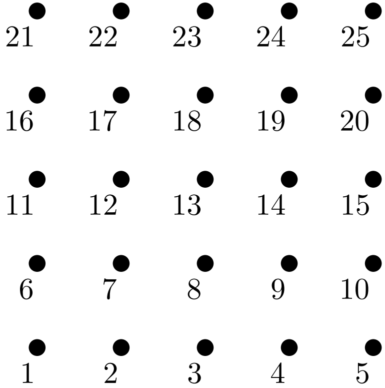
Overview of block designs

Race car tournament: 25 cars in tournament,
every race has 5 cars,
every car races 6 times,
every pair of cars race together once

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	8	15	17	24
2	9	11	18	25
3	10	12	19	21
4	6	13	20	22
5	7	14	16	23

$\mathbb{Z}_5^2$:



Overview of error-correcting codes

Encode messages so recipient can detect/correct errors

Overview of error-correcting codes

Encode messages so recipient can detect/correct errors

Example

$$\texttt{A} \to \texttt{000} \qquad \texttt{B} \to \texttt{111}$$

Overview of error-correcting codes

Encode messages so recipient can detect/correct errors

Example

$$\mathtt{A} \to \mathtt{000} \qquad \mathtt{B} \to \mathtt{111}$$

Send message ABBA:

$$\mathtt{000\ 111\ 111\ 000} \quad \rightsquigarrow \quad \mathtt{000\ 110\ 111\ 010}$$

Overview of error-correcting codes

Encode messages so recipient can detect/correct errors

Example

$$\texttt{A} \to 000 \qquad \texttt{B} \to 111$$

Send message ABBA:

$$000\ 111\ 111\ 000 \quad \rightsquigarrow \quad 000\ 110\ 111\ 010$$

Goal: *efficient* error-correcting codes

$$\text{Block designs} \longrightarrow \text{Error-correcting codes}$$

Course content

Content: finite fields (5 weeks)
block designs (2 weeks)
error-correcting codes (2 weeks)

Course content

Content: finite fields (5 weeks)
block designs (2 weeks)
error-correcting codes (2 weeks)

Students: 50% intro to proofs, 50% proof-based linear algebra
15% taken abstract algebra, 20% no modular arithmetic

Course content

Content: finite fields (5 weeks)
block designs (2 weeks)
error-correcting codes (2 weeks)

Students: 50% intro to proofs, 50% proof-based linear algebra
15% taken abstract algebra, 20% no modular arithmetic

Finite fields: modular arithmetic
rings and fields
polynomial rings, factorization
finite fields, fundamental theorem
finite geometry

Course content

Content: finite fields (5 weeks)
block designs (2 weeks)
error-correcting codes (2 weeks)

Students: 50% intro to proofs, 50% proof-based linear algebra
15% taken abstract algebra, 20% no modular arithmetic

Finite fields: modular arithmetic
rings and fields
polynomial rings, factorization
finite fields, fundamental theorem
finite geometry

Goals: emphasize usage in practice
some theory/proof practice

Course structure

Split days: 2 lecture days (Monday/Wednesday)
2 discussion days (Thursday/Friday)

Course structure

Split days: 2 lecture days (Monday/Wednesday)
2 discussion days (Thursday/Friday)

Discussion days: work in groups of 3-4
cover new/essential material
short preliminary assignment beforehand

Course structure

Split days: 2 lecture days (Monday/Wednesday)
2 discussion days (Thursday/Friday)

Discussion days: work in groups of 3-4
cover new/essential material
short preliminary assignment beforehand

Choosing split: introduce topic in lecture, discover theorems in discussion
preview topic in discussion, introduce formally in lecture

Course structure

Split days: 2 lecture days (Monday/Wednesday)
2 discussion days (Thursday/Friday)

Discussion days: work in groups of 3-4
cover new/essential material
short preliminary assignment beforehand

Choosing split: introduce topic in lecture, discover theorems in discussion
preview topic in discussion, introduce formally in lecture

Benefits of "half-IBL": adjust lecture after rough discussion
maintain "expected" pace
lower chance of student revolt

Course structure

Split days: 2 lecture days (Monday/Wednesday)
2 discussion days (Thursday/Friday)

Discussion days: work in groups of 3-4
cover new/essential material
short preliminary assignment beforehand

Choosing split: introduce topic in lecture, discover theorems in discussion
preview topic in discussion, introduce formally in lecture

Benefits of "half-IBL": adjust lecture after rough discussion
maintain "expected" pace
lower chance of student revolt

Bonus benefit: help sidestep theoretical aspects

Sample discussion: finite fields

(D1) *Finite fields.* The goal of this problem is to systematically build "small" finite fields.

(a) Suppose $F_3 = \{0, 1, a\}$ is a field with exactly 3 elements. Fill in as much of the addition and multiplication table as you can using only the field axioms.

(b) How many entries in your answer to part (a) remain? Which field(s) can F_3 be?

(c) Do the same for a field $F_4 = \{0, 1, a, b\}$ with exactly 4 elements.

(d) What is the order of each element of F_4? What familiar additive group did you obtain? With this in mind, is the multiplication structure what you expected it to be?

(e) Suppose F_6 is a field with exactly 6 elements. Can $1 \in F_6$ have order 6?

(f) It turns out the order of an element of a finite ring must divide the size of the ring. With this in mind, for each possible order of $1 \in F_6$, try writing out the addition and multiplication tables. When are you able to fill both tables?

(g) Fill in the addition and multiplication tables for a field $F_5 = \{0, 1, a, b, c\}$ with exactly 5 elements (this is tricky, but a fun challenge!). What ring(s) do you get?

Sample discussion: finite fields

(D1) *Finite fields.* The goal of this problem is to systematically build "small" finite fields.

(a) Suppose $F_3 = \{0, 1, a\}$ is a field with exactly 3 elements. Fill in as much of the addition and multiplication table as you can using only the field axioms.

(b) How many entries in your answer to part (a) remain? Which field(s) can F_3 be?

(c) Do the same for a field $F_4 = \{0, 1, a, b\}$ with exactly 4 elements.

(d) What is the order of each element of F_4? What familiar additive group did you obtain? With this in mind, is the multiplication structure what you expected it to be?

(e) Suppose F_6 is a field with exactly 6 elements. Can $1 \in F_6$ have order 6?

(f) It turns out the order of an element of a finite ring must divide the size of the ring. With this in mind, for each possible order of $1 \in F_6$, try writing out the addition and multiplication tables. When are you able to fill both tables?

(g) Fill in the addition and multiplication tables for a field $F_5 = \{0, 1, a, b, c\}$ with exactly 5 elements (this is tricky, but a fun challenge!). What ring(s) do you get?

$+$	0	1	a
0	0	1	a
1	1		
a	a		

$\times$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	

Sample discussion: finite fields

(D1) *Finite fields.* The goal of this problem is to systematically build "small" finite fields.

(a) Suppose $F_3 = \{0, 1, a\}$ is a field with exactly 3 elements. Fill in as much of the addition and multiplication table as you can using only the field axioms.

(b) How many entries in your answer to part (a) remain? Which field(s) can F_3 be?

(c) Do the same for a field $F_4 = \{0, 1, a, b\}$ with exactly 4 elements.

(d) What is the order of each element of F_4? What familiar additive group did you obtain? With this in mind, is the multiplication structure what you expected it to be?

(e) Suppose F_6 is a field with exactly 6 elements. Can $1 \in F_6$ have order 6?

(f) It turns out the order of an element of a finite ring must divide the size of the ring. With this in mind, for each possible order of $1 \in F_6$, try writing out the addition and multiplication tables. When are you able to fill both tables?

(g) Fill in the addition and multiplication tables for a field $F_5 = \{0, 1, a, b, c\}$ with exactly 5 elements (this is tricky, but a fun challenge!). What ring(s) do you get?

$+$	0	1	a
0	0	1	a
1	1		
a	a		

$\times$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Sample discussion: finite fields

(D1) *Finite fields.* The goal of this problem is to systematically build "small" finite fields.

(a) Suppose $F_3 = \{0, 1, a\}$ is a field with exactly 3 elements. Fill in as much of the addition and multiplication table as you can using only the field axioms.

(b) How many entries in your answer to part (a) remain? Which field(s) can F_3 be?

(c) Do the same for a field $F_4 = \{0, 1, a, b\}$ with exactly 4 elements.

(d) What is the order of each element of F_4? What familiar additive group did you obtain? With this in mind, is the multiplication structure what you expected it to be?

(e) Suppose F_6 is a field with exactly 6 elements. Can $1 \in F_6$ have order 6?

(f) It turns out the order of an element of a finite ring must divide the size of the ring. With this in mind, for each possible order of $1 \in F_6$, try writing out the addition and multiplication tables. When are you able to fill both tables?

(g) Fill in the addition and multiplication tables for a field $F_5 = \{0, 1, a, b, c\}$ with exactly 5 elements (this is tricky, but a fun challenge!). What ring(s) do you get?

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

$\times$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?

Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

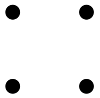
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

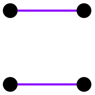
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?

Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?

Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

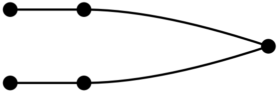
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

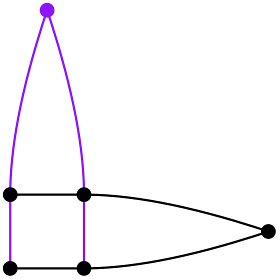
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

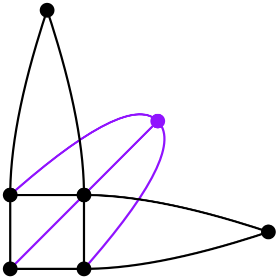
(ii) For each pair L_1, L_2 of parallel lines, draw a new point “off the edge of the plane” and extend L_1 and L_2 to contain the new point. They might not be “straight”!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

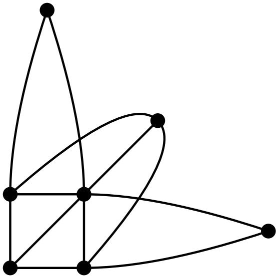
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

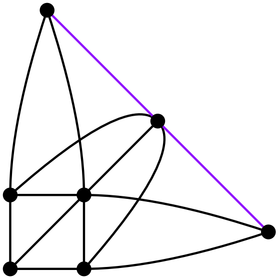
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



Sample discussion: projective plane

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

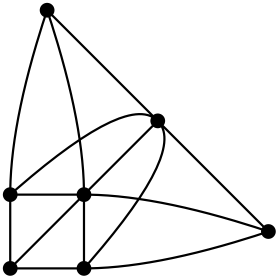
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?



(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.

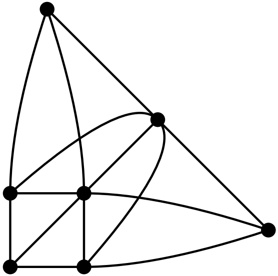
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!

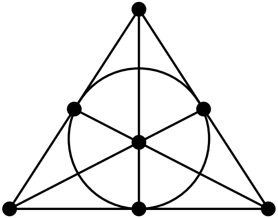
(iii) How many points does your space have? How many points does each line have?

(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?

(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}^2$. What is the maximum number of non-parallel lines?





Sample homework: modular arithmetic (week 1)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Sample homework: modular arithmetic (week 1)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Required problems. As the name suggests, you must submit *all* required problems with this homework set in order to receive full credit.

(R1) Write the addition and multiplication tables for $\mathbb{Z}_6$. You can leave off the $[\ \ ]_6$ notation and simply denote the elements by $0, 1, 2, 3, 4, 5 \in \mathbb{Z}_6$.

(R2) Determine whether each of the following statements is true or false. Justify your answer (you are not required to give a formal proof). You may *not* use a calculator.

- (a) 14323341327 is prime.
- (b) There exists $x \in \mathbb{Z}$ such that $x^2 + 1 = 123456789$.

(R3) Find all $x, y \in \mathbb{Z}_7$ that are solutions to both of the equations

$$x + 2y = [4]_7 \qquad \text{and} \qquad 4x + 3y = [4]_7$$

in $\mathbb{Z}_7$. Do the same for $x, y \in \mathbb{Z}_6$ (where $[4]_7$ is replaced with $[4]_6$).

(R4) Prove that an integer x is divisible by 4 if and only if the last two digits of x in base 10 form a 2-digit number that is divisible by 4.

Sample homework: modular arithmetic (week 1)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) (a) Suppose $(x_n \cdots x_1 x_0)_{10}$ expresses x in base 10. Prove that

$$x \equiv x_0 - x_1 + x_2 - x_3 + \cdots + (-1)^n x_n \bmod 11.$$

(b) Use part (a) to decide whether 1213141516171819 is divisible by 11.

(S2) The goal of this question is to prove that the "freshman's dream" equation

$$(x + y)^p = x^p + y^p$$

holds for any $x, y \in \mathbb{Z}_p$ when p is prime.

(a) Recall that for any $n, k \geq 0$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is an integer. Prove that if p is prime and $1 \leq k \leq p - 1$, then p divides $\binom{p}{k}$.

(b) Recall that for any $x, y \in \mathbb{R}$

Sample homework: modular arithmetic (week 1)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) We saw in class that an integer x is divisible by 9 if and only if the sum of the digits (base 10) of x is divisibile by 9, and you proved in discussion that the same holds for divisibility by 3. Fix a base b. State and prove a characterization of the n for which the following holds: an integer x is divisible by n if and only if the sum of the digits (base b) of x is divisible by n. As an example, for $b = 10$, this only holds for $n = 3$ and $n = 9$.

Sample homework: finite fields (week 4)

Required problems: computational, “1-line” proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Sample homework: finite fields (week 4)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) Factor $f(x) = x^5 + x^4 + 1$ over $\mathbb{F}_2$, $\mathbb{F}_4$, and $\mathbb{F}_8$.

(R2) Multiply all of the nonzero elements of $\mathbb{F}_5$ together. Do the same for $\mathbb{F}_{11}$ and $\mathbb{F}_4$. Find a formula for the product of all nonzero elements of $\mathbb{F}_{p^r}$.

(R3) For p prime, find a formula for the number of irreducible polynomials of degree at most 3 in $\mathbb{Z}_p[x]$. You are *not* required to prove your formula holds.

(R4) Provide a proof for either (R2) or (R3). Bonus points will be awarded if you prove both. Hint: use the theorem about how $x^q - x$ factors over $\mathbb{F}_q$.

Sample homework: finite fields (week 4)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) (a) Let $a(n)$ denote the number of degree-n irreducible polynomials over $\mathbb{F}_2$. Prove that

$$2^n = \sum_{d \mid n} d \cdot a(d).$$

Hint: use the theorem about how $x^{2^d} - x$ factors over $\mathbb{F}_2$.

(b) Find the number of irreducible polynomials over $\mathbb{F}_2$ with degree exactly 31.

(c) Find the number of irreducible polynomials over $\mathbb{F}_2$ with degree exactly 21.

(S2) A field F is *algebraically closed* if every polynomial in $F[x]$ has a root in F. For example, $\mathbb{C}$ is algebraically closed, but $\mathbb{R}$ is not since $x^2 + 1$ has no roots in $\mathbb{R}$. Prove that no finite field $\mathbb{F}_{p^r}$ is algebraically closed.

Sample homework: finite fields (week 4)

Required problems: computational, "1-line" proofs

Selection problems: proof-based, combine several ideas

Challenge problems: optional, requiring sizeable generalization

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) By the fundamental theorem of finite fields,

$$F = \mathbb{Z}_2[z]/\langle z^3 + z + 1\rangle \qquad \text{and} \qquad F' = \mathbb{Z}_2[z]/\langle z^3 + z^2 + 1\rangle$$

are both fields with 8 elements and thus must be the same. Find an explicit bijection $F \to F'$ that preserves both addition and multiplication.

Verdict (based on exit interviews & course evalutations)

Overall very positive feedback

Students develop "just try it and see what happens" attitude

Many students initially dread discussion, later look forward to it

Many liked seeing nonstandard topics (projective geometry, latin squares)

Some found it helpful later in abstract algebra

A few said is was too theoretical

A few said it wasn't rigorous enough

References

N. Biggs (2002)
Discrete Mathematics (2nd edition)
Oxford University Press.

C. O'Neill, L. Silverstein (2018)
Discovery learning in an interdisciplinary course on finite fields and applications
in preparation.

C. O'Neill, L. Silverstein (2018)
Math 148 course materials
https://www.math.ucdavis.edu/~coneill/teaching/w18-148/.

Thanks!