Kirkman's Schoolgirls
wearing hats and walking through fields of numbers

Keith E. Mellinger
University of Mary Washington

October 2010

The Kirkman Schoolgirls Problem

Imagine fifteen young ladies at the Emmy Noether Boarding School.

The Kirkman Schoolgirls Problem

Imagine fifteen young ladies at the Emmy Noether Boarding School.

Every day, they walk to school in the Official ENBS Formation, namely, in five rows of three each. One of the ENBS rules is that during the walk, a student may only talk with the other students in her row of three.

The Kirkman Schoolgirls Problem

Imagine fifteen young ladies at the Emmy Noether Boarding School.

Every day, they walk to school in the Official ENBS Formation, namely, in five rows of three each. One of the ENBS rules is that during the walk, a student may only talk with the other students in her row of three.

These fifteen are all good friends and like to talk with each other – and they are all mathematically inclined.

The Kirkman Schoolgirls Problem

One day Julia says, "I wonder if it's possible for us to walk to school in the Official Formation in such a way that we all have a chance to talk with each other at least once a week?"

The Kirkman Schoolgirls Problem

"But that means nobody walks with anybody else in a line more than once a week," observes Anita.

The Kirkman Schoolgirls Problem

"I'll bet we can do that," concludes Lori.
"Let's get to work."

Solution

MON	TUE	WED	THU	FRI	SAT	SUN
a, b, e	a, c, f	a, d, h	a, g, k	a, j, m	a, n, o	a, i, l
c, l, o	b, m, o	b, c, g	b, h, l	b, f, k	b, d, i	b, j, n
d, f, m	d, g, n	e, j, o	c, d, j	c, i, n	c, e, k	c, h, m
g, i, j	e, h, i	f, l, n	e, m, n	d, e, l	f, h, j	d, k, o
h, k, n	j, k, l	i, k, m	f, i, o	g, h, o	g, l, m	e, f, g

T. P. Kirkman

Rev. Thomas Penyngton Kirkman (31 March 1806 - 3 February 1895) was a British mathematician.

T. P. Kirkman

The problem first appeared in 1850 in the unlikely-sounding *Lady's and Gentlemen's Diary*, it reads as follows:

"Fifteen young ladies of a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk abreast more than once."

T. P. Kirkman

- Published his first mathematical paper when he was 40
- first to describe many structures in discrete mathematics: block designs, bipartite graphs, and Hamiltonian circuits
- combinatorialists regard him as the "Father of Design Theory"

T. P. Kirkman

- Published his first mathematical paper when he was 40
- first to describe many structures in discrete mathematics: block designs, bipartite graphs, and Hamiltonian circuits
- combinatorialists regard him as the "Father of Design Theory"

his fame outside the field rests entirely on the Schoolgirls Problem and his solution

What is this talk about?

Solutions to Kirkman's Problem are not so hard to find. In fact, I can find solutions to the problem in

What is this talk about?

Solutions to Kirkman's Problem are not so hard to find. In fact, I can find solutions to the problem in

1. Algebraic number fields

What is this talk about?

Solutions to Kirkman's Problem are not so hard to find. In fact, I can find solutions to the problem in

1. Algebraic number fields
2. Finite geometry

What is this talk about?

Solutions to Kirkman's Problem are not so hard to find. In fact, I can find solutions to the problem in

1. Algebraic number fields
2. Finite geometry
3. Coding theory

What is this talk about?

Solutions to Kirkman's Problem are not so hard to find. In fact, I can find solutions to the problem in

1. Algebraic number fields

2. Finite geometry

3. Coding theory

4. Recreational mathematics

block designs

A collection of v points, broken into subset of size k is called a *design* when every set of t points lies in the same number of blocks.

block designs

A collection of v points, broken into subset of size k is called a *design* when every set of t points lies in the same number of blocks.

For the Kirkman problem, we want $v = 15$, $k = 3$, and every set of 2 girls appears together in a block (or a row of the formation) exactly 1 time.

block designs

A collection of v points, broken into subset of size k is called a *design* when every set of t points lies in the same number of blocks.

For the Kirkman problem, we want $v = 15$, $k = 3$, and every set of 2 girls appears together in a block (or a row of the formation) exactly 1 time.

We say that a solution to the Kirkman problem is a $2 - (15, 3, 1)$ design

block designs

We can do some counting.

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total.

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total. So, each girl should appear in 7 different blocks.

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total. So, each girl should appear in 7 different blocks.

How many block do we need?

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total. So, each girl should appear in 7 different blocks.

How many block do we need? Well, we need 5 each day for 7 days...

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total. So, each girl should appear in 7 different blocks.

How many block do we need? Well, we need 5 each day for 7 days... that's **35** blocks.

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total. So, each girl should appear in 7 different blocks.

How many block do we need? Well, we need 5 each day for 7 days... that's **35** blocks.

Moreover, every day we use 5 blocks that partition the girls.

block designs

We can do some counting.

Every girl walks with every other girl exactly once, and every block contains 3 girls total. So, each girl should appear in 7 different blocks.

How many block do we need? Well, we need 5 each day for 7 days... that's **35** blocks.

Moreover, every day we use 5 blocks that partition the girls.

When the block can be broken up like this, we say the design is *resolvable.*

what do we need?

Mathematical formulation of the Kirkman Schoolgirls Problem:

what do we need?

Mathematical formulation of the Kirkman Schoolgirls Problem:

Find a resolvable $2 - (15, 3, 1)$ design containing 35 blocks.

Fields

Fields allow for multiplication by inverses, commutativity, associativity, additive and multiplicative identities, etc. They have about as much structure as you could want under the two operations of addition and multiplication.

Fields

Fields allow for multiplication by inverses, commutativity, associativity, additive and multiplicative identities, etc. They have about as much structure as you could want under the two operations of addition and multiplication.

Common fields: Complex Numbers ($\mathbb{C}$), Real Numbers, ($\mathbb{R}$), Rational Numbers ($\mathbb{Q}$)

Fields

Fields allow for multiplication by inverses, commutativity, associativity, additive and multiplicative identities, etc. They have about as much structure as you could want under the two operations of addition and multiplication.

Common fields: Complex Numbers ($\mathbb{C}$), Real Numbers, ($\mathbb{R}$), Rational Numbers ($\mathbb{Q}$)

Non-fields:

Fields

Fields allow for multiplication by inverses, commutativity, associativity, additive and multiplicative identities, etc. They have about as much structure as you could want under the two operations of addition and multiplication.

Common fields: Complex Numbers ($\mathbb{C}$), Real Numbers, ($\mathbb{R}$), Rational Numbers ($\mathbb{Q}$)

Non-fields: Integers ($\mathbb{Z}$),

Fields

Fields allow for multiplication by inverses, commutativity, associativity, additive and multiplicative identities, etc. They have about as much structure as you could want under the two operations of addition and multiplication.

Common fields: Complex Numbers ($\mathbb{C}$), Real Numbers, ($\mathbb{R}$), Rational Numbers ($\mathbb{Q}$)

Non-fields: Integers ($\mathbb{Z}$), Natural Numbers ($\mathbb{N}$)

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

4,

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

4, $\frac{1}{5}$,

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

4, $\frac{1}{5}$, $\sqrt{2}$,

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

4, $\frac{1}{5}$, $\sqrt{2}$, $\frac{\sqrt{2}}{5}$,

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

4, $\frac{1}{5}$, $\sqrt{2}$, $\frac{\sqrt{2}}{5}$, $1 + 2\sqrt{2}$

Extending a field

If we start with a field like $\mathbb{Q}$, we can always extend it to a larger field by adding elements from outside the base structure.

For instance, take the field of rational numbers and add to it the irrational number $\sqrt{2}$.

This field is denoted $\mathbb{Q}[\sqrt{2}]$ and contains:

4, $\frac{1}{5}$, $\sqrt{2}$, $\frac{\sqrt{2}}{5}$, $1 + 2\sqrt{2}$

In fact, every element of this field can be written as $a + b\sqrt{2}$ for some rational numbers a and b (i.e., $a, b \in \mathbb{Q}$).

Extending a field

You can show that this set forms a field (typical undergraduate abstract algebra problem!). For instance,

Extending a field

You can show that this set forms a field (typical undergraduate abstract algebra problem!). For instance,

Closed under multiplication:

Extending a field

You can show that this set forms a field (typical undergraduate abstract algebra problem!). For instance,

Closed under multiplication:

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$$

Since $a_1a_2 + 2b_1b_2 \in \mathbb{Q}$ and $a_1b_2 + a_2b_1 \in \mathbb{Q}$, we have shown closure.

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

$$\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

$\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Here, the field elements can all be written as

$$a+$$

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

$\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Here, the field elements can all be written as

$$a+b\sqrt{2}$$

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

$\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Here, the field elements can all be written as

$$a+b\sqrt{2}+c\sqrt{3}$$

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

$\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Here, the field elements can all be written as

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}.$$

Extending a field

You can repeat the process. For instance, take our field above and add the element $\sqrt{3}$.

$\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

Here, the field elements can all be written as

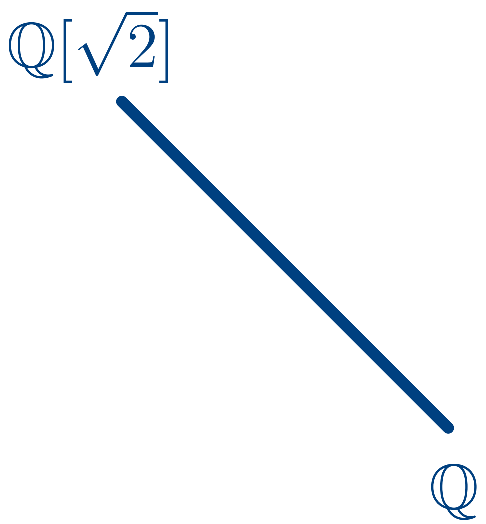
$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}.$$

Notice that by letting $c = d = 0$, we have all of the elements of our smaller field.

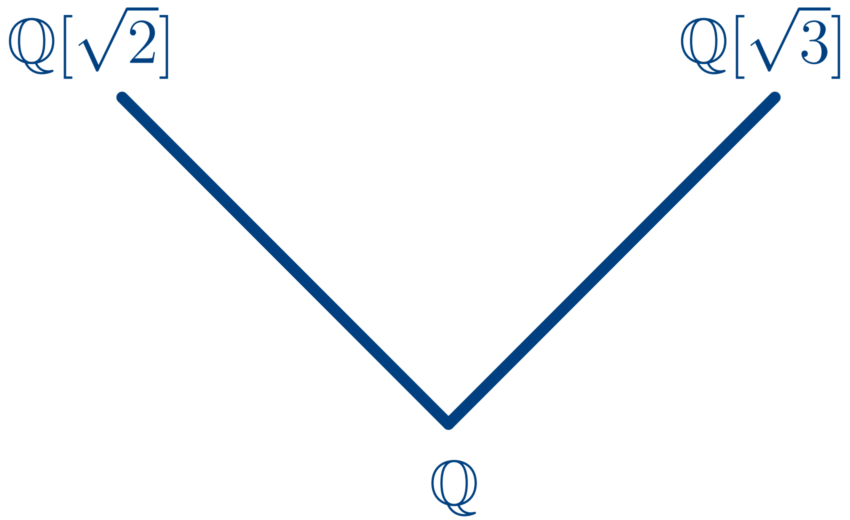
Extending a field

$\mathbb{Q}$

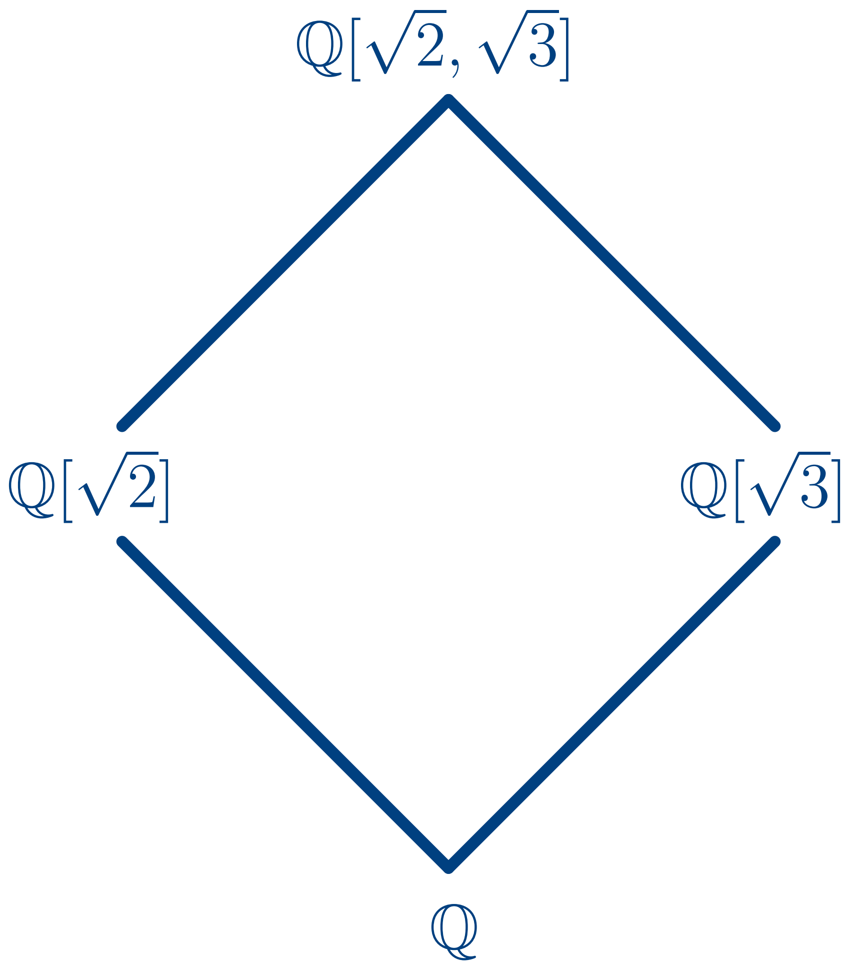
Extending a field



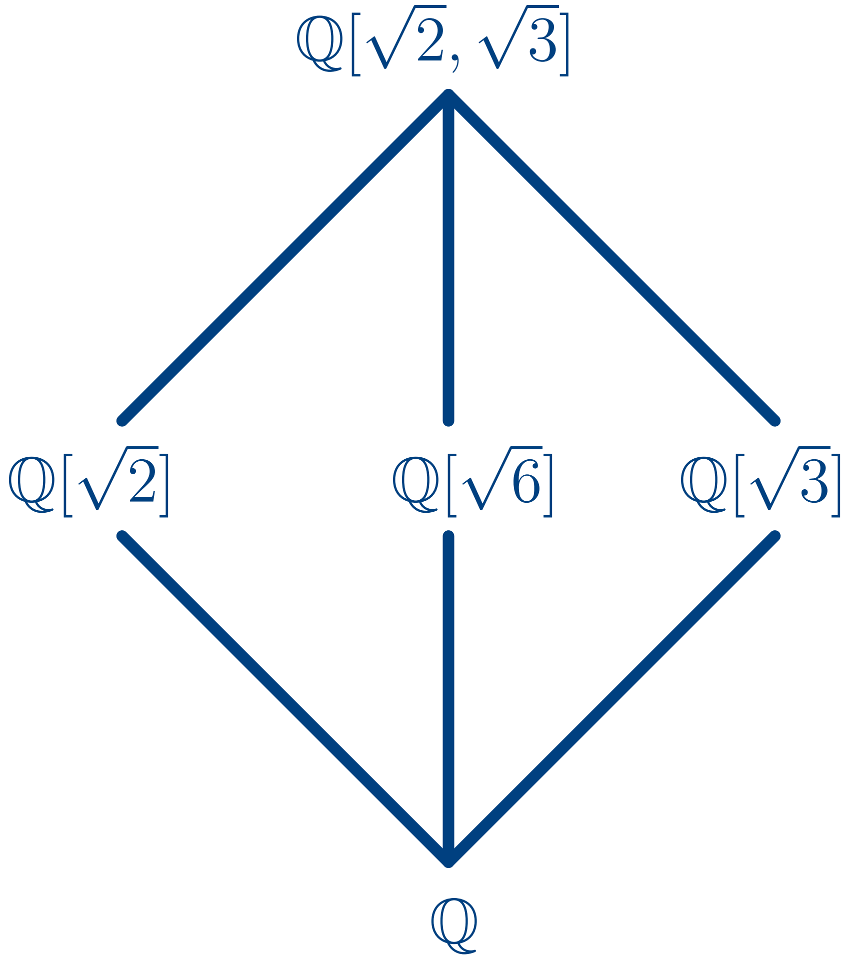
Extending a field



Extending a field



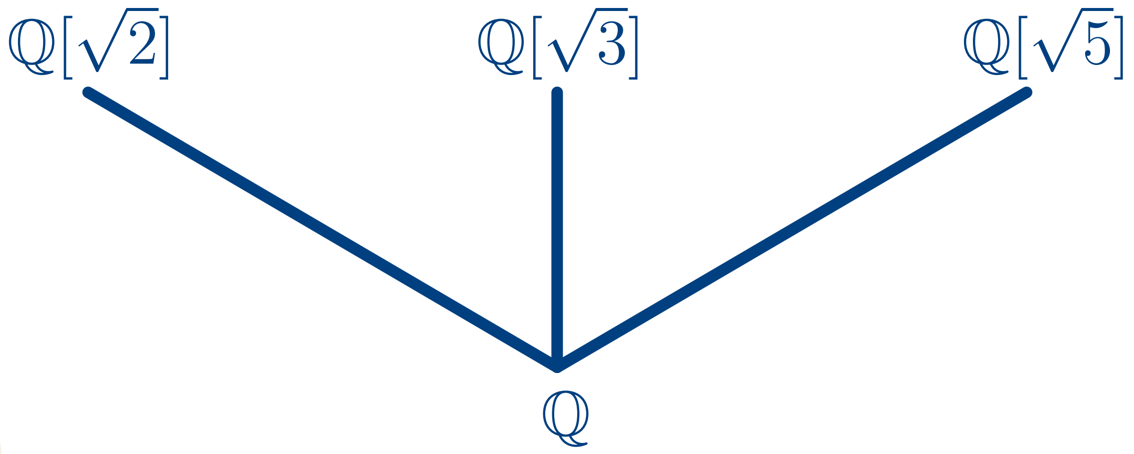
Extending a field



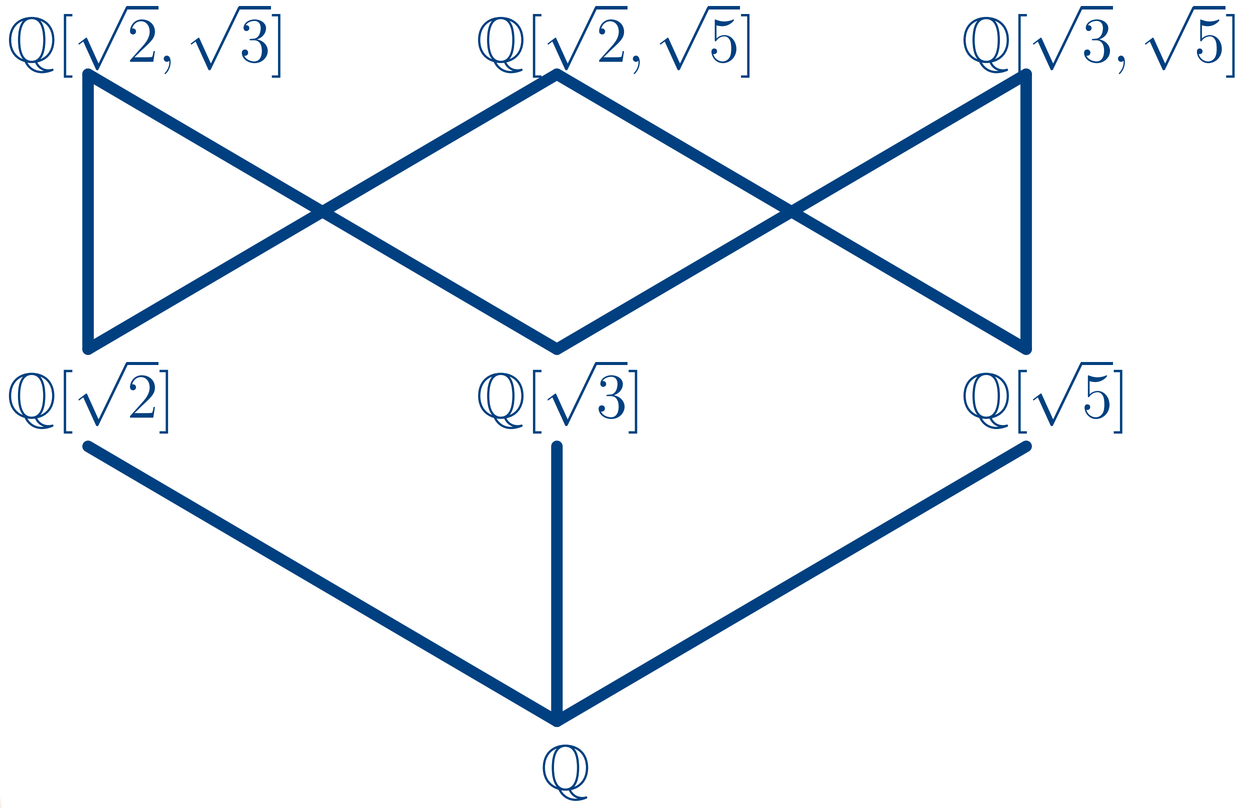
Extending a field

$\mathbb{Q}$

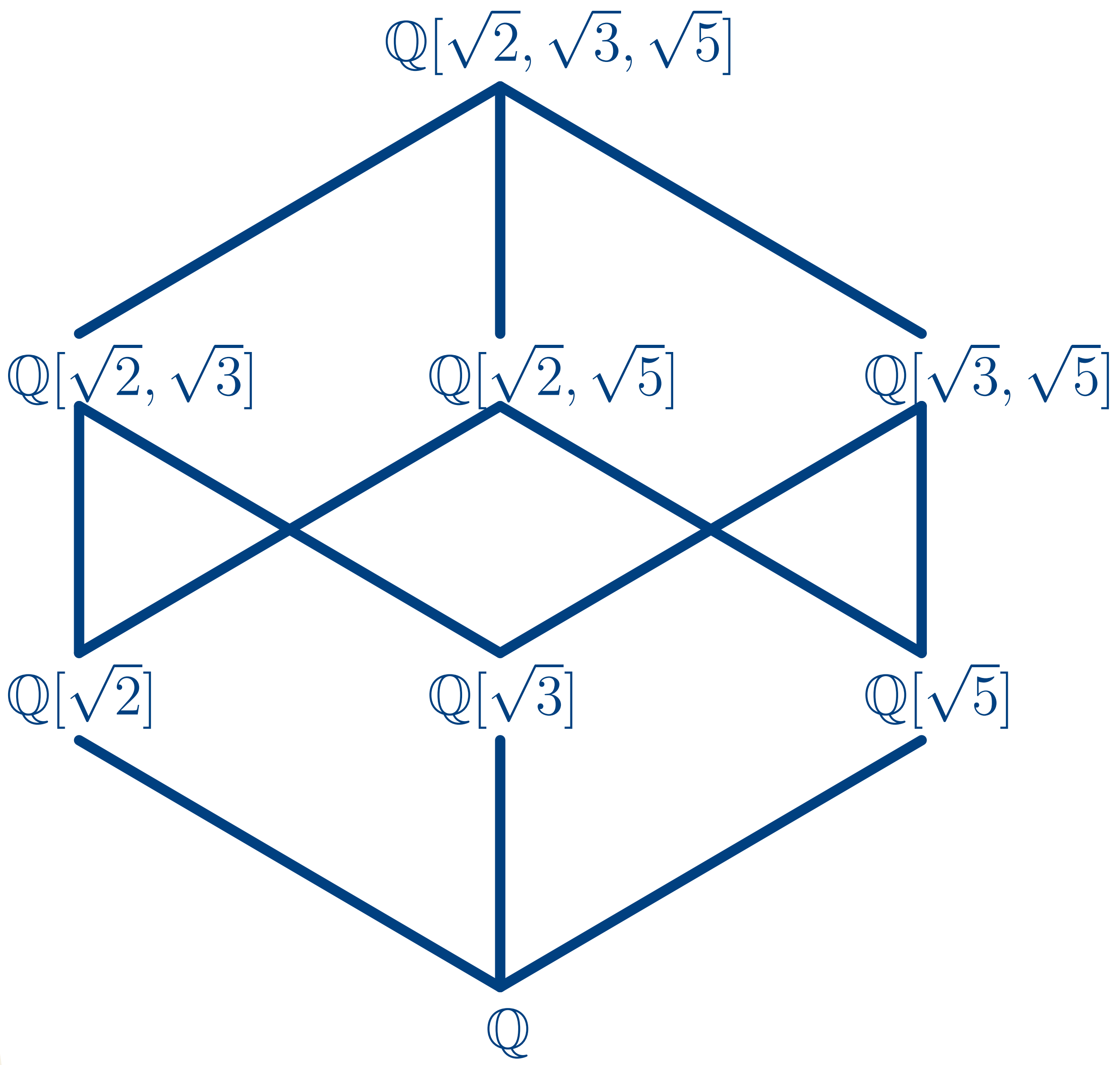
Extending a field



Extending a field



Extending a field



Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{6}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{10}]$

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{10}]$, ...

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{10}]$, ...

How many total?

Extending a field

What if we start with $\mathbb{Q}$ and add *four* irrationals to it?

Consider the field: $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}]$

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{10}]$, ...

How many total? **15**

Extending a field

Now consider how the quadratic subfields lie in the biquadratic subfields. For instance, $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ each lie in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Extending a field

Now consider how the quadratic subfields lie in the biquadratic subfields. For instance, $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ each lie in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$.

Extending a field

Now consider how the quadratic subfields lie in the biquadratic subfields. For instance, $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ each lie in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$.

How many total?

Extending a field

Now consider how the quadratic subfields lie in the biquadratic subfields. For instance, $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ each lie in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

We have lots of subfields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$.

How many total? **35**

A Kirkman Solution

A Kirkman Solution

The Schoolgirls are

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

The rows that they walk in are

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

The rows that they walk in are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

The rows that they walk in are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

Note that any biquadratic field, say $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, contains three quadratic subfields. In this case, they are $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt{6}]$.

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

The rows that they walk in are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

Note that any biquadratic field, say $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, contains three quadratic subfields. In this case, they are $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt{6}]$.

Some of them get tricky. For instance, the field $\mathbb{Q}[\sqrt{15}, \sqrt{6}]$, contains the three quadratic subfields

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

The rows that they walk in are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

Note that any biquadratic field, say $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, contains three quadratic subfields. In this case, they are $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt{6}]$.

Some of them get tricky. For instance, the field $\mathbb{Q}[\sqrt{15}, \sqrt{6}]$, contains the three quadratic subfields $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{15}]$, and

A Kirkman Solution

The Schoolgirls are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

The rows that they walk in are Algebraic Number Fields of the form $\mathbb{Q}[\sqrt{a}, \sqrt{b}]$ lying in the big field $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$.

Note that any biquadratic field, say $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, contains three quadratic subfields. In this case, they are $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt{6}]$.

Some of them get tricky. For instance, the field $\mathbb{Q}[\sqrt{15}, \sqrt{6}]$, contains the three quadratic subfields $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{15}]$, and $\mathbb{Q}[\sqrt{10}]$.

A Kirkman Solution

MON	TUE	WED	THU
$2, 3, 6$	$2, 5, 10$	$2, 7, 14$	$2, 15, 30$
$5, 21, 105$	$3, 70, 210$	$3, 5, 15$	$3, 14, 42$
$7, 30, 210$	$6, 14, 21$	$6, 35, 210$	$5, 7, 35$
$10, 14, 35$	$7, 15, 105$	$10, 42, 105$	$6, 70, 105$
$15, 42, 70$	$30, 35, 42$	$21, 30, 70$	$10, 21, 210$

FRI	SAT	SUN
$2, 21, 42$	$2, 35, 70$	$2, 105, 210$
$3, 35, 105$	$3, 7, 21$	$3, 10, 30$
$5, 6, 30$	$5, 42, 210$	$5, 14, 70$
$7, 10, 70$	$6, 10, 15$	$6, 7, 42$
$14, 15, 210$	$14, 30, 105$	$15, 21, 35$

Finite Projective Geometry

Finite projective 3-space is sort of like Euclidean 3-space, except that

Finite Projective Geometry

Finite projective 3-space is sort of like Euclidean 3-space, except that

(a) there are only a finite number of points, and

Finite Projective Geometry

Finite projective 3-space is sort of like Euclidean 3-space, except that

(a) there are only a finite number of points, and

(b) any two lines that are in the same plane intersect.

Finite Projective Geometry

Every finite space has an associated *order* that tells us now many points lie on a line. If we call the order q, one can show that every line contains $q+1$ points.

Finite Projective Geometry

Every finite space has an associated *order* that tells us now many points lie on a line. If we call the order q, one can show that every line contains $q + 1$ points.

Finite projective 3-space, denoted by $PG(3, q)$ contains $q^3 + q^2 + q + 1$ points.

Finite Projective Geometry

Every finite space has an associated *order* that tells us now many points lie on a line. If we call the order q, one can show that every line contains $q+1$ points.

Finite projective 3-space, denoted by $PG(3,q)$ contains q^3+q^2+q+1 points.

Notice that, conceivably one could take the entire space and partition it.

$$q^3+q^2+q+1=(q^2+1)(q+1)$$

Finite Projective Geometry

Every finite space has an associated *order* that tells us now many points lie on a line. If we call the order q, one can show that every line contains $q + 1$ points.

Finite projective 3-space, denoted by $PG(3, q)$ contains $q^3 + q^2 + q + 1$ points.

Notice that, conceivably one could take the entire space and partition it.

$$q^3 + q^2 + q + 1 = (q^2 + 1)(q + 1)$$

Is it possible to partition $PG(3, q)$ into $q^2 + 1$ lines?

let $q = 2$

Number of points of $PG(3,2) = 2^3 + 2^2 + 2 + 1 = 15$.

let $q = 2$

Number of points of $PG(3, 2) = 2^3 + 2^2 + 2 + 1 = 15$.

Number of points on a line of $PG(3, 2) = 2 + 1 = 3$.

let $q = 2$

Number of points of $PG(3,2) = 2^3 + 2^2 + 2 + 1 = 15$.

Number of points on a line of $PG(3,2) = 2 + 1 = 3$.

Number of lines in a line-partition of $PG(3,2) = 2^2 + 1 = 5$.

let $q = 2$

Number of points of $PG(3, 2) = 2^3 + 2^2 + 2 + 1 = 15$.

Number of points on a line of $PG(3, 2) = 2 + 1 = 3$.

Number of lines in a line-partition of $PG(3, 2) = 2^2 + 1 = 5$.

Number of lines in $PG(3, 2)$ is

let $q = 2$

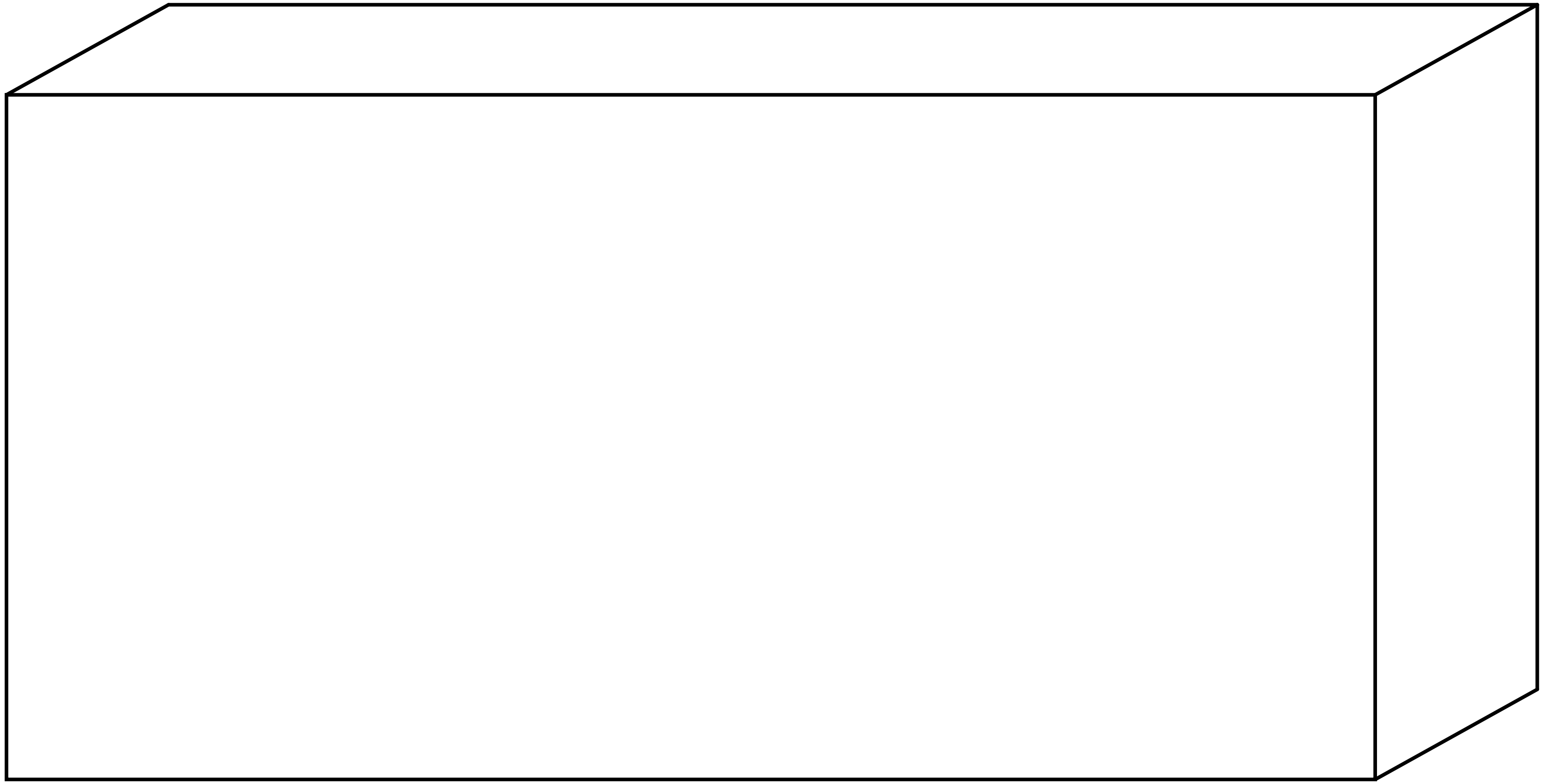
Number of points of $PG(3,2) = 2^3 + 2^2 + 2 + 1 = 15$.

Number of points on a line of $PG(3,2) = 2 + 1 = 3$.

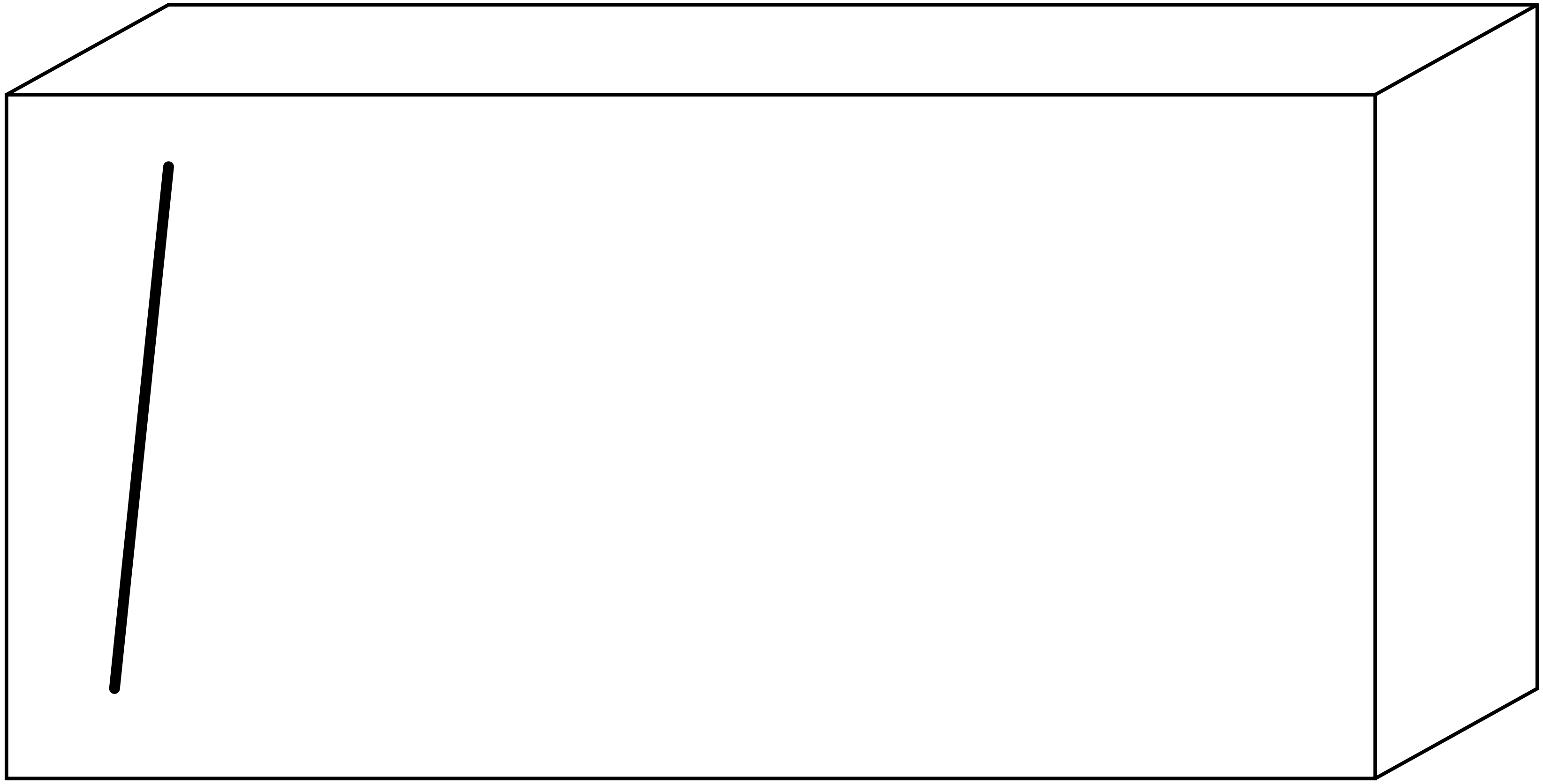
Number of lines in a line-partition of $PG(3,2) = 2^2 + 1 = 5$.

Number of lines in $PG(3,2)$ is **35**.

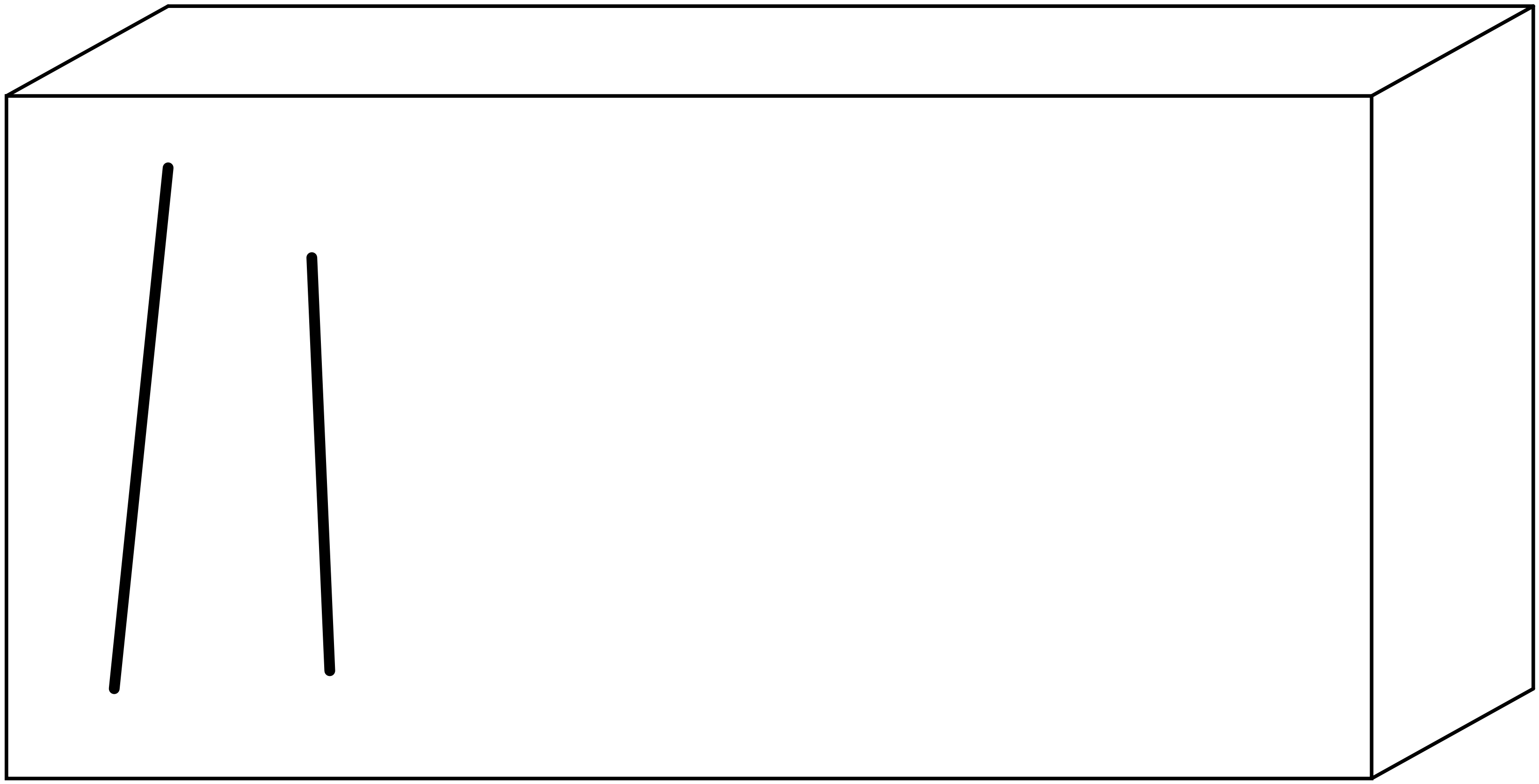
Partitioning 3-space



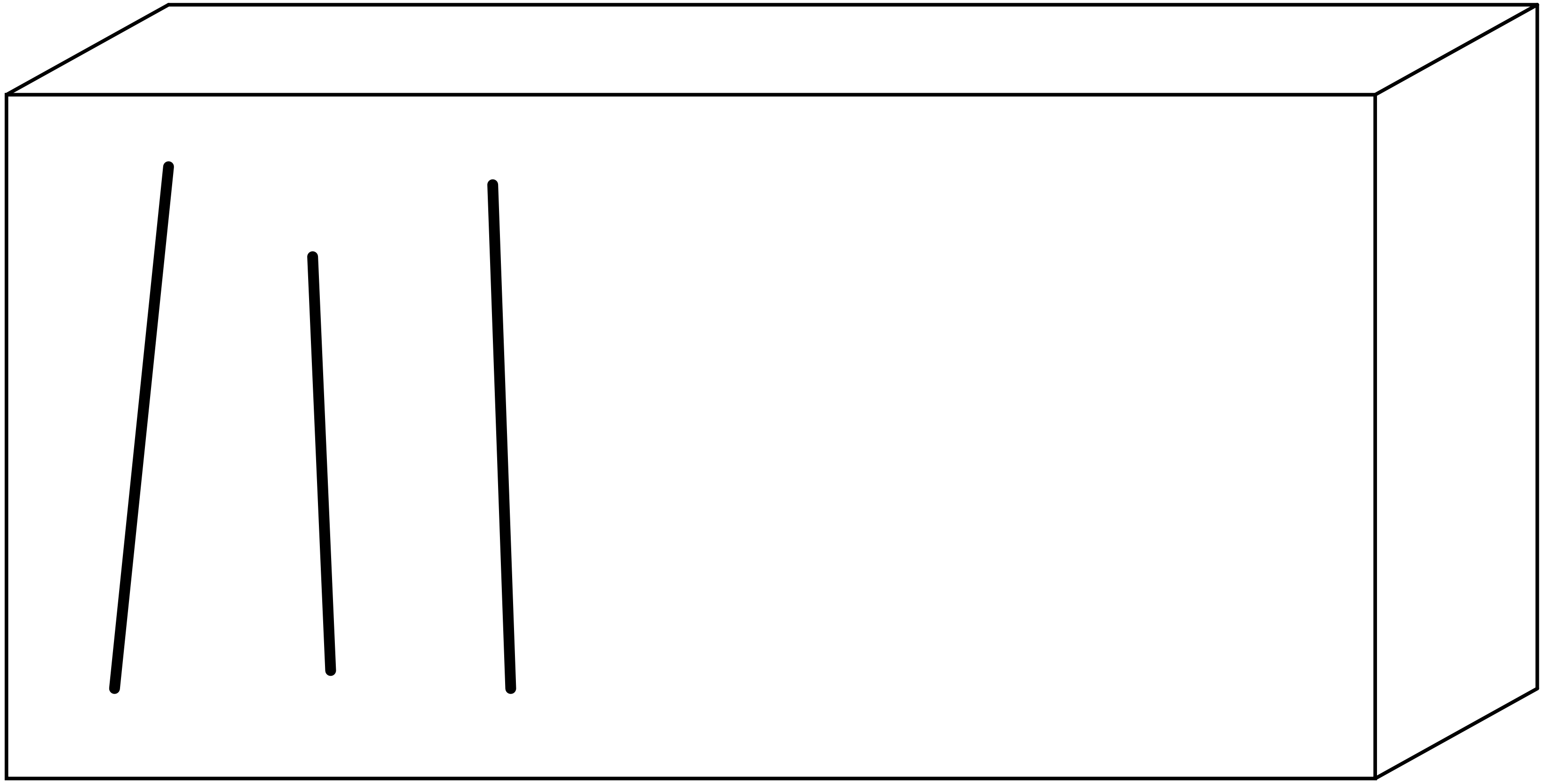
Partitioning 3-space



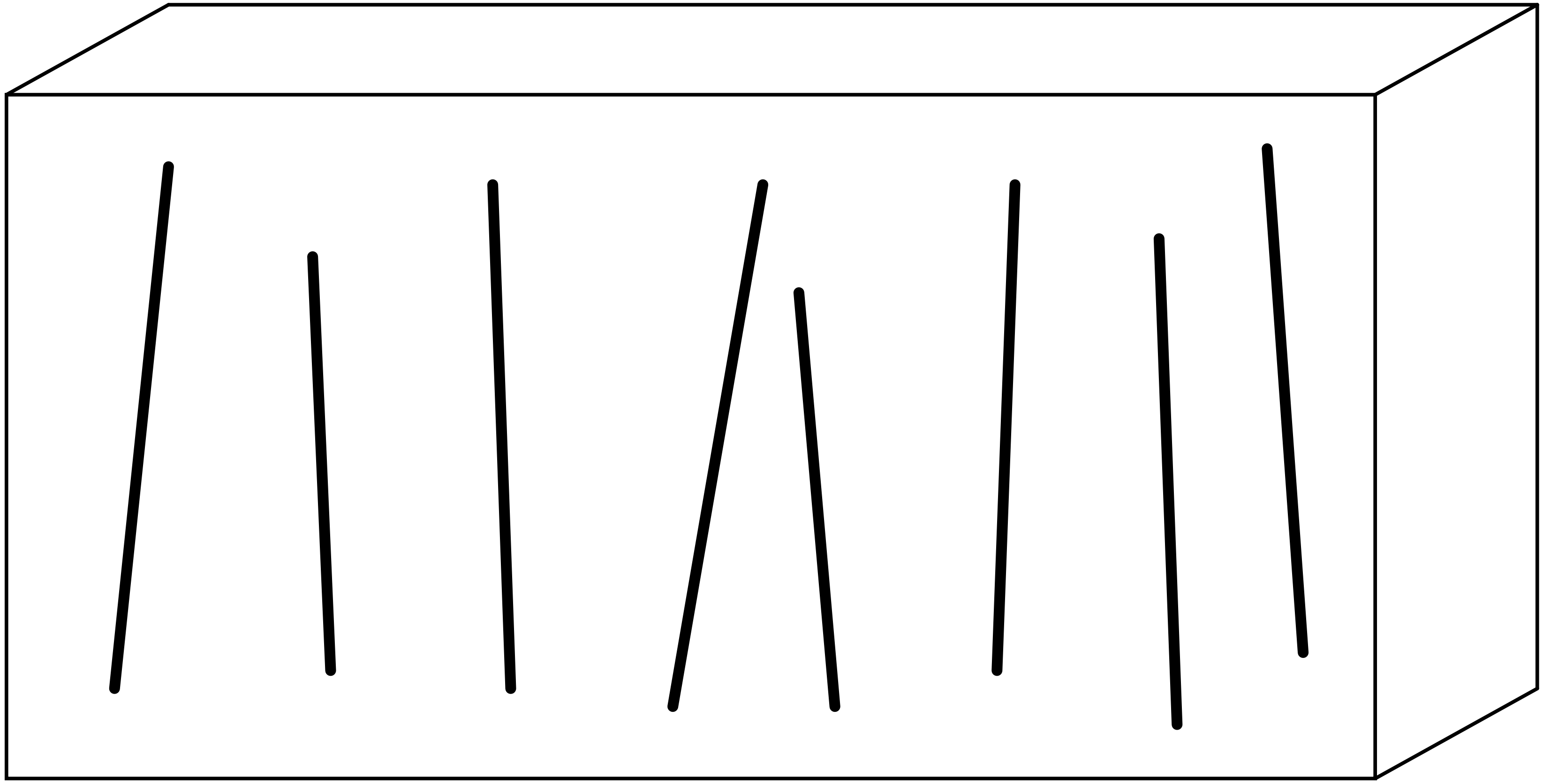
Partitioning 3-space



Partitioning 3-space



Partitioning 3-space



General Partitioning of 3-space

There are $q^3 + q^2 + q + 1$ points in finite projective 3-space, Σ.

General Partitioning of 3-space

There are $q^3 + q^2 + q + 1$ points in finite projective 3-space, Σ.

There are $q + 1$ points on each line of Σ.

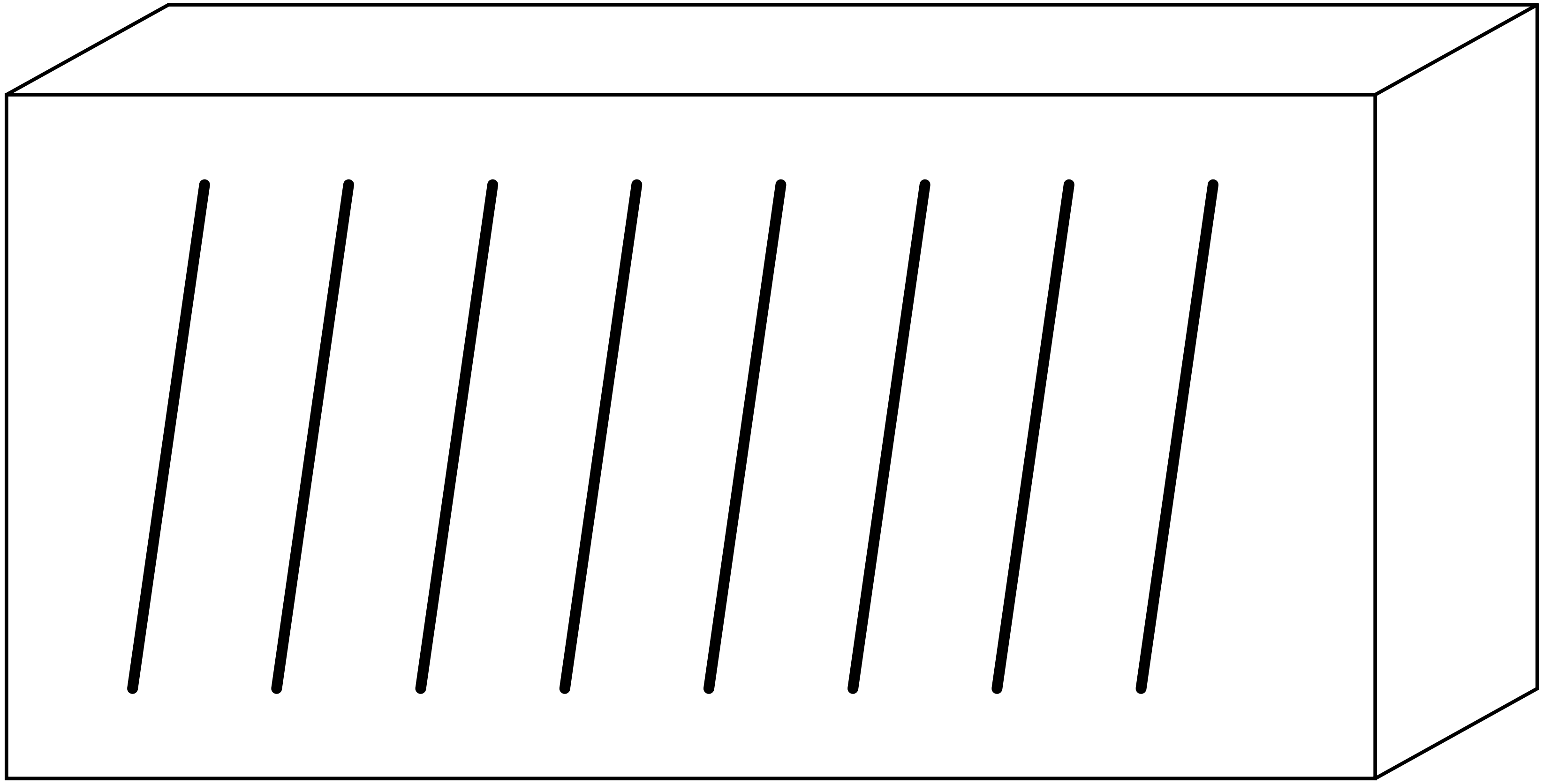
General Partitioning of 3-space

There are $q^3 + q^2 + q + 1$ points in finite projective 3-space, Σ.

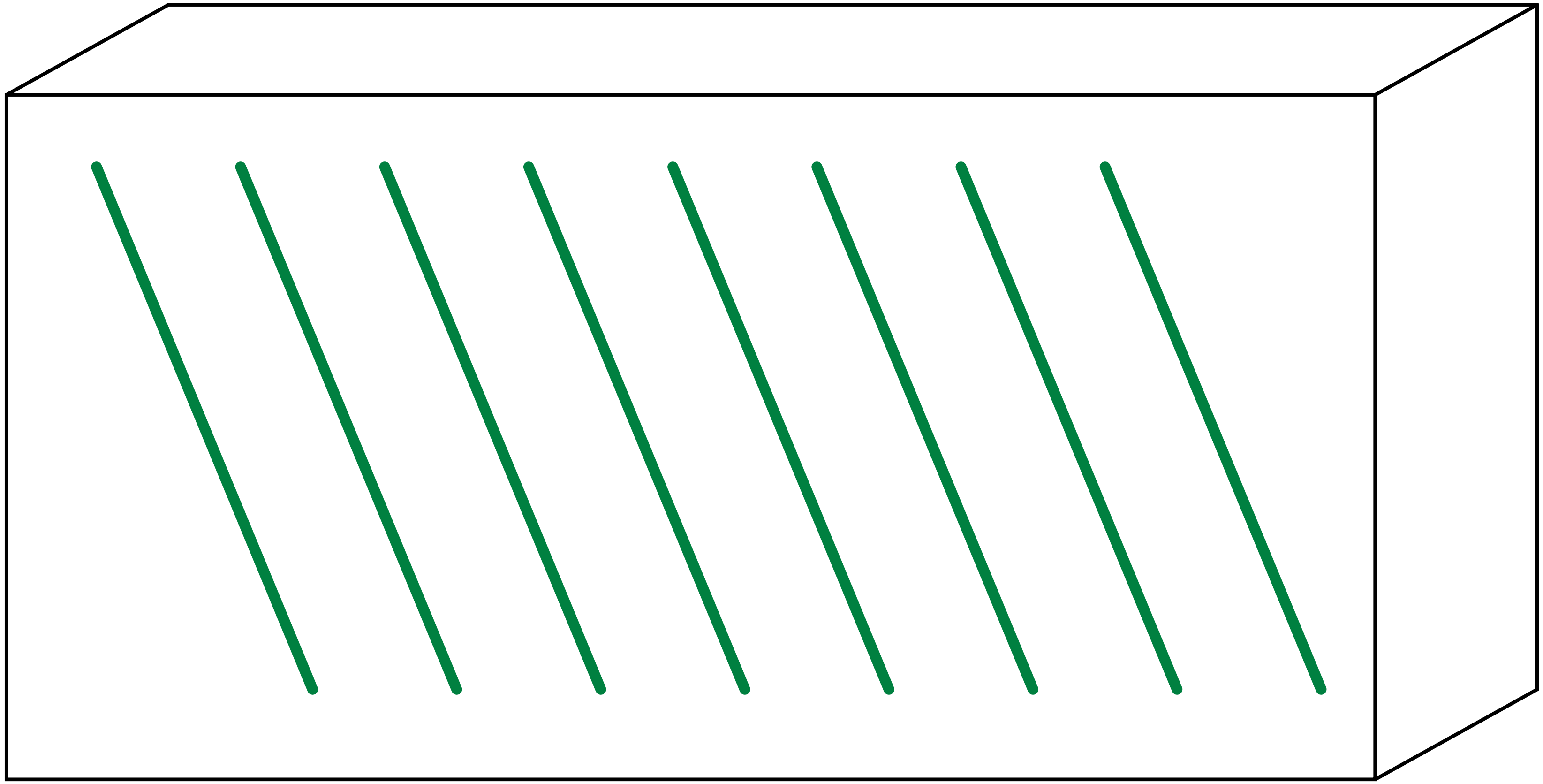
There are $q + 1$ points on each line of Σ.

A set of $q^2 + 1$ pairwise disjoint lines would then partition the points of Σ. Such a set is called a *spread*, and spreads have a close connection of finite affine translation planes, a big are of research for some people.

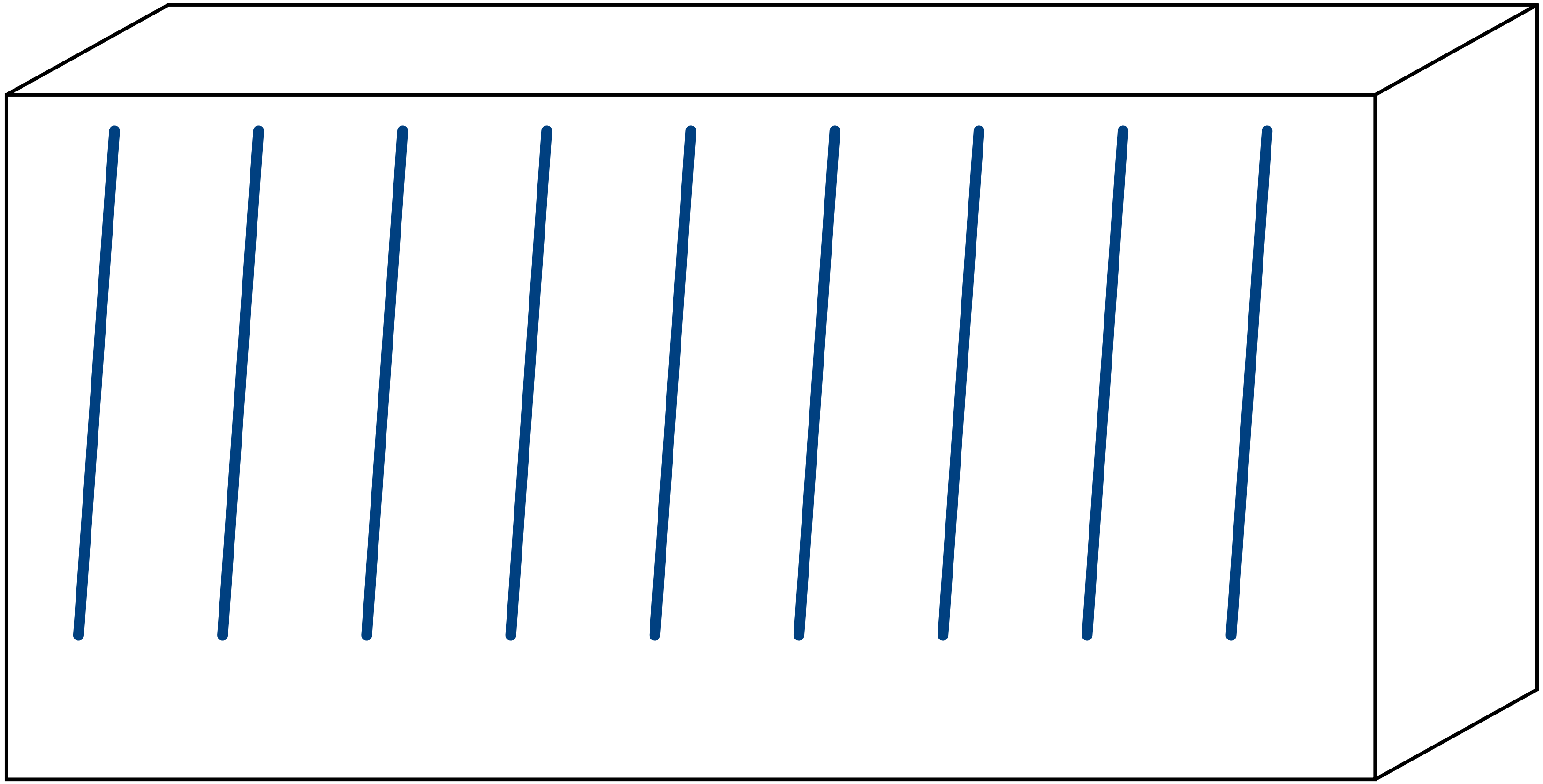
Packings



Packings



Packings



generalized solution

Spreads and packings of $PG(3, q)$, in general, give us a solution to a more generalized Kirkman Schoolgirls problem:

generalized solution

Spreads and packings of $PG(3, q)$, in general, give us a solution to a more generalized Kirkman Schoolgirls problem:

If $(q^2 + 1)(q + 1)$ *schoolgirls go walking each day in* $q^2 + 1$ *rows of* $q + 1$*, they can walk for* $q^2 + q + 1$ *days so that each girl has walked in the same row as has every other girl and hence with no girl twice.*

The Hat game

Three players enter a room and a red or white hat is placed on each person's head. The color of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others. Each person can see the other players' hats but not his own.

The Hat game

Three players enter a room and a red or white hat is placed on each person's head. The color of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others. Each person can see the other players' hats but not his own.

No communication of any sort is allowed, except for an initial strategy session before the game begins. Once they have had a chance to look at the other hats, the players must simultaneously guess the color of their own hats or pass.

The Hat game

Three players enter a room and a red or white hat is placed on each person's head. The color of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others. Each person can see the other players' hats but not his own.

No communication of any sort is allowed, except for an initial strategy session before the game begins. Once they have had a chance to look at the other hats, the players must simultaneously guess the color of their own hats or pass.

The group shares a hypothetical $3 million prize if at least one player guesses correctly and no players guess incorrectly. The problem is to find a strategy whereby the group's chance of winning exceeds 50%.

history

Mathematicians credit the Three Hats Game to Todd Ebert, a computer science professor at the University of California at Irvine.

history

Mathematicians credit the Three Hats Game to Todd Ebert, a computer science professor at the University of California at Irvine.

He introduced it in his Ph.D. thesis in 1998.

history

Mathematicians credit the Three Hats Game to Todd Ebert, a computer science professor at the University of California at Irvine.

He introduced it in his Ph.D. thesis in 1998.

The problem was then popularized by an April 2001 article in the *New York Times*.

NYT article

April 10, 2001

Why Mathematicians Now Care About Their Hat Color

By SARA ROBINSON

BERKELEY, Calif., April 9 — It takes a particularly clever puzzle to stump a mind accustomed to performing mental gymnastics.

So it's no ordinary puzzle that's spreading through networks of mathematicians like a juicy bit of gossip. Known as "the hat problem" in its most popular incarnation, this seemingly simple puzzle is consuming brain cycles at universities and research labs across the country and has become a vibrant topic of discussion on the Internet.

The reason this problem is so captivating, mathematicians say, is that it is not just a recreational puzzle to be solved and put away.

Rather, it has deep and unexpected connections to coding theory, an active area of mathematical research with broad applications in telecommunications and computer science.

In their attempts to devise a complete solution to the problem, researchers are proving new theorems in coding theory that may have applications well beyond mathematical puzzles.

"This puzzle is unique since it connects to unsolved mathematical questions," said Dr. Joe Buhler, deputy director of the Mathematical Sciences Research Institute here and a hat problem enthusiast.

The hat problem goes like this:

understanding codes

A linear code is simply a vector space over the binary alphabet. If the vectors all have n entries in them, we say the code has *length* n. The dimension of the code is denoted by k.

understanding codes

A linear code is simply a vector space over the binary alphabet. If the vectors all have n entries in them, we say the code has *length* n. The dimension of the code is denoted by k.

The last important parameter is the so-called *minimum distance* of the code.

understanding codes

A linear code is simply a vector space over the binary alphabet. If the vectors all have n entries in them, we say the code has *length* n. The dimension of the code is denoted by k.

The last important parameter is the so-called *minimum distance* of the code.

The distance between two codewords is the number of coordinate positions where they differ. The minimum value, taken over all codewords in the code, is called the minimum distance.

Hamming code of length 3

$$\{(0,0,0),(1,1,1)\}$$

Hamming code of length 3

$$\{(0,0,0),(1,1,1)\}$$

Suppose the vector $(1,0,0)$ is received.

Hamming code of length 3

$$\{(0,0,0),(1,1,1)\}$$

Suppose the vector $(1,0,0)$ is received. It will be decoded as $(0,0,0)$.

Hamming code of length 3

$$\{(0,0,0),(1,1,1)\}$$

Suppose the vector $(1,0,0)$ is received. It will be decoded as $(0,0,0)$.

KEY: For Hamming codes, every vector is either a codeword, or is distance 1 from a codeword.

Hamming code of length 15

Let's redo the game now with 15 players (maybe even Schoolgirls!)

Hamming code of length 15

Let's redo the game now with 15 players (maybe even Schoolgirls!)

After receiving their hats, they line up and each girl looks at the row, associated the sequence of red and white hats with a binary vector of length 15.

Hamming code of length 15

Let's redo the game now with 15 players (maybe even Schoolgirls!)

After receiving their hats, they line up and each girl looks at the row, associated the sequence of red and white hats with a binary vector of length 15.

They each ask themselves the question:

Hamming code of length 15

Let's redo the game now with 15 players (maybe even Schoolgirls!)

After receiving their hats, they line up and each girl looks at the row, associated the sequence of red and white hats with a binary vector of length 15.

They each ask themselves the question:

If I had a red/white hat, would we be a codeword?

Hamming code of length 15

Let's redo the game now with 15 players (maybe even Schoolgirls!)

After receiving their hats, they line up and each girl looks at the row, associated the sequence of red and white hats with a binary vector of length 15.

They each ask themselves the question:

If I had a red/white hat, would we be a codeword?

Players assume that "they" are not in the code and answer accordingly...

to guess or not to guess...

If wearing white makes them a codeword, then the player guesses red.

If wearing red makes them a codeword, then the player guesses white.

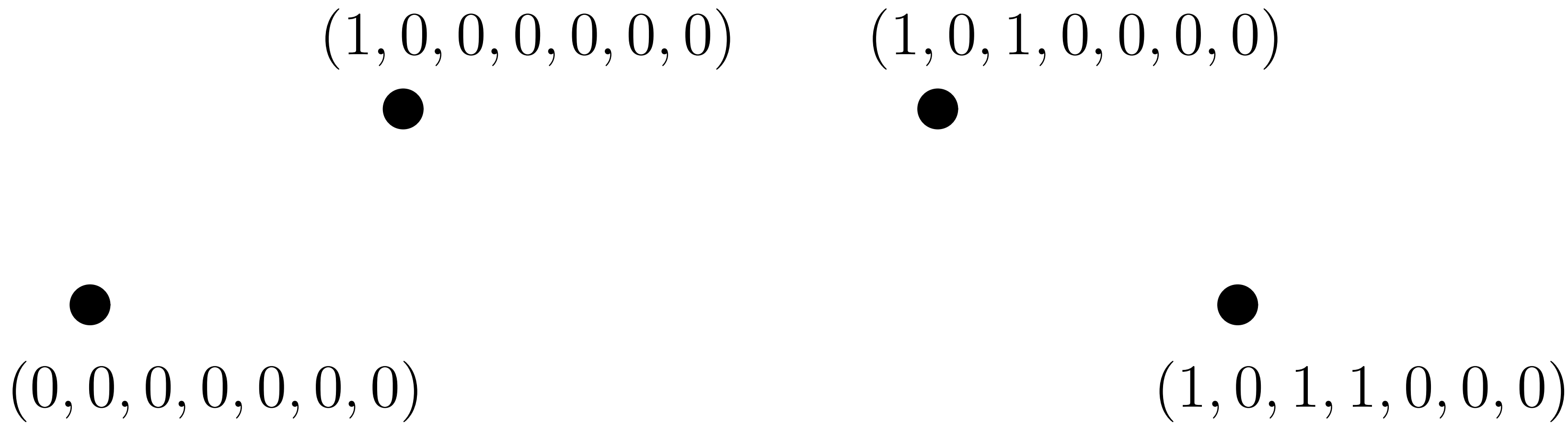
If neither color makes them a codeword, then the player passes.

how does it work?

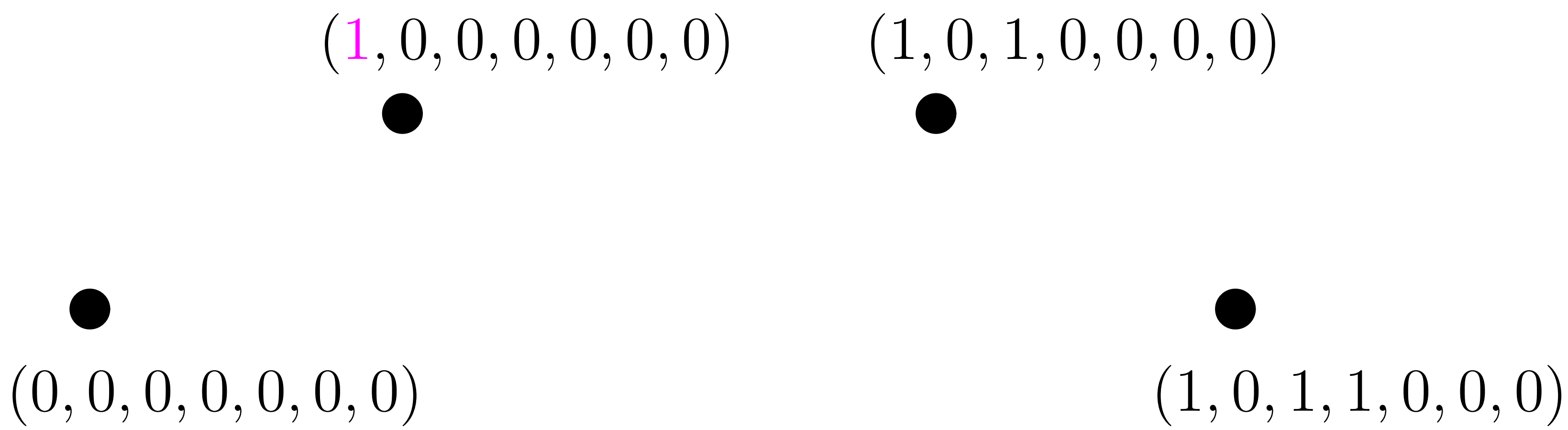
●
$(0, 0, 0, 0, 0, 0, 0)$

●
$(1, 0, 1, 1, 0, 0, 0)$

how does it work?



how does it work?



how does it work?

❖ Kirkman's Problem
❖ Block Designs
❖ Algebraic Fields
❖ Finite Geometry
❖ **Hamming Codes**
❖ Conclusions

$(1,0,0,0,0,0,0)$ $(1,0,1,0,0,0,0)$

$(0,0,0,0,0,0,0)$ $(1,0,1,1,0,0,0)$

how does it work?

$(1, 0, 0, 0, 0, 0, 0)$ $(1, 0, 1, 0, 0, 0, 0)$

$(0, 0, 0, 0, 0, 0, 0)$ $(1, 0, 1, 1, 0, 0, 0)$

how does it work?

$(1, 0, 0, 0, 0, 0, 0)$

$(1, 0, 1, 0, 0, 0, 0)$

$(0, 0, 0, 0, 0, 0, 0)$

$(1, 0, 1, 1, 0, 0, 0)$

chances of success

The team will win precisely when they are wearing a color combination that determines a binary vector **not** lying in the Hamming code.

chances of success

The team will win precisely when they are wearing a color combination that determines a binary vector **not** lying in the Hamming code.

In general, Hamming codes have length $2^r - 1$ and the dimension of the code is $2^r - r - 1$. With 15 players, $r = 4$. So, the probability of losing is

chances of success

The team will win precisely when they are wearing a color combination that determines a binary vector **not** lying in the Hamming code.

In general, Hamming codes have length $2^r - 1$ and the dimension of the code is $2^r - r - 1$. With 15 players, $r = 4$. So, the probability of losing is

$$\frac{2^{11}}{2^{15}} = \frac{1}{2^4} = \frac{1}{16}.$$

chances of success

The team will win precisely when they are wearing a color combination that determines a binary vector **not** lying in the Hamming code.

In general, Hamming codes have length $2^r - 1$ and the dimension of the code is $2^r - r - 1$. With 15 players, $r = 4$. So, the probability of losing is

$$\frac{2^{11}}{2^{15}} = \frac{1}{2^4} = \frac{1}{16}.$$

In general, the probability of losing with $2^r - 1$ players is only $\frac{1}{2^r}$.

one missing hole

one missing hole

How do the girls know *how* to line up?

one missing hole

How do the girls know *how* to line up?

Here's where the solution to the hats problem falls back to the solution to the Kirkman Schoolgirls problem.

one missing hole

How do the girls know *how* to line up?

Here's where the solution to the hats problem falls back to the solution to the Kirkman Schoolgirls problem.

In fact, the association will tie all of the solutions together!

one missing hole

Integers: $\{1, 2, ..., 15\}$

one missing hole

Integers: $\{1, 2, ..., 15\}$

$$\Updownarrow$$

4-bit long bitstrings: $\{[0001], [0010], [0011], ..., [1111]\}$

one missing hole

Integers: $\{1, 2, ..., 15\}$

$\Updownarrow$

4-bit long bitstrings: $\{[0001], [0010], [0011], ..., [1111]\}$

$\Updownarrow$

points of $PG(3, 2)$

one missing hole

Integers: $\{1, 2, ..., 15\}$

$\Updownarrow$

4-bit long bitstrings: $\{[0001], [0010], [0011], ..., [1111]\}$

$\Updownarrow$

points of $PG(3, 2)$

$\Updownarrow$

quadratic subfields of K:

one missing hole

- Kirkman's Problem
- Block Designs
- Algebraic Fields
- Finite Geometry
- **Hamming Codes**
- Conclusions

Integers: $\{1, 2, ..., 15\}$

$$\Updownarrow$$

4-bit long bitstrings: $\{[0001], [0010], [0011], ..., [1111]\}$

$$\Updownarrow$$

points of $PG(3, 2)$

$$\Updownarrow$$

quadratic subfields of K:

$$[b_1 b_2 b_3 b_4] \leftrightarrow \mathbb{Q}(\sqrt{2^{b_1} 3^{b_2} 5^{b_3} 7^{b_4}})$$

one missing hole

Integers: $\{1, 2, ..., 15\}$

$\Updownarrow$

4-bit long bitstrings: $\{[0001], [0010], [0011], ..., [1111]\}$

$\Updownarrow$

points of $PG(3, 2)$

$\Updownarrow$

quadratic subfields of K:

$$[b_1 b_2 b_3 b_4] \leftrightarrow \mathbb{Q}(\sqrt{2^{b_1} 3^{b_2} 5^{b_3} 7^{b_4}})$$

Under this ordering, the 3-tuples of integers generate the codewords in the Hamming code!

If you like what you've heard, you may be interested in reading the article

KIRKMAN'S SCHOOLGIRLS WEARING HATS AND WALKING THROUGH FIELDS OF NUMBERS

by Ezra Brown and Keith E. Mellinger

freely available on the MAA website.

- ❖ Kirkman’s Problem
- ❖ Block Designs
- ❖ Algebraic Fields
- ❖ Finite Geometry
- ❖ Hamming Codes
- ❖ Conclusions

Questions?