# *The Polynomial Method*

I’m going to talk about this particular mathematical proof technique —- the Polynomial Method —- and at the end, discuss how feasible it might be to formalize or automate it.

## Talk Outline

- What the polynomial method is and why we care
- Two different proofs that utilize the polynomial method
- Discussion on potential formalization or automation of this method

I'll start by talking about what the method is, spend the majority of the talk delving into two different proofs that use this method, and we can conclude by discussing applications of automated theorem proving to this method.

# What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

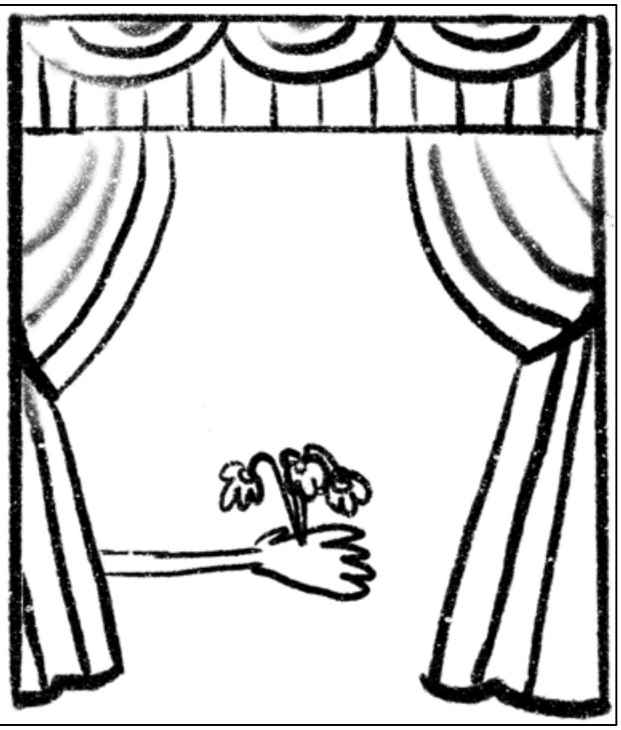
The polynomial method is a single proof technique that's proved a whole lot of theorems, mostly in combinatorics.

## What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

It involves...

1. Taking a combinatorics problem



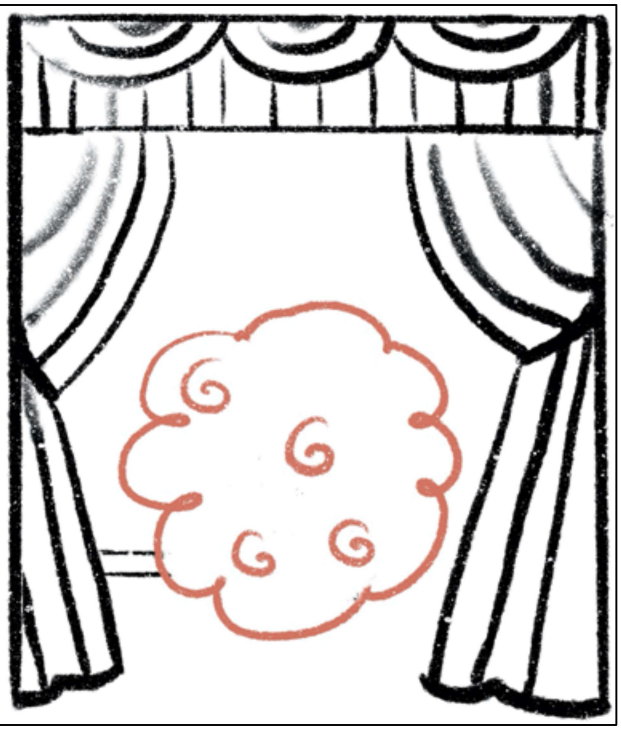
The technique involves starting with some problem in combinatorics...

## What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

It involves...

1. Taking a combinatorics problem and turning it into a problem about polynomial



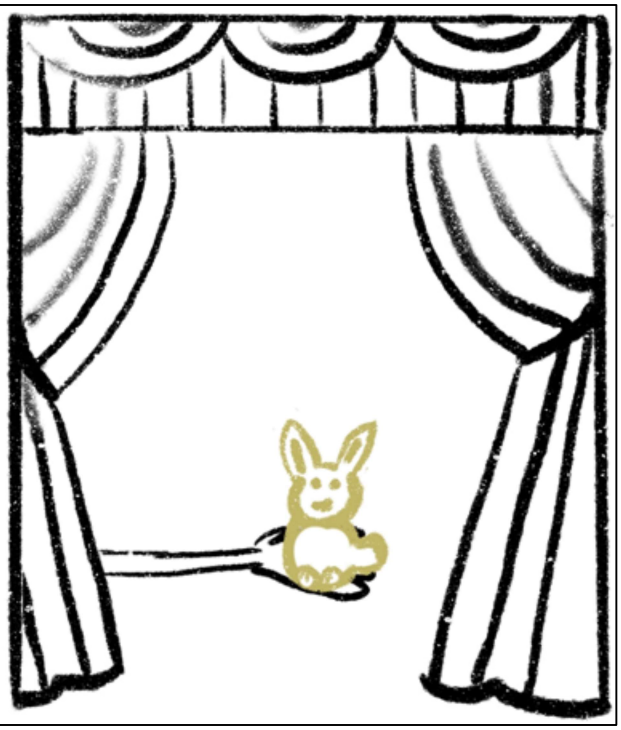
...and then reducing the problem to a problem that has to do with a polynomial.

# What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

It involves...

1. Taking a combinatorics problem and turning it into a problem about polynomial

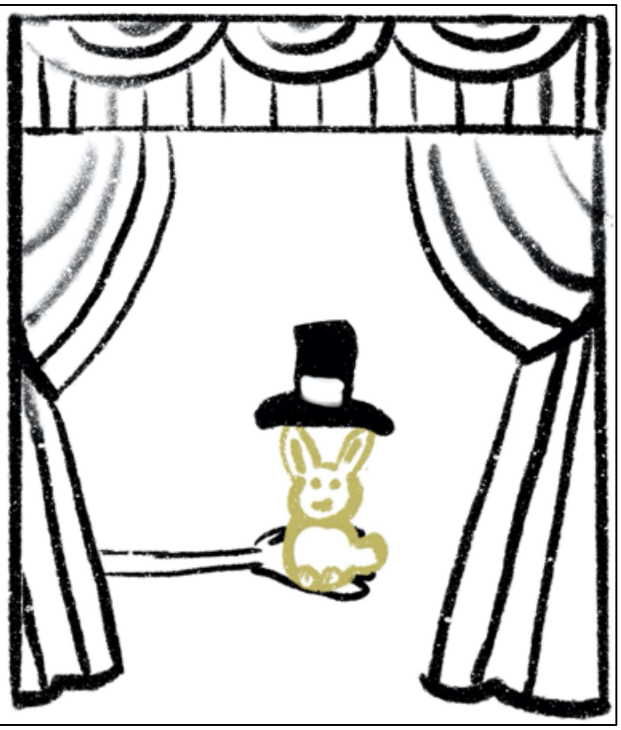


## What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

It involves...

1. Taking a combinatorics problem and turning it into a problem about polynomial
2. Finding some properties out about the polynomial



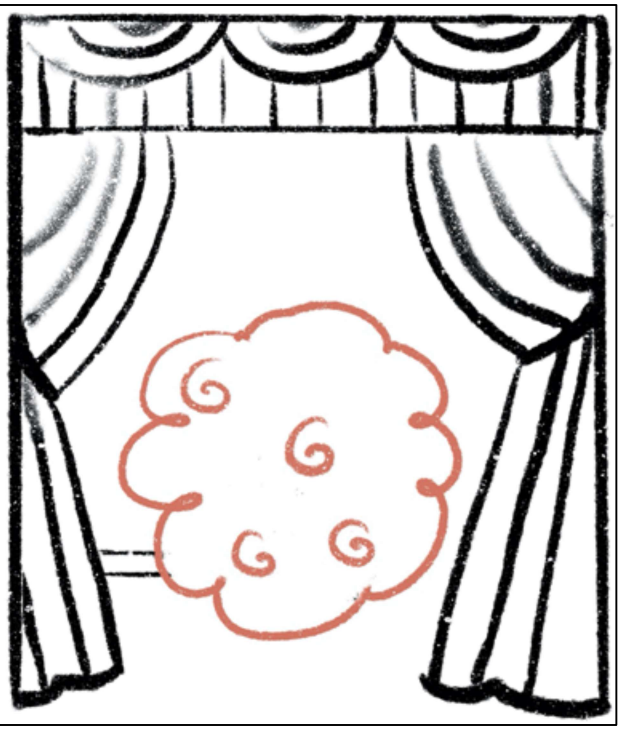
Then, we figure out some properties of the polynomial (often involving where the polynomial equals zero).

## What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

It involves...

1. Taking a combinatorics problem and turning it into a problem about polynomial
2. Finding some properties out about the polynomial
3. Turning the polynomial problem back into the original combinatorics problem



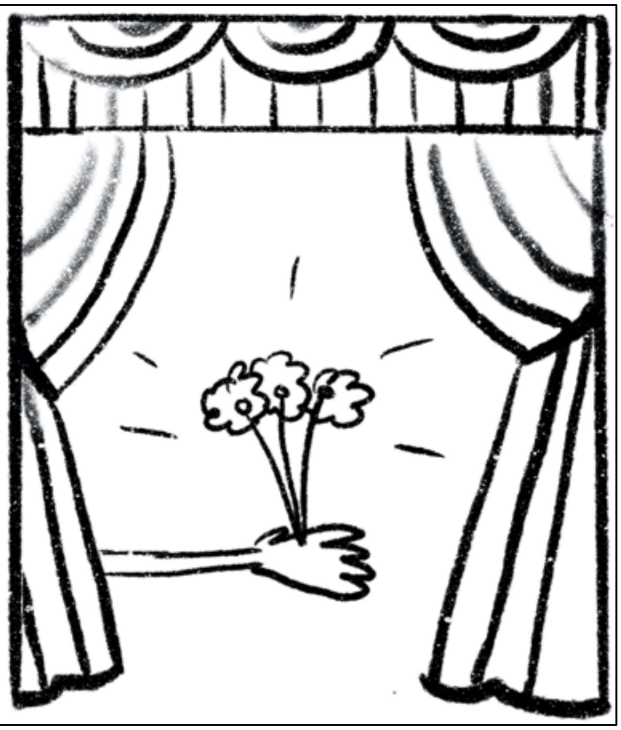
And then, we use that information to deduce some information about the original combinatorics problem.

# What it is

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems.**

It involves...

1. Taking a combinatorics problem and turning it into a problem about polynomial
2. Finding some properties out about the polynomial
3. Turning the polynomial problem back into the original combinatorics problem



## Why it's impressive

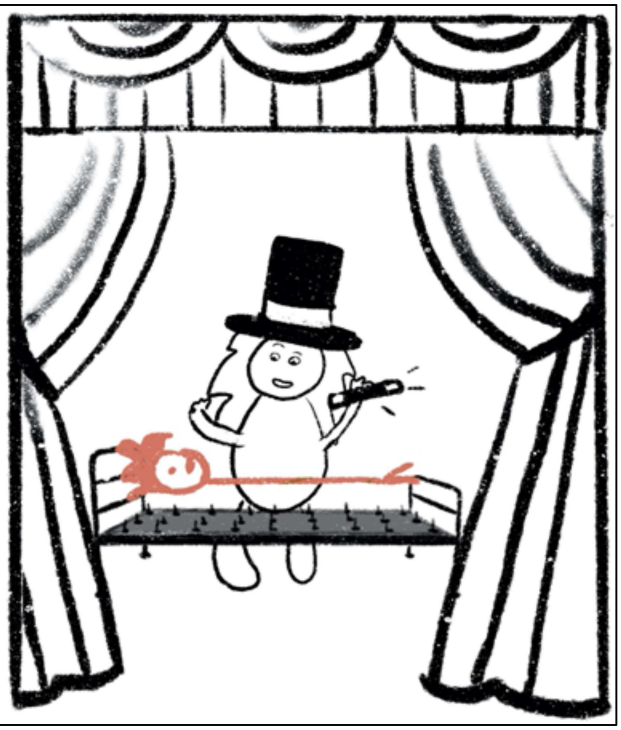
The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems** (often long standing open problems, and often with one-page-or-less proofs). For example...

And so why do we care? It seems pretty powerful. It's only been out in its current form for about 10 years, and already it has solved some long-standing open problems (many with proofs less than a page long).

# Why it's impressive

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems** (often long standing open problems, and often with one-page-or-less proofs). For example...

- ***Finite Field Kakeya Conjecture*** **(Geometric measure theory)**
  - Let $F$ be a finite field, let $K \subseteq F^n$ be a Kakeya set, i.e. for each vector $y \in F^n$ there exists $x \in F^n$ such that $K$ contains a line $\{x + ty : t \in F\}$. What's the minimum size of such a set?
  - **Open since 1999, solved in 2008 with the polynomial method.**

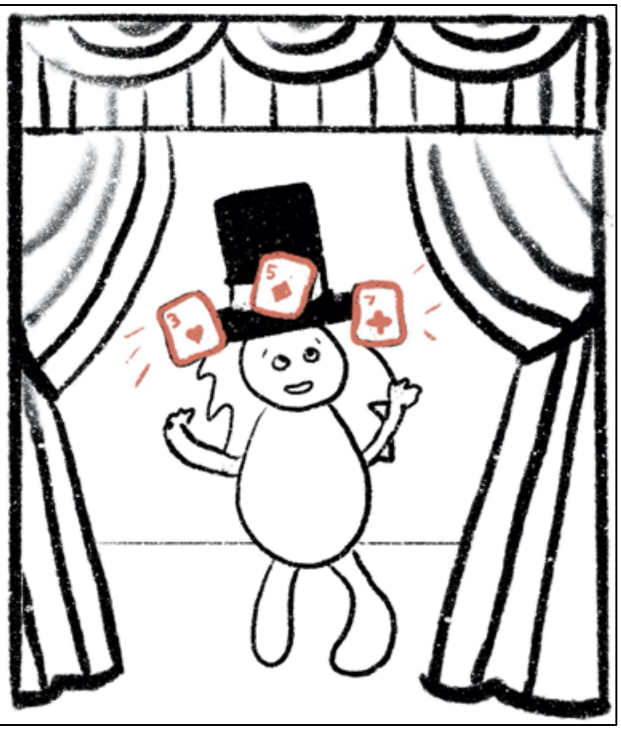


For example...

# Why it's impressive

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems** (often long standing open problems, and often with one-page-or-less proofs). For example...

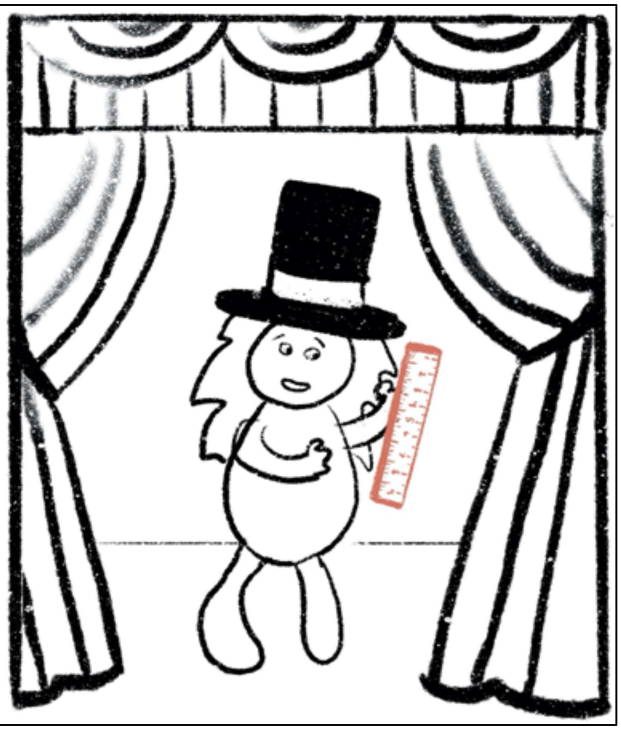
- *Finite Field Kakeya Conjecture* (Geometric measure theory)
  - Let $F$ be a finite field, let $K \subseteq F^n$ be a Kakeya set, i.e. for each vector $y \in F^n$ there exists $x \in F^n$ such that $K$ contains a line $\{x + by : t \in F\}$. What's the minimum size of such a set?
  - Open since 1999, solved in 2008 with the polynomial method.
- *Cap set problem* (Additive number theory)
  - A cap set is a subset of $Z_3^n$ with no three-element arithmetic progressions. What's the size of the largest possible cap set?
  - Open since 1971, mostly-solved in 2016 with the polynomial method.



# Why it's impressive

The polynomial method is a **single proof technique** that's been used to solve a bunch of **seemingly unrelated combinatorics problems** (often long standing open problems, and often with one-page-or-less proofs). For example...

- *Finite Field Kakeya Conjecture* (Geometric measure theory)
  - Let $F$ be a finite field, let $K \subseteq F^n$ be a Kakeya set, i.e. for each vector $y \in F^n$ there exists $x \in F^n$ such that $K$ contains a line $\{x + ty : t \in F\}$. What's the minimum size of such a set?
  - Open since 1999, solved in 2008 with the polynomial method.
- *Cap set problem* (Additive number theory)
  - A cap set is a subset of $Z_3^n$ with no three-element arithmetic progressions. What's the size of the largest possible cap set?
  - Open since 1971, mostly-solved in 2016 with the polynomial method.
- *Erdos distance problem* (Combinatorial incidence geometry)
  - Does every set of points in the plane have a nearly-linear number of distinct distances?
  - Open since 1946, mostly-solved in 2015 with the polynomial method.



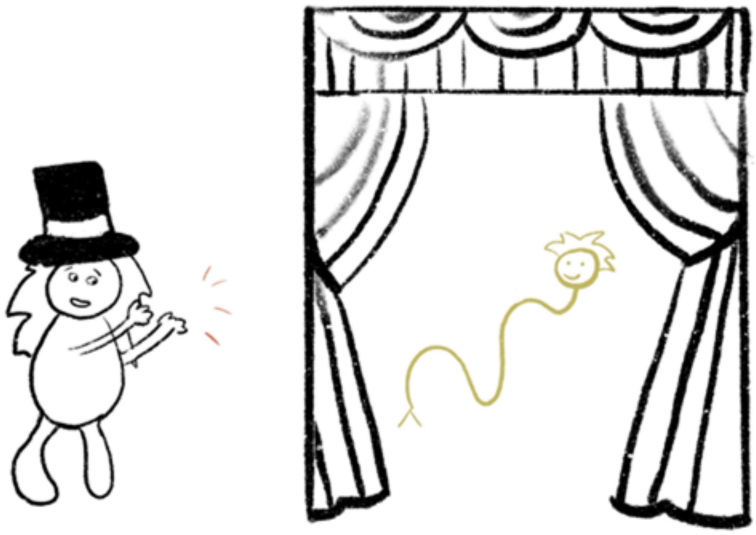
## The point of this talk

- If we wanted to make a tool that helped mathematicians solve problems using the polynomial method, what should that tool be?

And so the point of this talk is to get everybody's ideas on a question I've been asking myself: If we wanted to make a tool that helped mathematicians solve problems using the polynomial method, what should that tool be? (And yes, this is quite a vague, open-ended question...)

But in any case, while you guys are thinking about that, I'm going to go over some details of proofs that use this technique, and maybe it will inspire us.

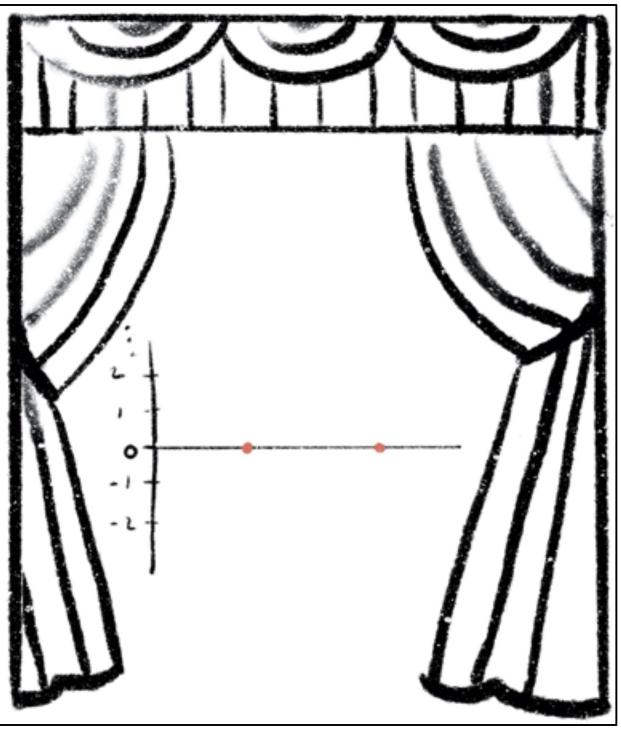
## Some key lemmas used in the polynomial method



The polynomial method is essentially a successive application of several important lemmas. Some key ones are as follows...

## Some key lemmas used in the polynomial method

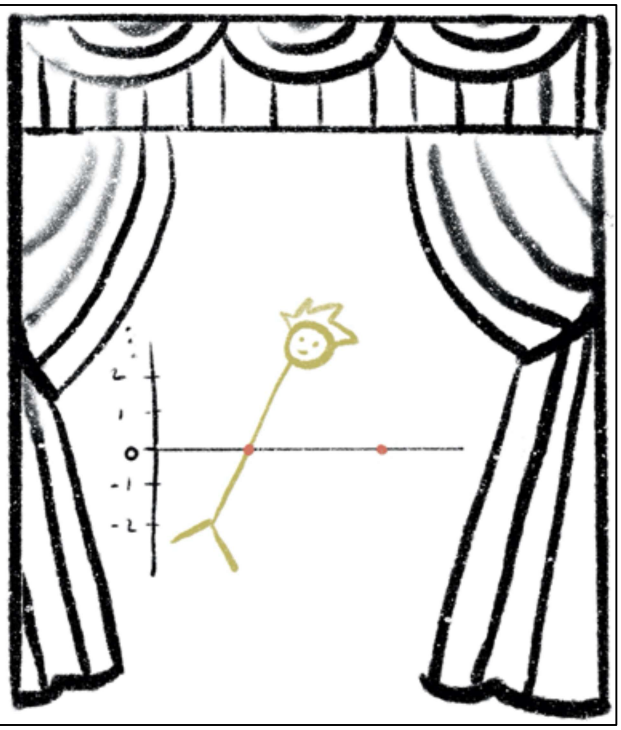
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



The first of these is the Vanishing lemma, which, roughly stated, means that if a polynomial vanishes too many times, it vanishes everywhere.

## Some key lemmas used in the polynomial method

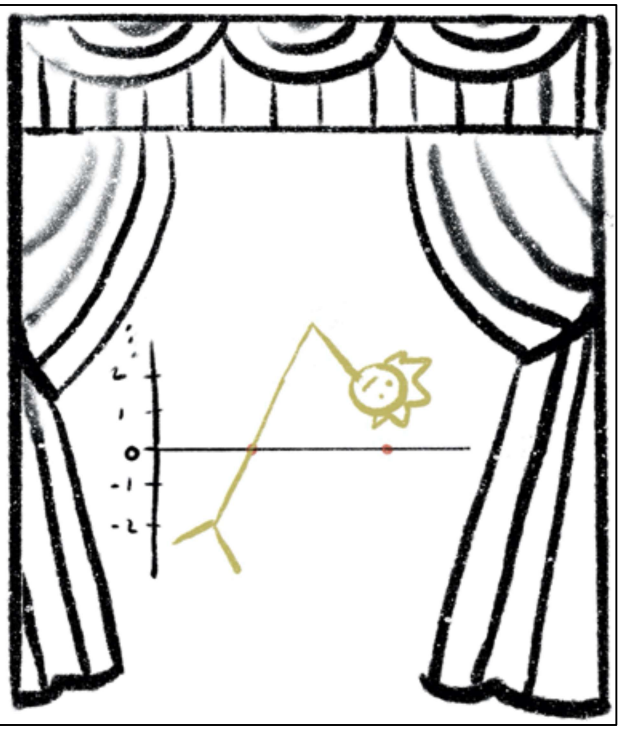
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



We already have an intuitive sense of this. For example, if we have a line, we can make it zero at any one point.

## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



But if we try to make that line zero at two points...

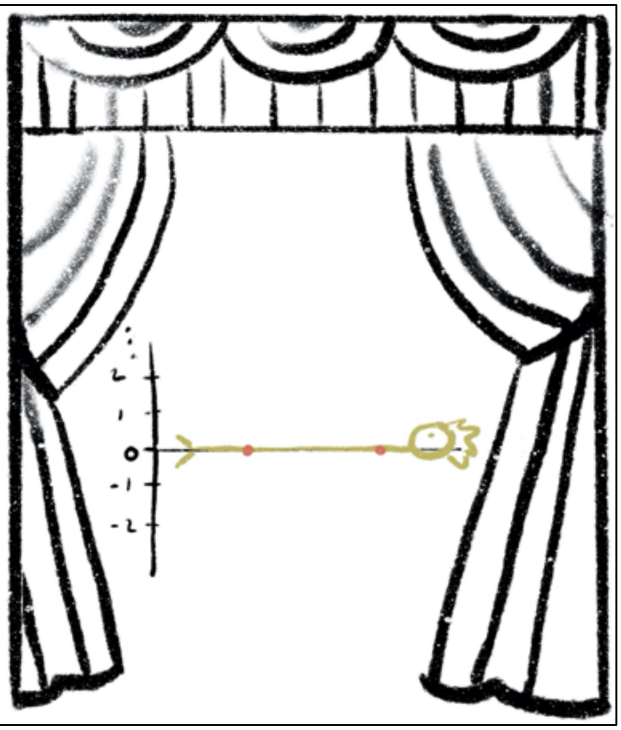
## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.


It vanishes...

## Some key lemmas used in the polynomial method

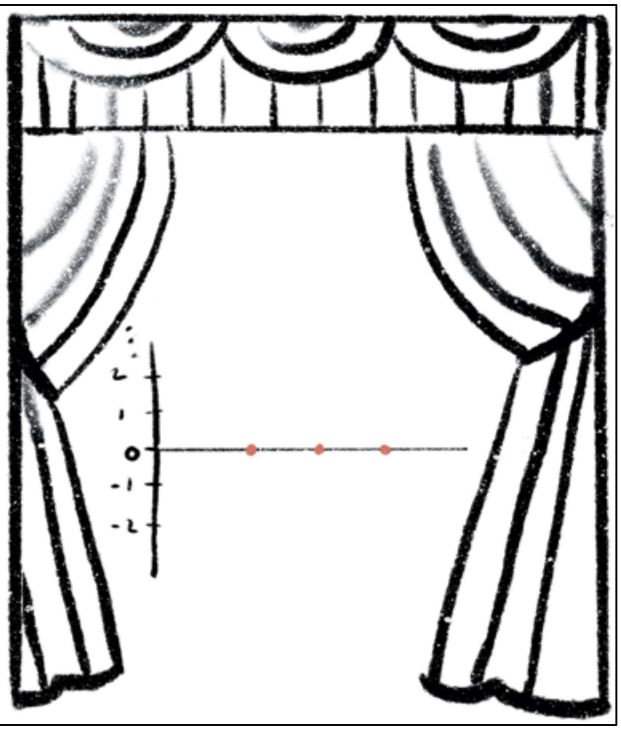
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



And is actually the zero function.

## Some key lemmas used in the polynomial method

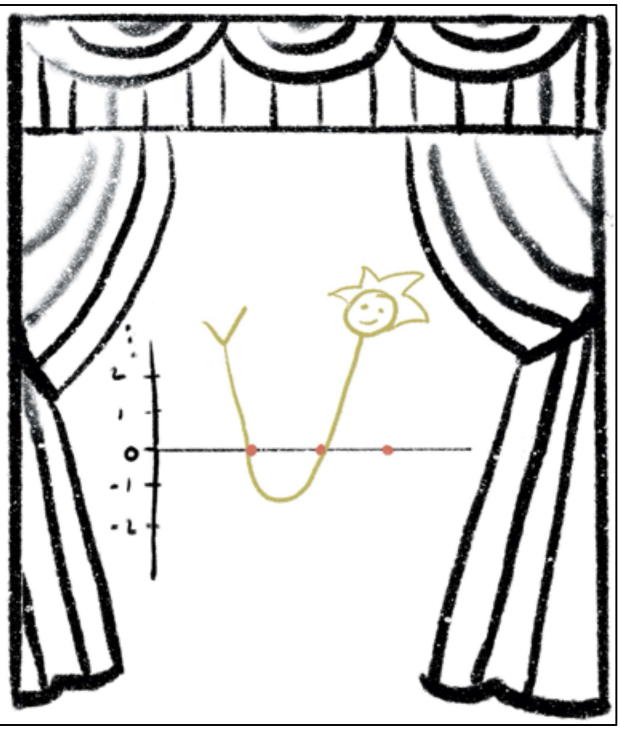
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



A similar phenomenon happens with higher degree polynomials.

## Some key lemmas used in the polynomial method

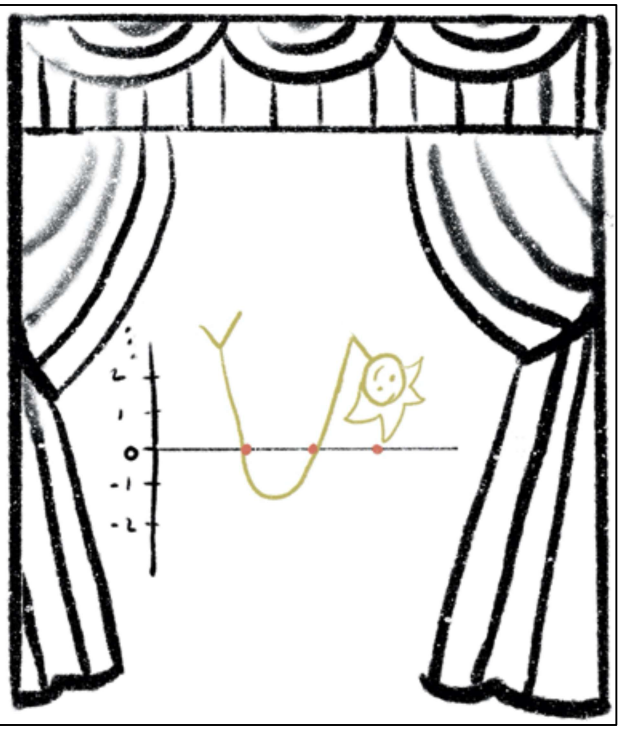
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



We know we can make a quadratic zero at any two points.

## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



...but as soon as we try to make it zero at three points...

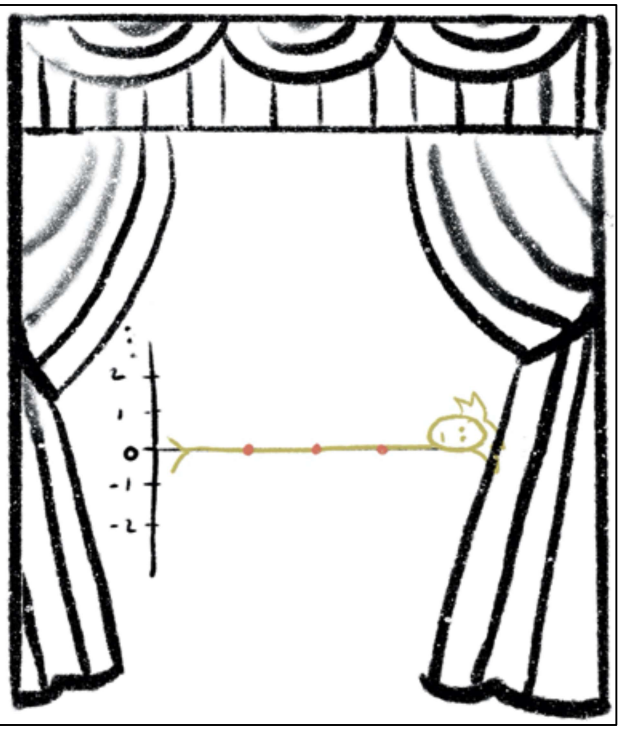
## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.


...it vanishes...

## Some key lemmas used in the polynomial method

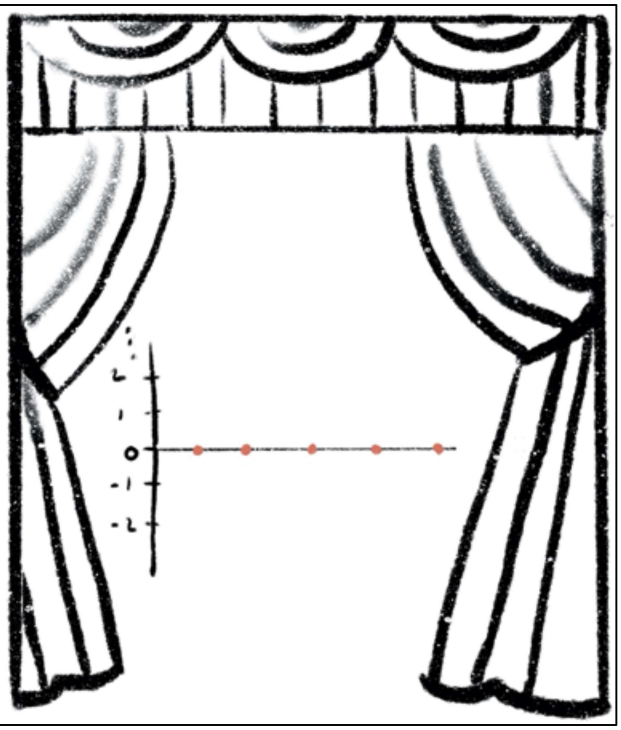
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.



...and becomes the zero polynomial.

## Some key lemmas used in the polynomial method

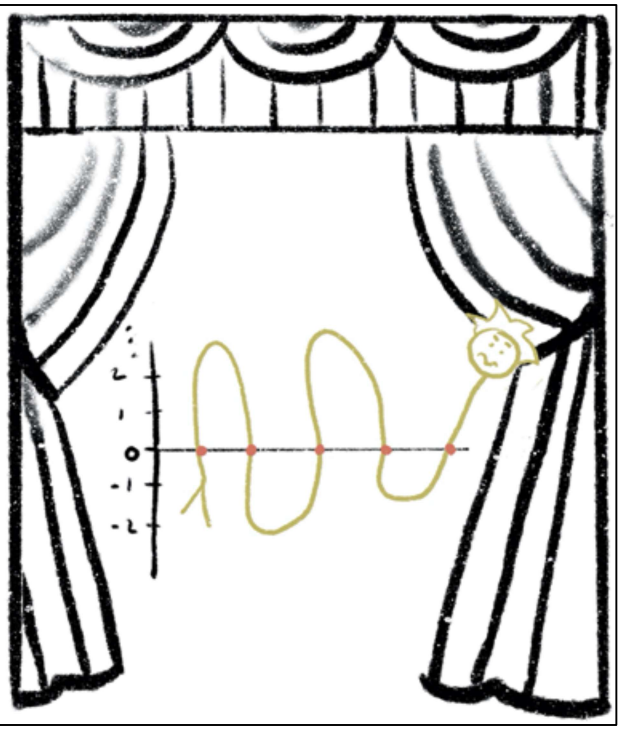
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.



We can generalize this statement further...

## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.



...and say that if we try to make a d-degree polynomial vanish on q points in a finite field where d < q, then...

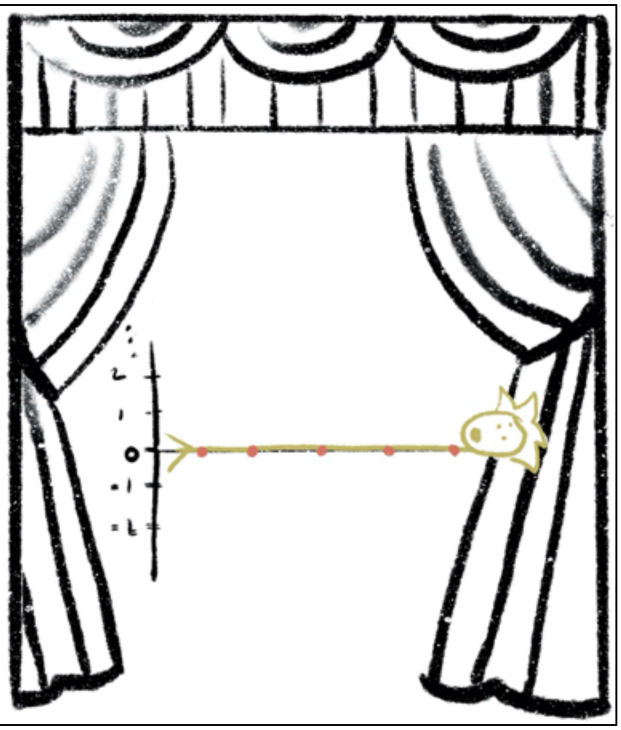
## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.


...the polynomial vanishes everywhere...

## Some key lemmas used in the polynomial method

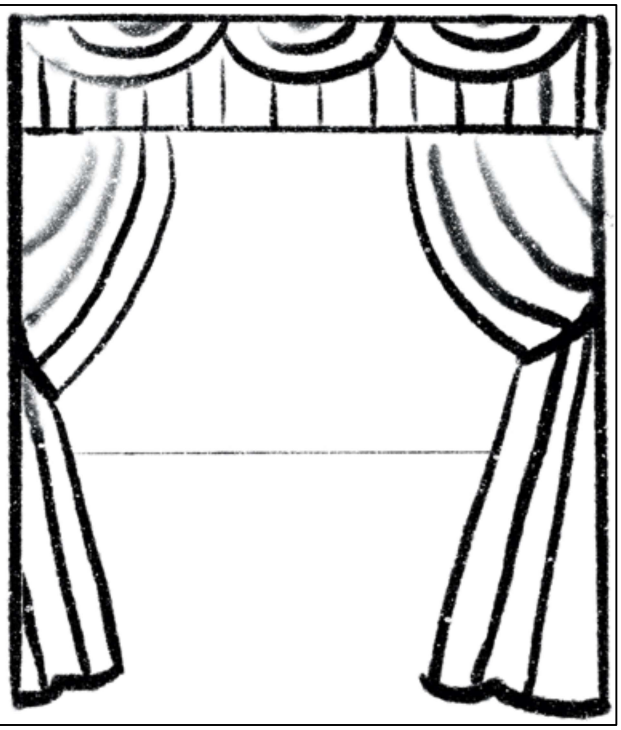
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.



...and is the zero polynomial.

## Some key lemmas used in the polynomial method

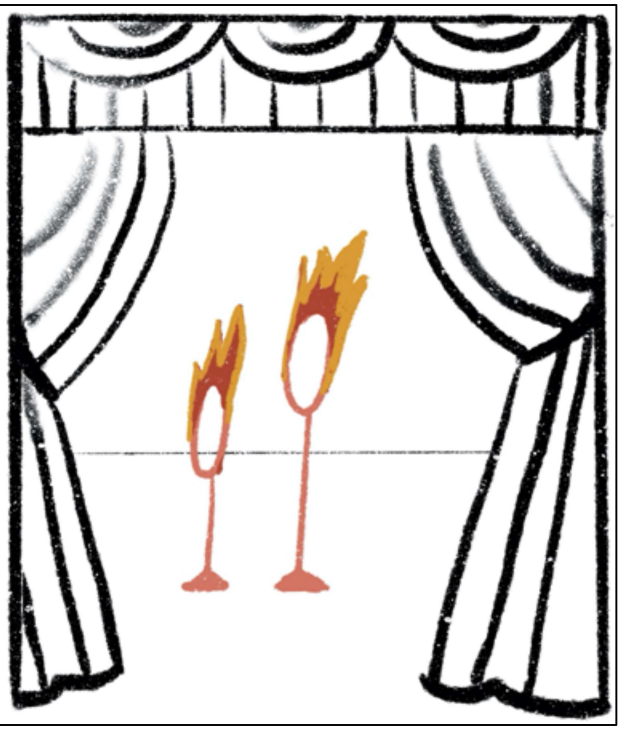
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



The next important lemma that is often used when applying the polynomial method is the Interpolation lemma.
Again loosely stated, it says that if we're given few enough points, we can find a low-degree polynomial that passes through all of them.

## Some key lemmas used in the polynomial method

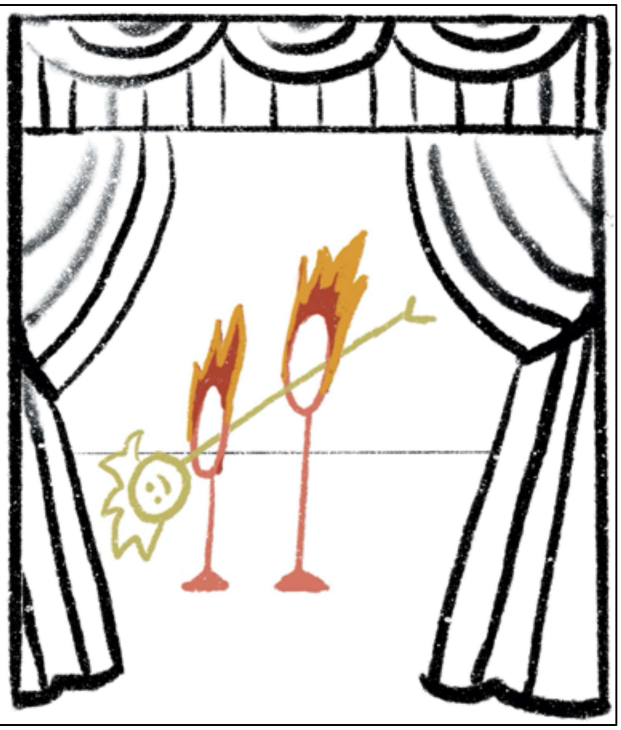
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



We also have an intuitive understanding of this. For example, we know that given any two points...

## Some key lemmas used in the polynomial method

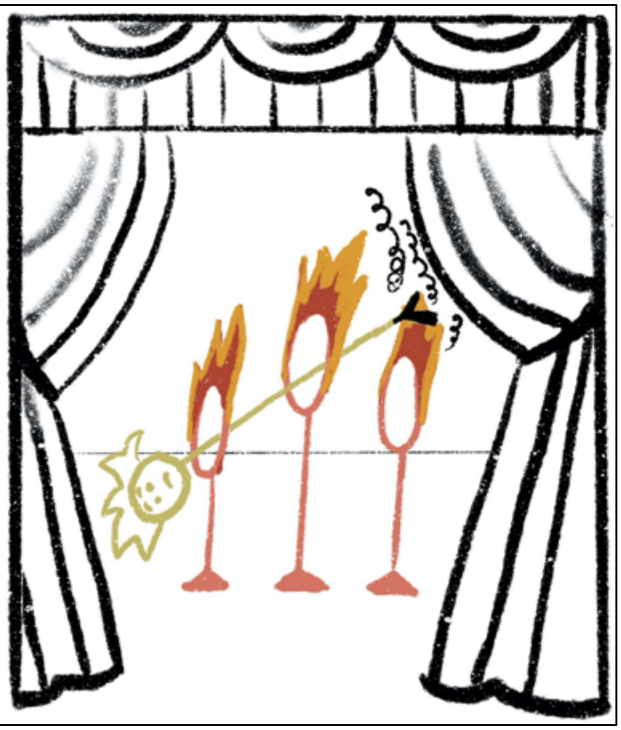
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



...we can always find a line that passes through both of them.

## Some key lemmas used in the polynomial method

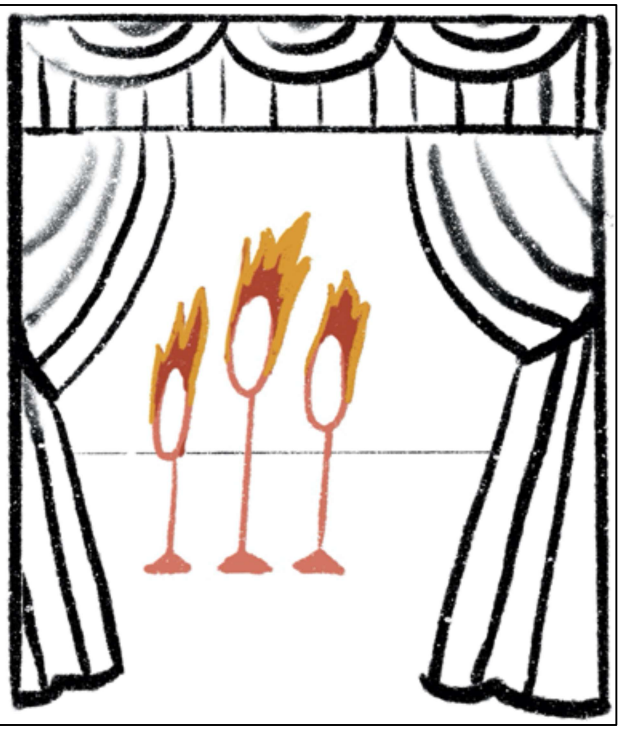
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



However, if we're given any three points, there's no guarantee that we can make a line go through all of them.

## Some key lemmas used in the polynomial method

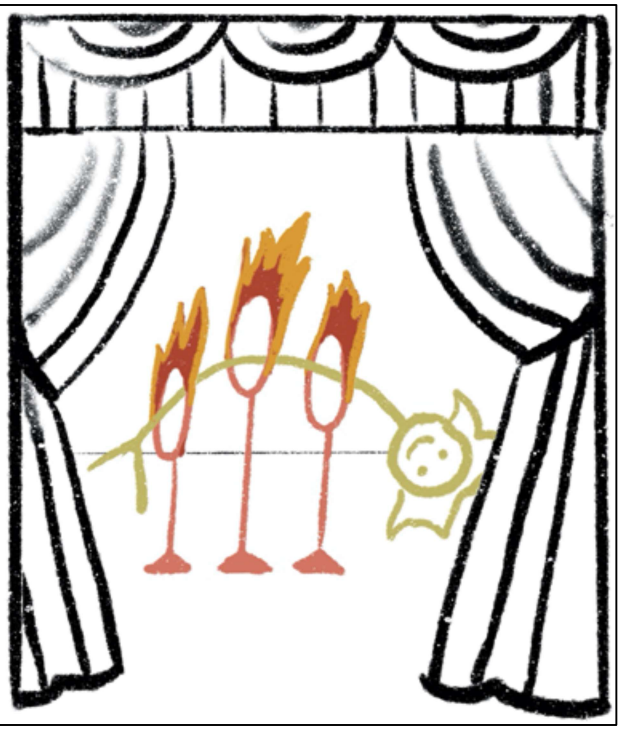
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



But now say you're given any three points...

## Some key lemmas used in the polynomial method

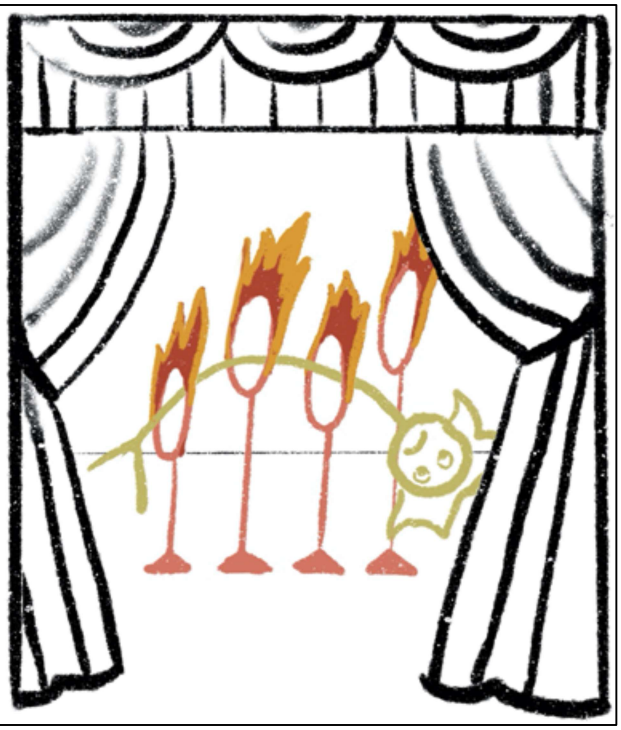
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



...and you need a quadratic to go through all of them. We can do that.

## Some key lemmas used in the polynomial method

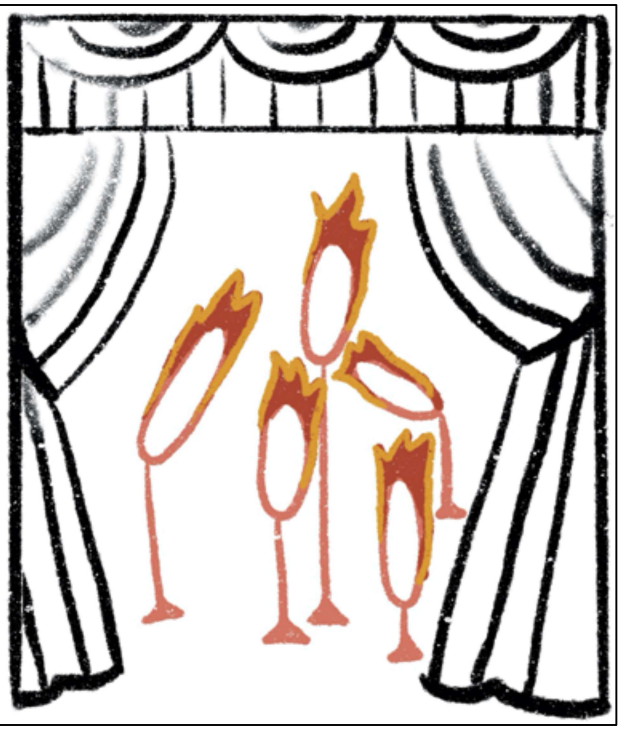
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.



But now again, if we're given any four points, there's no guarantee that we can make a quadratic go through all of them.

## Some key lemmas used in the polynomial method

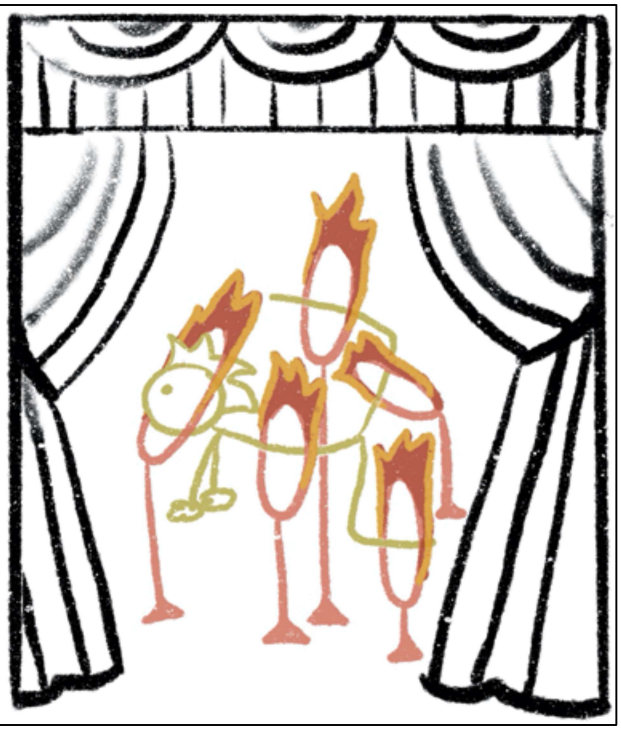
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where $d < q$, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.



The general version of this statement is as follows.

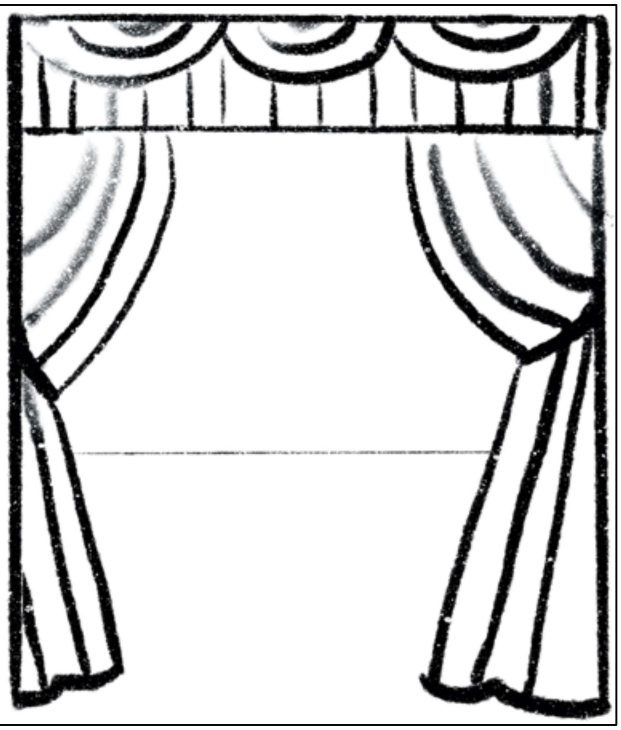
# Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where $d < q$, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.



## Some key lemmas used in the polynomial method

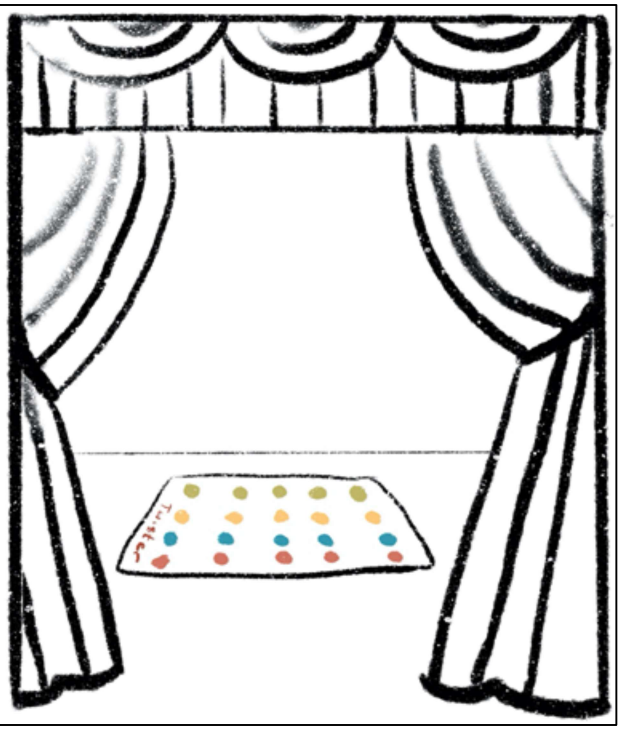
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.



The last key lemma of the polynomial method that I'll discuss here is called the rigidity lemma. It's called this way because, roughly stated again, it means that once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place, and then the only points the line passes through must be roots of that polynomial.

## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.

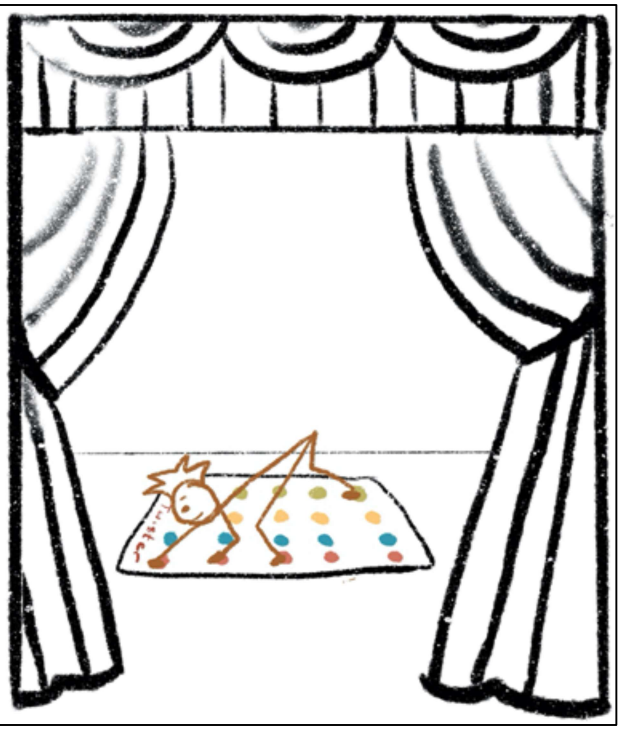


So, we can consider the n-dimensional vector space F^n over the finite field F.

And then we consider an n-variable F-polynomial (a n-variable polynomial whose coefficients lie in F) defined on that vector space. More formally, P is an element of F[X_1, X_2,...X_n].

## Some key lemmas used in the polynomial method

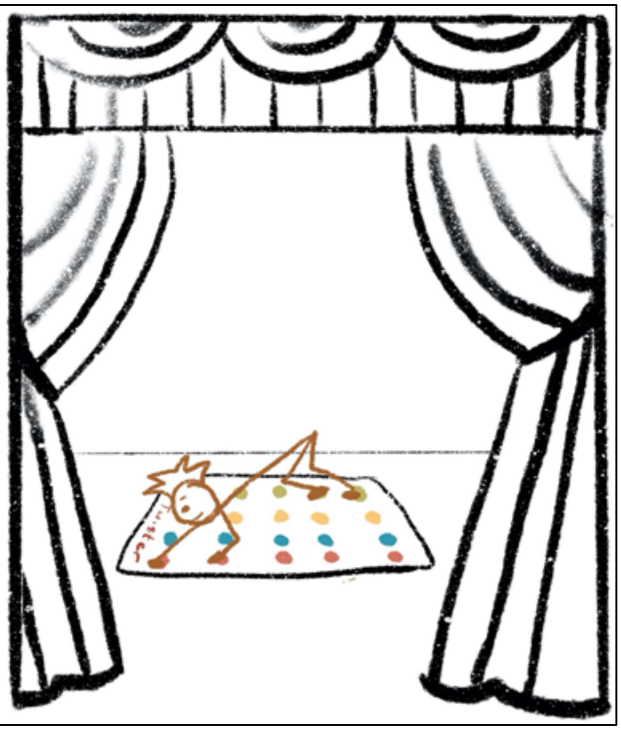
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where $d < q$, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.



Then maybe that a line can go through one root of that polynomial...

# Some key lemmas used in the polynomial method

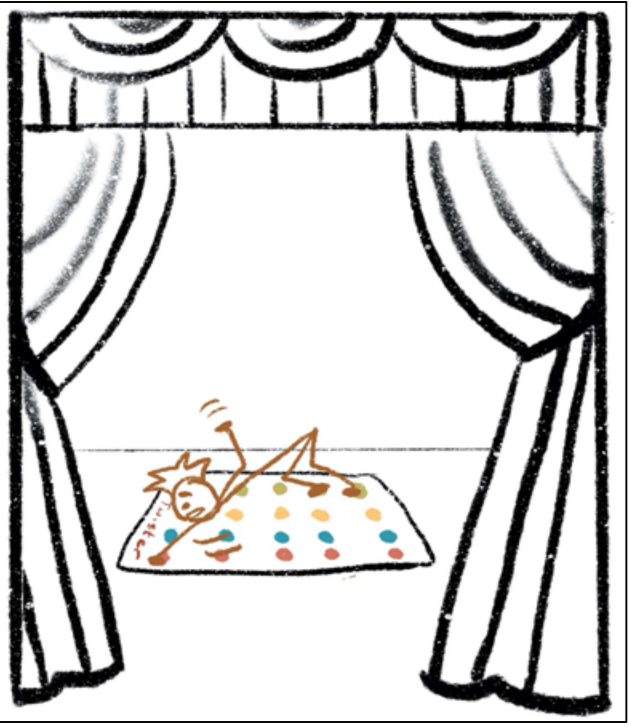
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.



...And maybe two...

## Some key lemmas used in the polynomial method

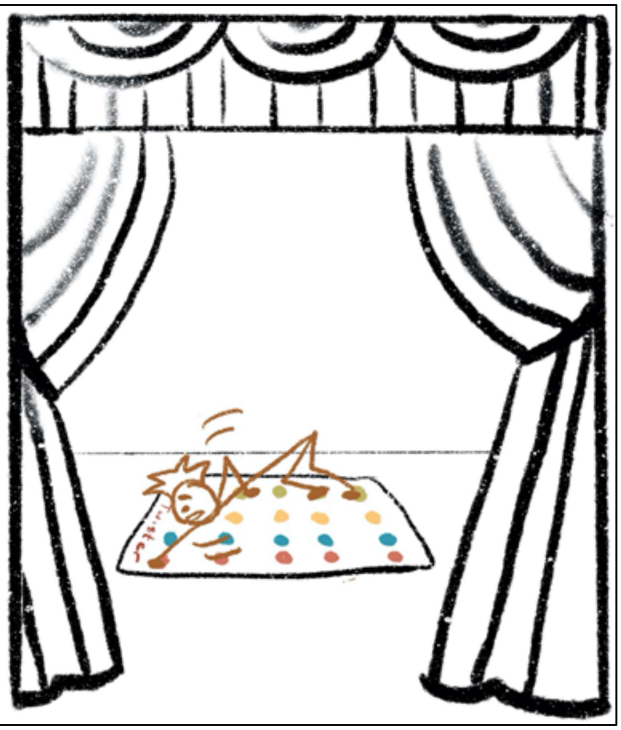
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where $d < q$, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.



...But perhaps once it goes through a certain number of roots of the polynomial...

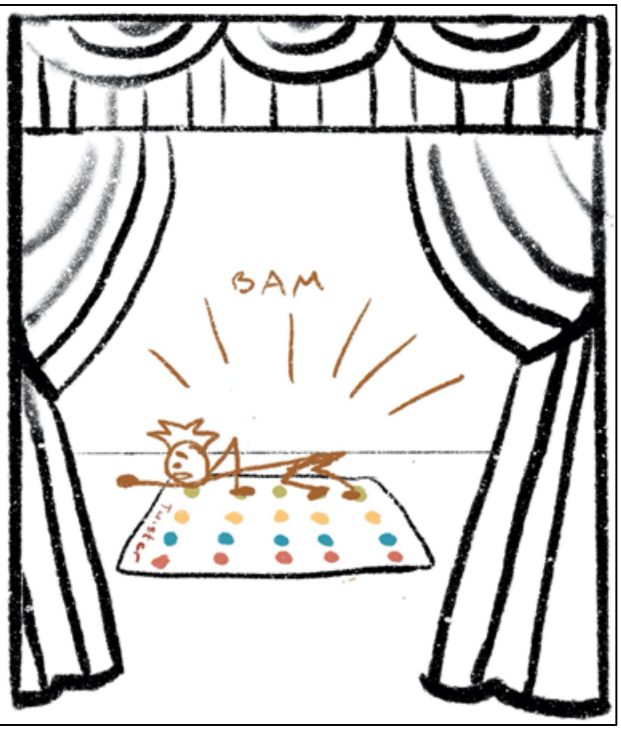
# Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.



## Some key lemmas used in the polynomial method

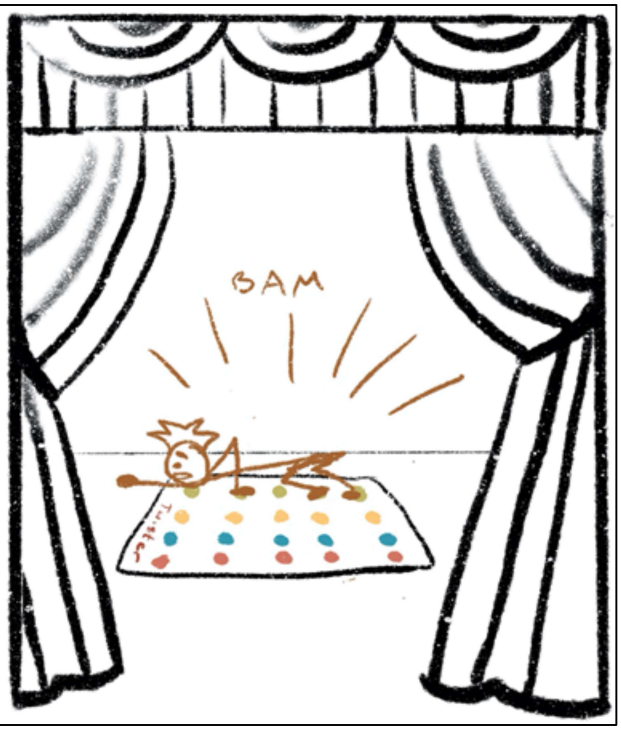
- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.



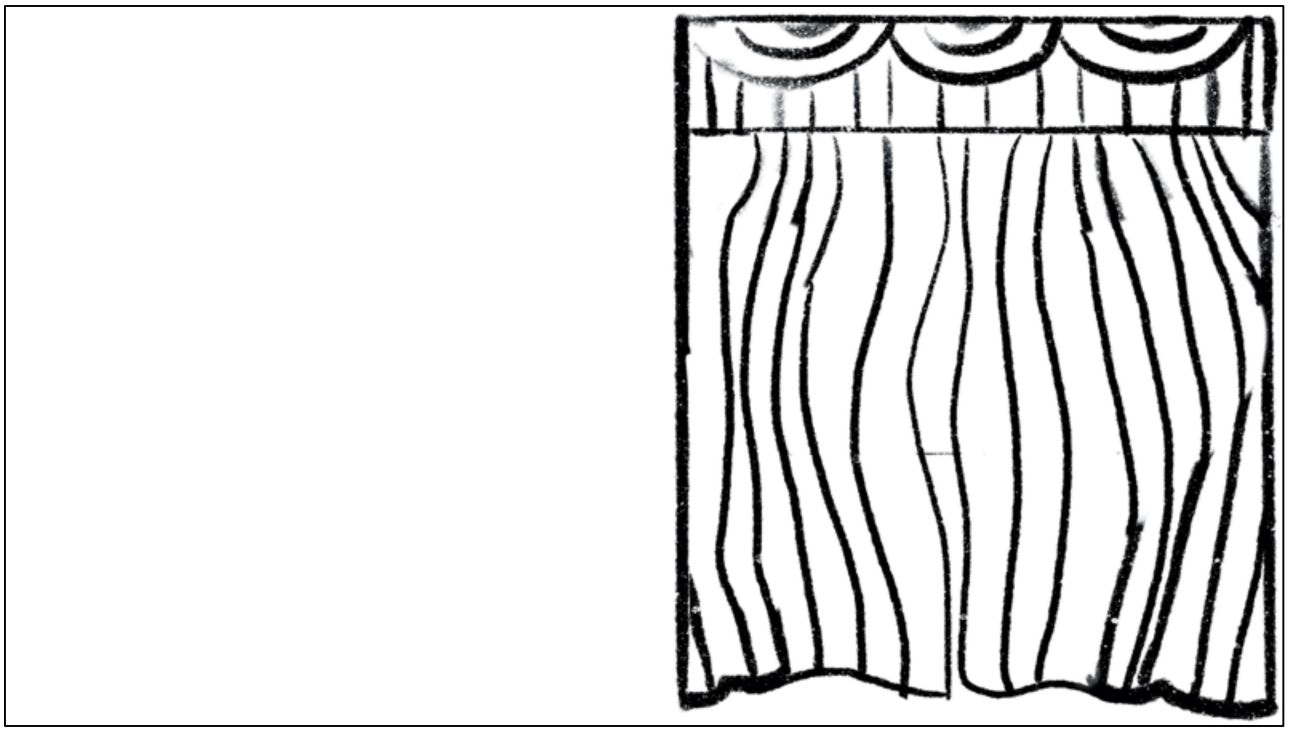

...it snaps into place, and the line must be entirely contained within the zeroes of the polynomial.

## Some key lemmas used in the polynomial method

- **(Vanishing Lemma)** If a polynomial vanishes too many times, it vanishes everywhere.
  - More precisely: If a d-degree polynomial vanishes on q points in a finite field where d < q, then it must vanish everywhere, and be the zero-polynomial.
- **(Interpolation Lemma)** If we're given few enough points, we can find a low-degree polynomial that passes through all of them.
  - More precisely: If we're given less than $\binom{d+n}{n}$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.
- **(Rigidity Lemma)** Once a line in a field passes through too many roots of a low-degree polynomial, it "snaps" into place and then the only points the line passes through must be roots.
  - More precisely: Consider a d-degree polynomial over a finite field. Every line in that field either (a) passes through at most d roots of that polynomial or (b) passes through roots of that polynomial at every



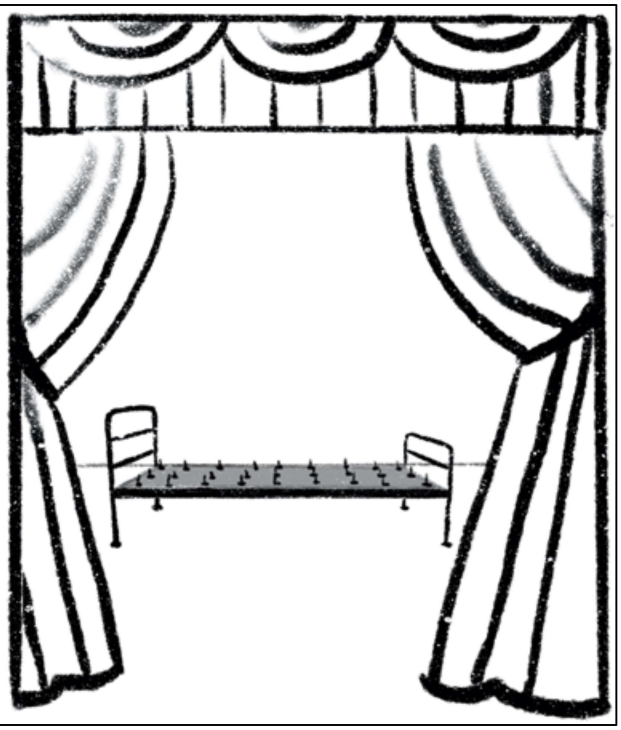

More formally stated, the rigidity lemma is as follows. Consider a d-degree polynomial over a finite field. Every line in that field either (a) passes through at most d roots of that polynomial or (b) passes through roots of that polynomial at every point along the line.



And that's it for the lemmas used in the polynomial method.  Now we'll get in to our first application of these lemmas.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

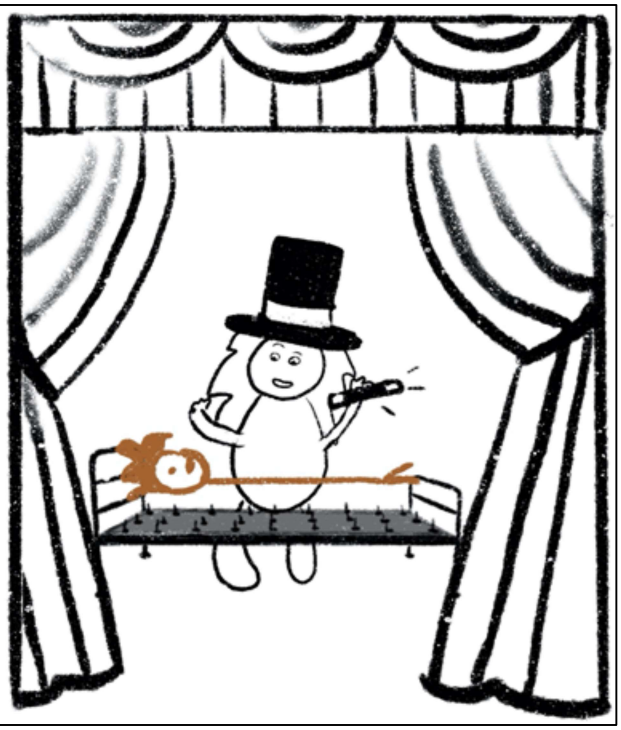
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



This theorem is called the finite-field nikodym problem — and it is a simplified version of the somewhat famous Kakeya problem.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

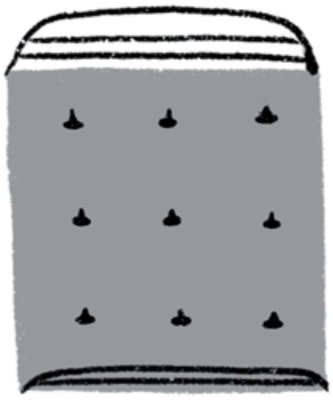


We want to say: Let's say a set is "Nikodym" if it is a set such that, for every point in the vector space, we can always find a line through the point that goes through at least "d" points in the Nikodym set.

How small can a Nikodym set be?

## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

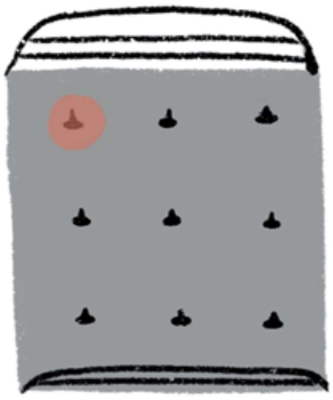


Again, we consider a vector space F^n defined over a finite field F.

Here in particular, we can consider the vector space F^3 defined over the finite field with three elements. And let's set d=2.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

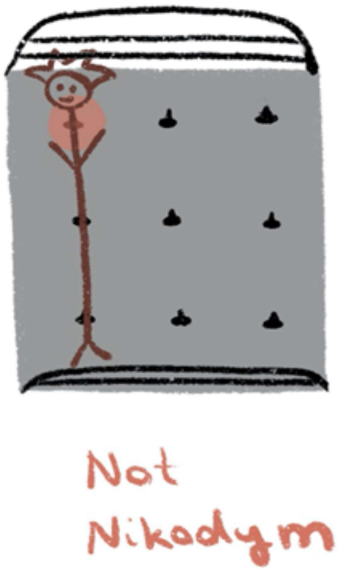
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



Then we know that any set with just one point will not be a Nikodym set of characteristic d=2. Because for example...

## Polynomial Method Application #1: The Finite-field Nikodym Problem

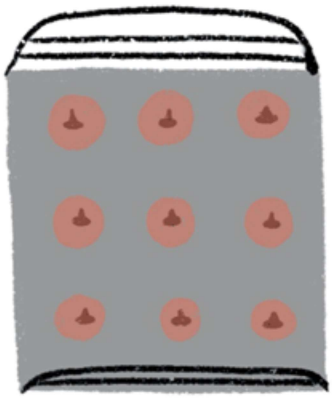
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*




...we cannot find a line through that point that intersects the Nikodym set at more than d=2 points.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

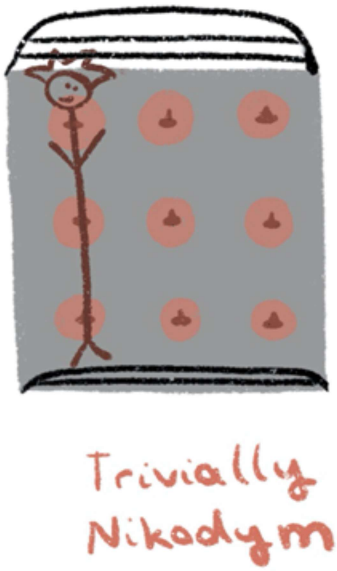
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



On the opposite end of the spectrum, we know any set that contains all the elements of the vector space is trivially a Nikodym set.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

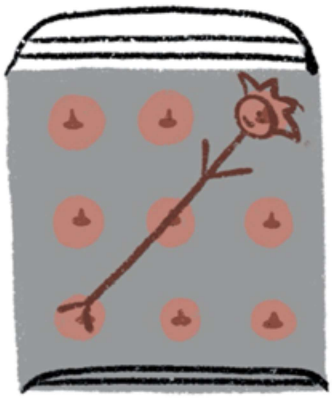
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*




Because every line through every point will go through at least d=2 points in the Nikodym set.

# Polynomial Method Application #1: The Finite-field Nikodym Problem

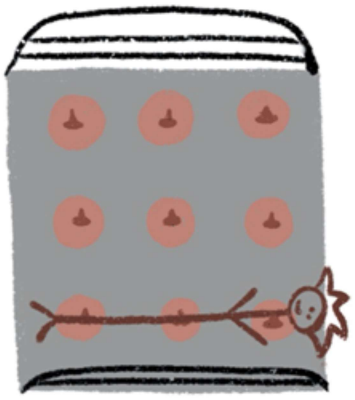
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



Trivially Nikodym

# Polynomial Method Application #1: The Finite-field Nikodym Problem

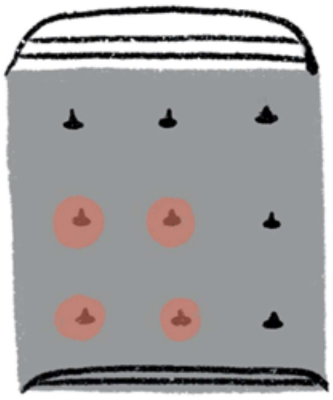
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



Trivially Nikodym

## Polynomial Method Application #1: The Finite-field Nikodym Problem

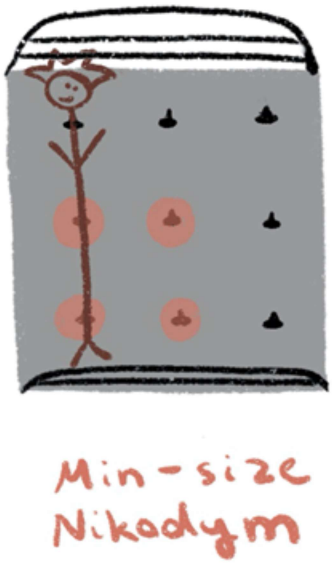
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



So the interesting question is, how small can such a set be? It turns out for this vector field F^3 defined over the three-element finite field F, the minimal-size Nikodym set has size four.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

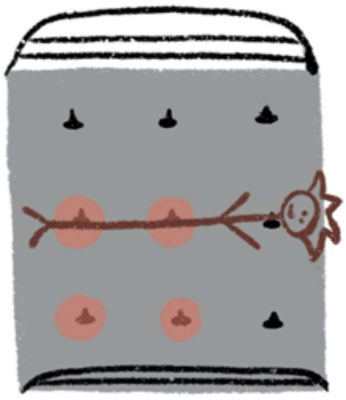
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*




And you can somehow convince yourself of this just by drawing several lines through this set.

# Polynomial Method Application #1: The Finite-field Nikodym Problem

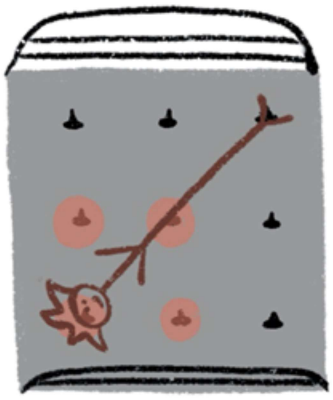
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



Min-size Nikodym

# Polynomial Method Application #1: The Finite-field Nikodym Problem

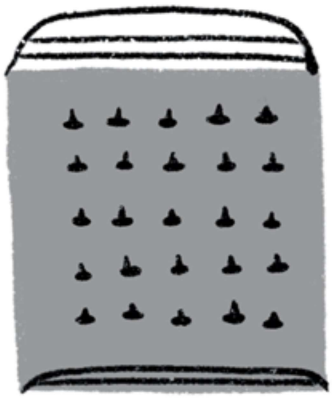
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*



Min-size Nikodym

## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

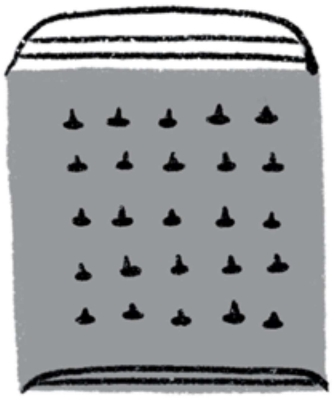


But now, we're concerned with finding these minimal-size sets in a more general vector space.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes

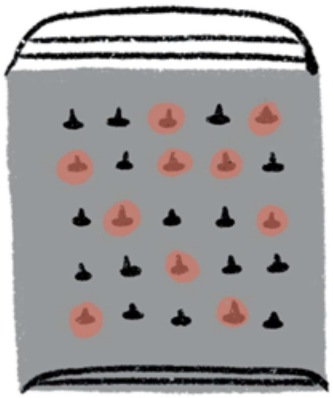


So now, the first step in applying the polynomial method to a problem is turning this problem into one related to a polynomial that vanishes.

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.



# Polynomial Method Application #1: The Finite-field Nikodym Problem

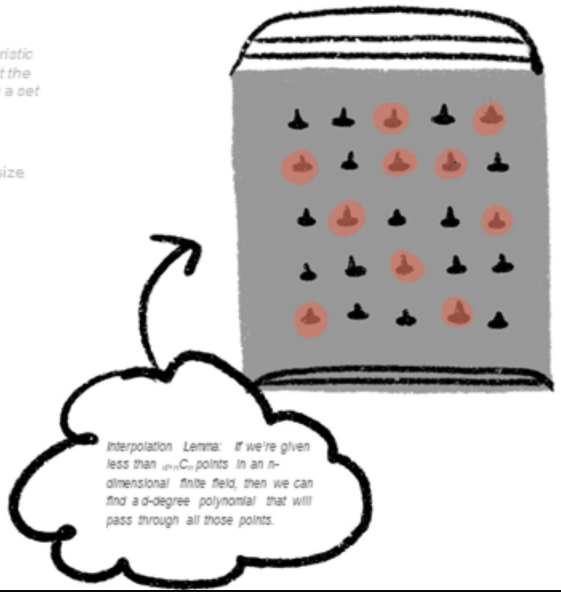
*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma...

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma...

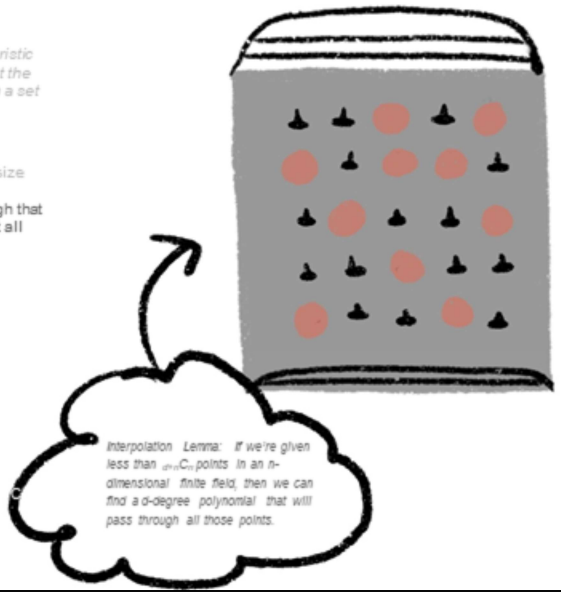


*Interpolation Lemma: If we're given less than $_{d+n}C_n$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.*

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.

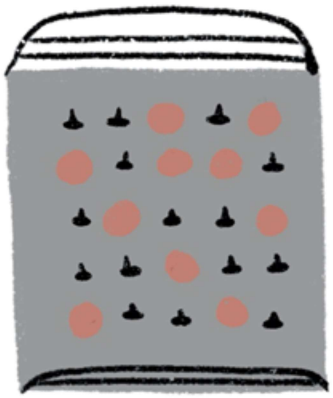


*Interpolation Lemma: If we're given less than $_{d+n}C_n$ points in an n-dimensional finite field, then we can find a d-degree polynomial that will pass through all those points.*

## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction

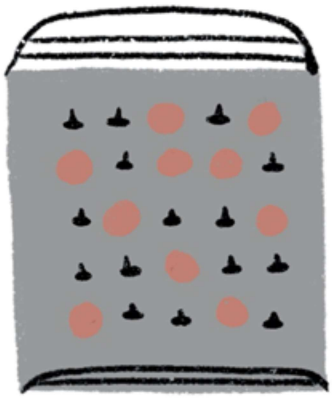


Then, typically, we try to find some sort of contradiction.

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

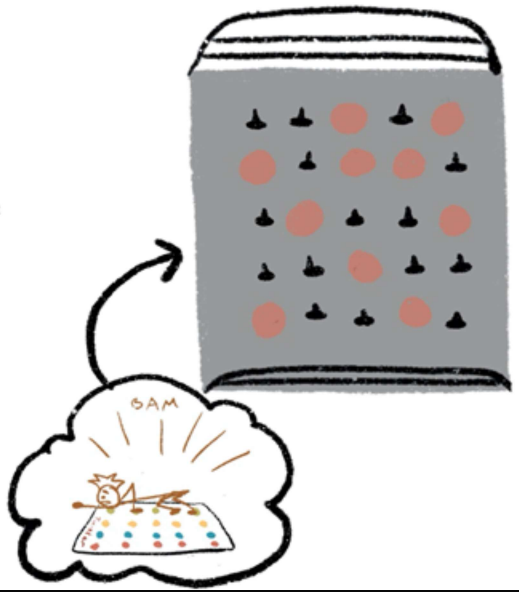
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.



# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

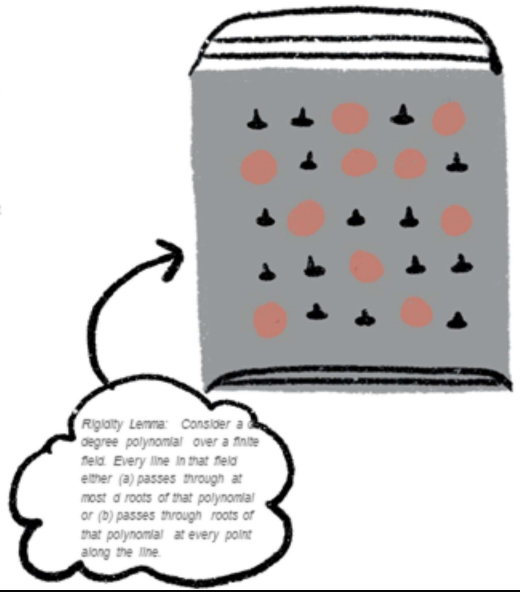
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...



# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

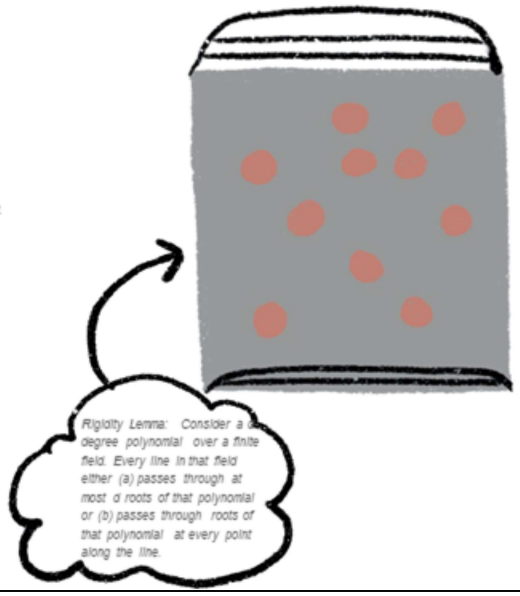
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...



# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $d+1C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.



*Rigidity Lemma: Consider a [illegible] degree polynomial over a finite field. Every line in that field either (a) passes through at most d roots of that polynomial or (b) passes through roots of that polynomial at every point along the line.*

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.

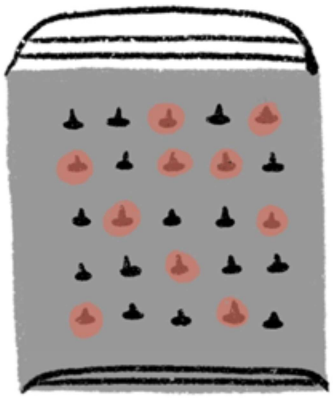
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.
   - So the polynomial vanishes everywhere, and by the vanishing lemma, is the zero polynomial.

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.

2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.
   - So the polynomial vanishes everywhere, and by the vanishing lemma, is the zero polynomial.
   - We have a contradiction: this polynomial was supposed to be non-zero.



# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

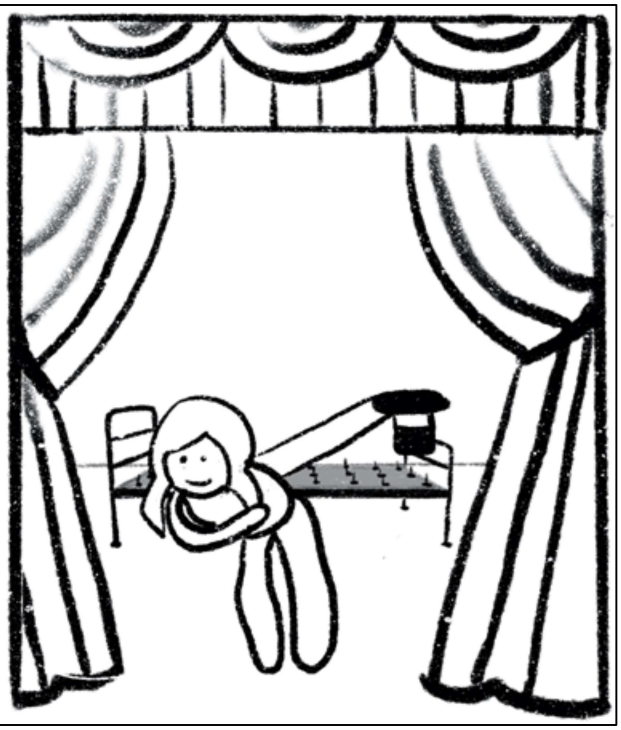
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.

2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.
   - So the polynomial vanishes everywhere, and by the vanishing lemma, is the zero polynomial.
   - We have a contradiction: this polynomial was supposed to be non-zero.

## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.
   - So the polynomial vanishes everywhere, and by the vanishing lemma, is the zero polynomial.
   - We have a contradiction: this polynomial was supposed to be non-zero.
3. Solve the original problem

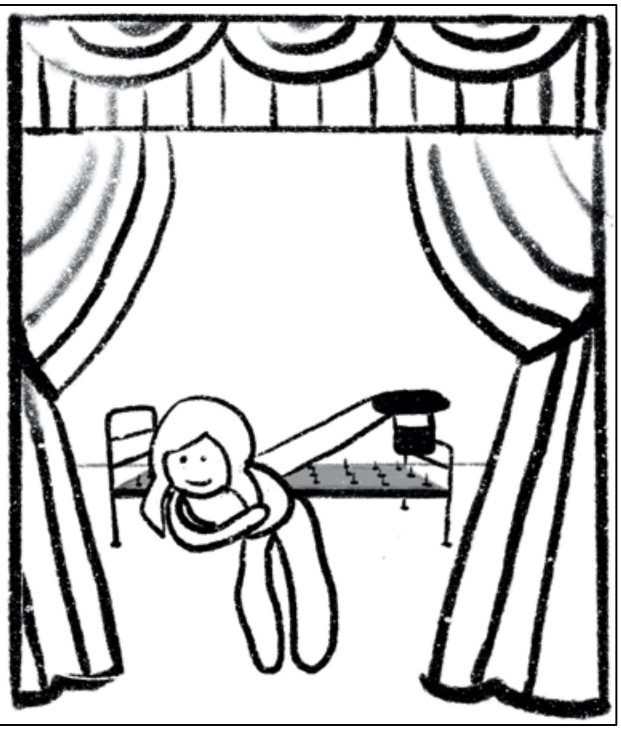


And now, given the contradiction we found, we can solve the original problem.

# Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

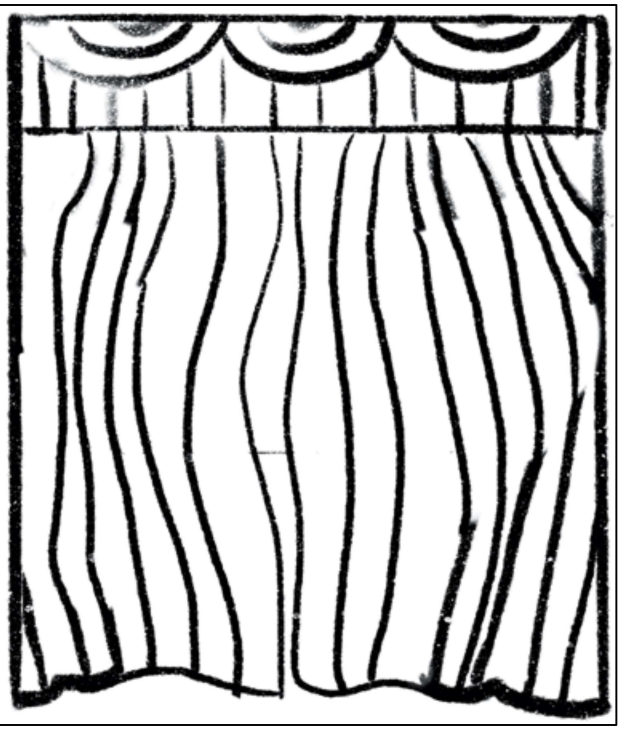
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.
   - So the polynomial vanishes everywhere, and by the vanishing lemma, is the zero polynomial.
   - We have a contradiction: this polynomial was supposed to be non-zero.
3. Solve the original problem
   - So, we could never have a Nikodym set E of size less than $_{d+n}C_n$. Therefore, $|E| \geq {}_{d+n}C_n$.



## Polynomial Method Application #1: The Finite-field Nikodym Problem

*Let $F^n$ be a finite field in n-dimensions. Let E be a Nikodym set of characteristic d within F, i.e. for each point $x \in F^n$ you can find a direction $y \in F^n$ such that the line $\{x + ty : t \in F\}$ intersects E at more than d points. How small can such a set be?*

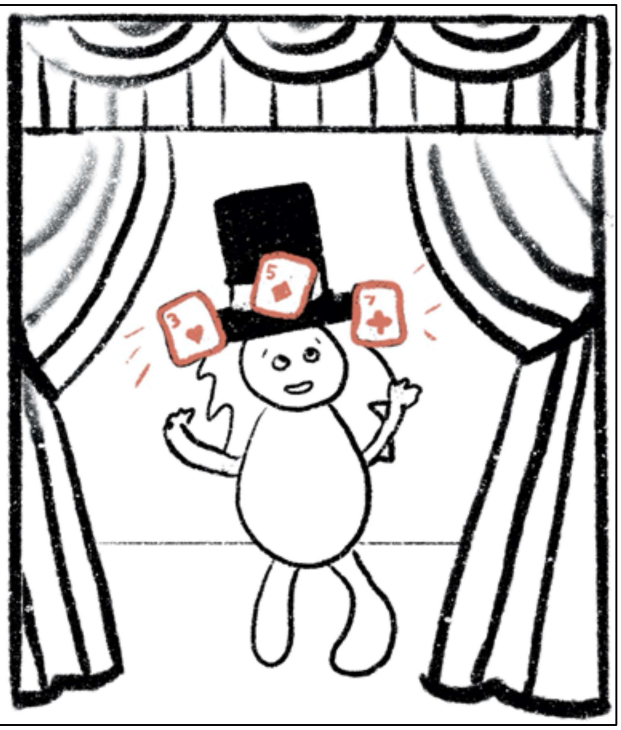
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, we have a Nikodym set E of size less than $_{d+n}C_n$.
   - Then by the interpolation lemma... the set is small enough that we can find a non-zero polynomial of degree d such that all elements of E are zeroes of the polynomial.
2. Find a contradiction
   - By the problem statement, there's a line through every point that goes through at least d points in the set E.
   - So by the rigidity lemma...there's a line through every point that goes through only zeros of the polynomial.
   - So the polynomial vanishes everywhere, and by the vanishing lemma, is the zero polynomial.
   - We have a contradiction: this polynomial was supposed to be non-zero.
3. Solve the original problem
   - So, we could never have a Nikodym set E of size less than $_{d+n}C_n$. Therefore, $|E| \geq {}_{d+n}C_n$.



...And now, onto our next application of the polynomial method.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?



This problem is called the cap-set problem.

A particular case of this problem can be applied to the card game Set — the relevant question being "what is the largest set of cards you can lay out in the game, without there being a single "Set" (cards that all have the same attribute)"? But for the purposes of this proof, we'll stick to the more general statement of the problem.

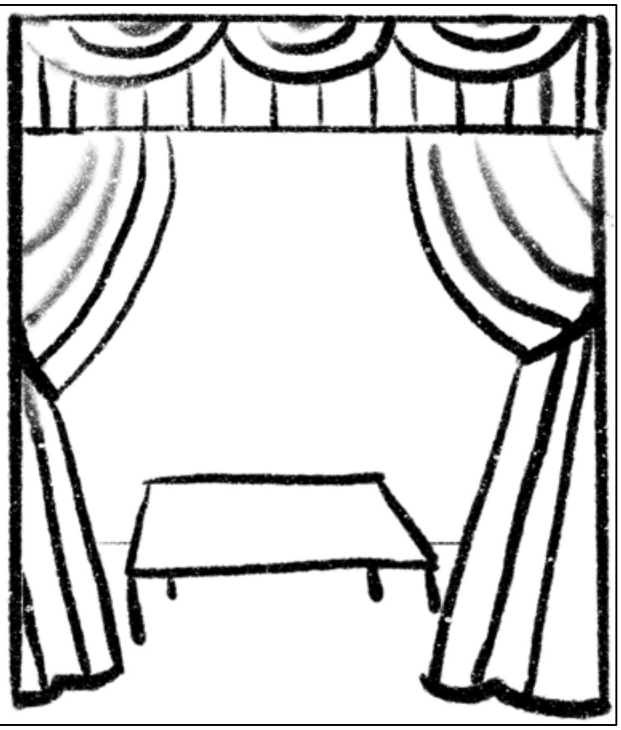
We consider a vector space F^n defined on a q-element finite field F_q. Then we consider a set "A" in this space with no three-element arithmetic progressions (e.g. 3,5,7 or 0,1,2). Obviously if you choose a set A with only two elements, you guarantee this condition. So the interesting question is — how large can such a set be?

As a warning, this proof is more involved...so, I'm just going to focus on the part of the proof that employs the polynomial method, and be a little hand-wavy at the other parts.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes

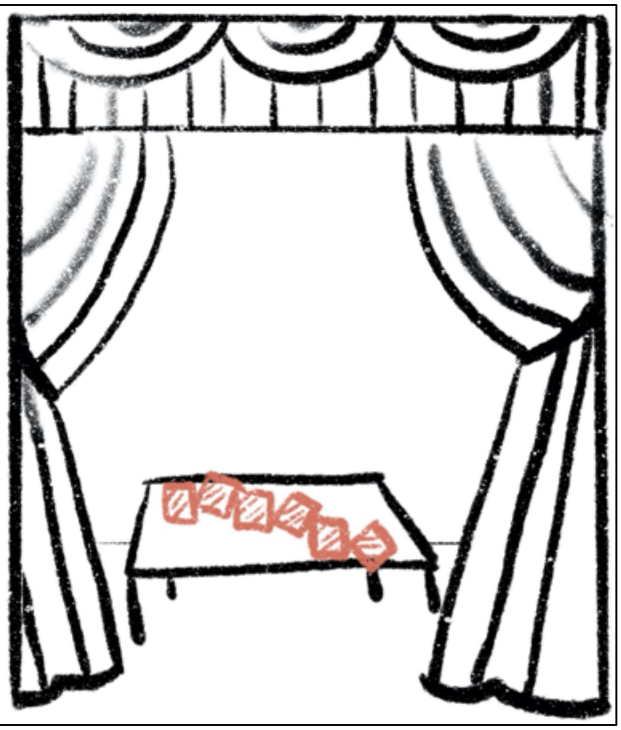


So first, just as before, we want to turn this problem into a problem about a vanishing polynomial.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.

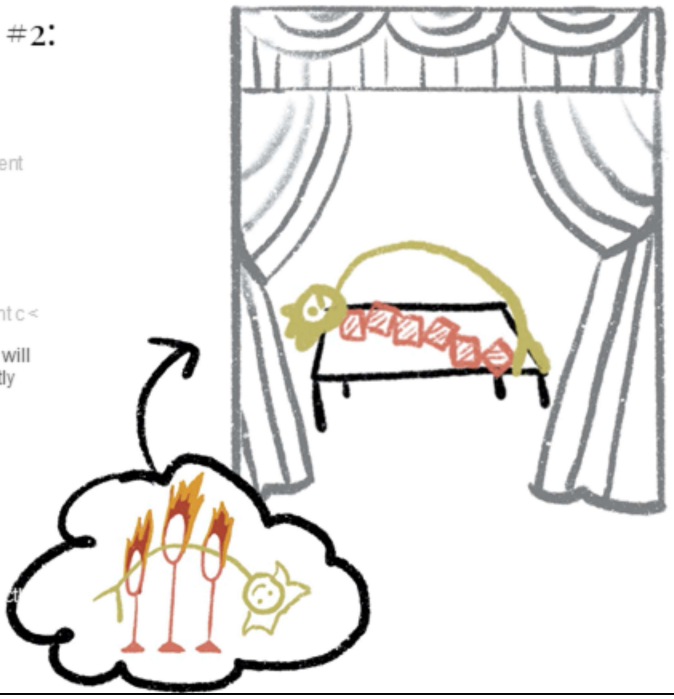


So let's first suppose that a cap set A can be bigger than we think it is...

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A



...and then find a polynomial that is mostly nonzero on the set 2A.

# Polynomial Method Application #2: The Cap Set Problem

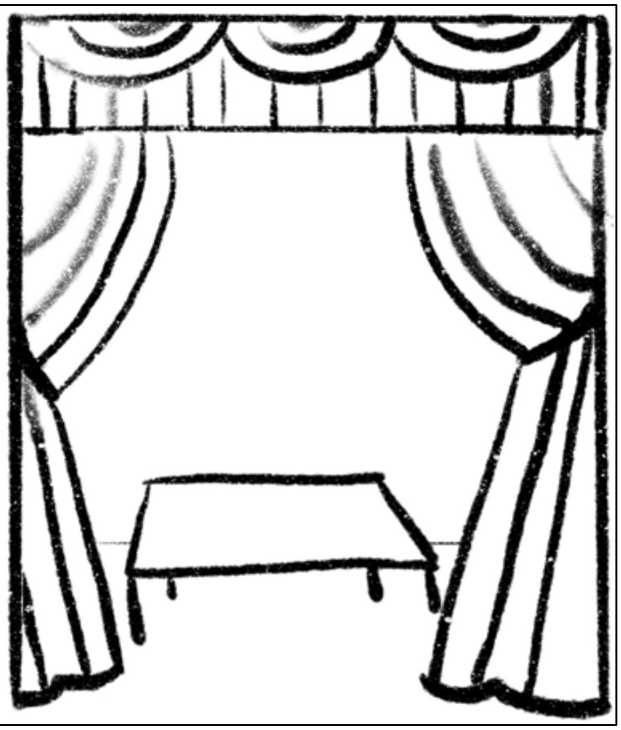
A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction

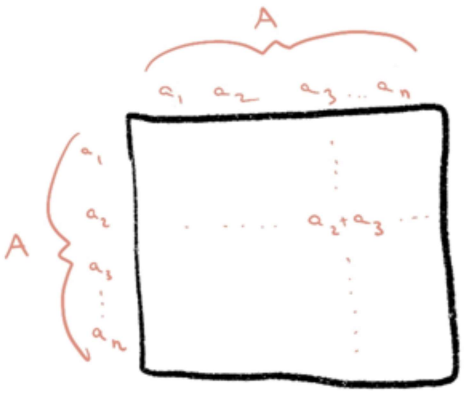


Now we find a contradiction.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A... that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.

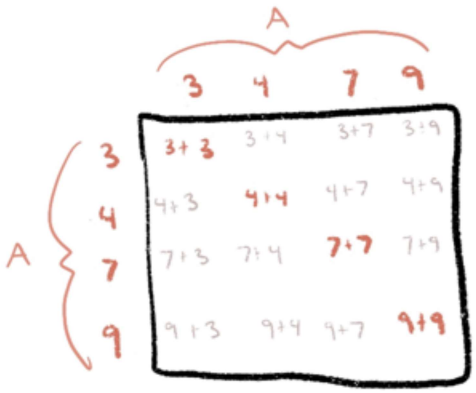



We cleverly construct the above particular matrix, and note that it must contain the elements of 2A on its diagonal, and elements of the complement of (2A) everywhere else. Why?

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.

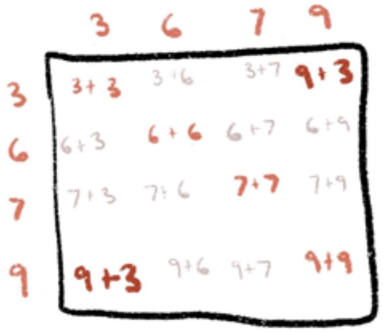



To see this, consider a sequence of numbers {3,4,7,9} that contains no three-element arithmetic progression. Note that the diagonal contains elements of 2A, and elements of the complement on the off-diagonal.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.




*Fun fact: A sequence has no three-term arithmetic progressions if it has no x,y,z such that x+z=2y.*

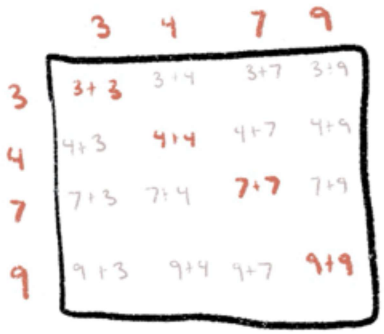
But now, if we consider a sequence of numbers {3,6,7,9} that *does* contain the three-element arithmetic progression {3,6,9}, note that the diagonal contains elements of 2A, and off-diagonal also contains an element of 2A (namely, 12).

This is because saying a sequence has no three-term arithmetic progressions is equivalent to saying the sequence has no x,y,z such that x+z=2y. (You can convince yourself of this by considering the equations x+c=y and y+c=z, and simplifying to x-y=y-z, and then further to x+z=2y.)

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $F_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{ij}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.

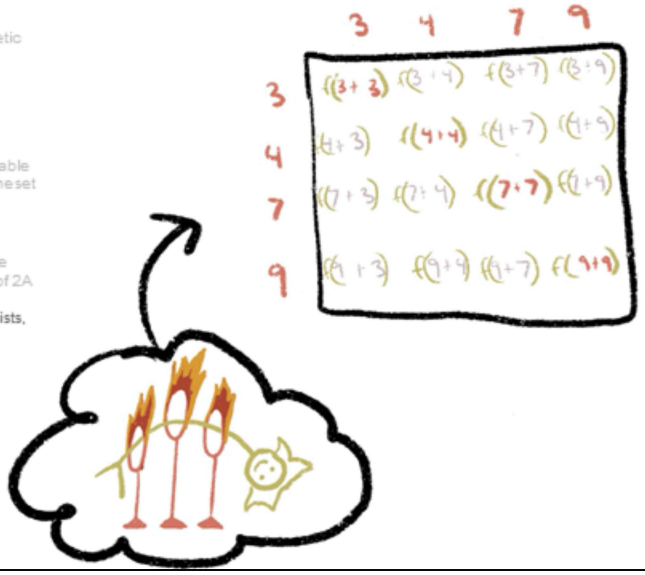



In any case, we're assuming that our set A has no three-term arithmetic progressions, so for this small example, we can switch back to this sample matrix where A={3,4,7,9}.

# Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{ij}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix...

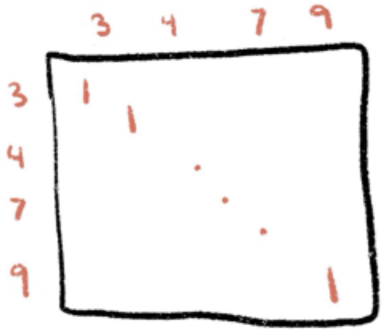



We now want to apply our monomial function f to every element of the matrix.

# Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{ij}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix, we get a matrix of rank strictly greater than a certain size.

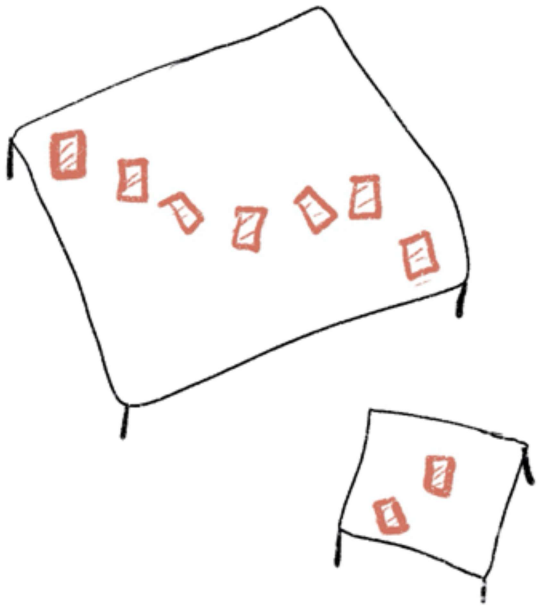



And end up with a matrix with a certain minimal rank.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix, we get a matrix of rank strictly greater than a certain size.
   - But we can apply another lemma that shows the matrix must have a rank strictly less than that size. We have a contradiction.



But (and now this is the hand-wavy part), we can also apply a separate lemma, that shows the matrix has strictly less than that rank. So we have a contradiction.

# Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

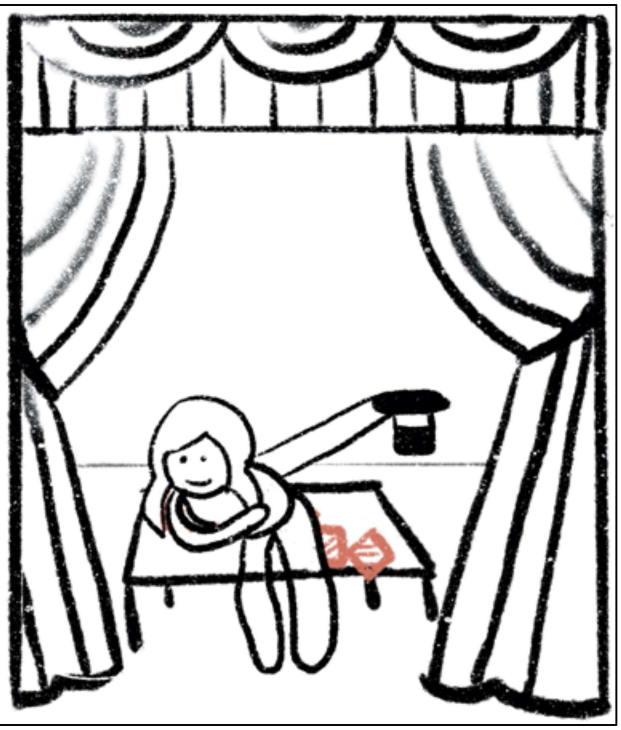
1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{ij}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix, we get a matrix of rank strictly greater than a certain size.
   - But we can apply another lemma that shows the matrix must have a rank strictly less than that size. We have a contradiction.


And so...

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix, we get a matrix of rank strictly greater than a certain size.
   - But we can apply another lemma that shows the matrix must have a rank strictly less than that size. We have a contradiction.
3. Solve the original problem

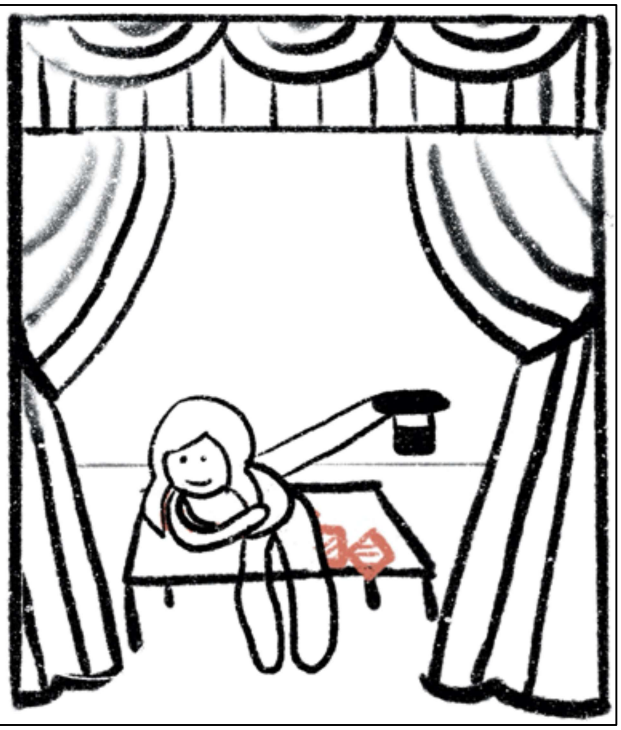


We can conclude that our assumption was false.

## Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix, we get a matrix of rank strictly greater than a certain size.
   - But we can apply another lemma that shows the matrix must have a rank strictly less than that size. We have a contradiction.
3. Solve the original problem
   - So, we could never have a cap set of size bigger than $c^n$. Therefore, $|A| \leq c^n$.

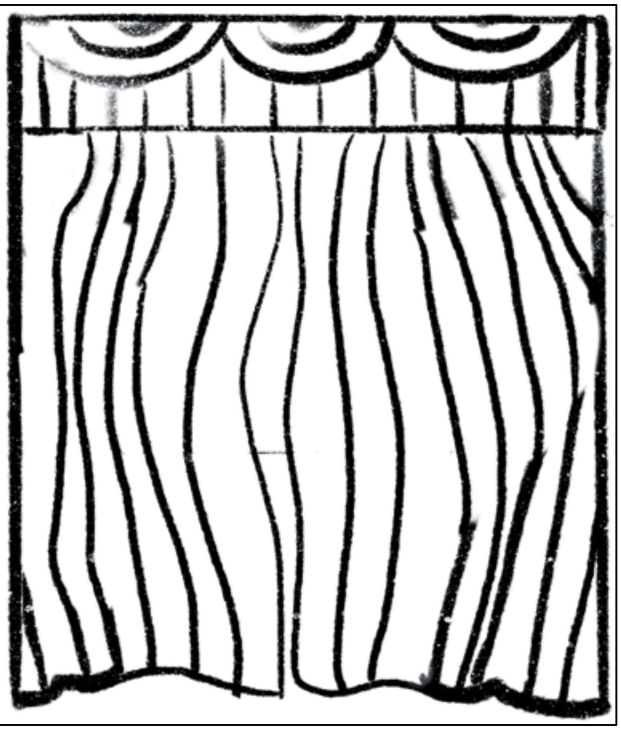


And therefore the cap set size is bounded above by c^n. (Although, note that we didn't prove the bound is tight, although it is probably pretty close to tight.)

# Polynomial Method Application #2: The Cap Set Problem

A cap set is a subset of the vector space $\mathbb{F}_q^n$ with no three-element arithmetic progressions. How big can such a set be?

1. Turn the problem into a polynomial that vanishes
   - Suppose, for contradiction, that the cap set A is a set of size bigger than $c^n$ for some constant $c < q$.
   - Then by a variant of the interpolation lemma, we will be able to find a monomial function f that is mostly nonzero on the set 2A, and vanishes on its complement $(2A)^c$.
2. Find a contradiction
   - If we construct a matrix $(a_i + a_j)_{i,j}$ made of the sums of the elements of A, that must mean it contains the elements of 2A on its diagonal, and elements of $(2A)^c$ everywhere else.
   - So, if we apply our monomial function f (that we know exists, due to the interpolation lemma) to each element of the matrix, we get a matrix of rank strictly greater than a certain size.
   - But we can apply another lemma that shows the matrix must have a rank strictly less than that size. We have a contradiction.
3. Solve the original problem
   - So, we could never have a cap set of size bigger than $c^n$. Therefore, $|A| \leq c^n$.



# The Cap Set Problem: Formalization in Lean

```
theorem general_cap_set {α : Type} [discrete_field α] [fintype α] :
  ∃ C B : ℝ, B > 0 ∧ C > 0 ∧ C < fintype.card α ∧
    ∀ {a b c : α} {n : ℕ} {A : finset (fin n → α)},
      c ≠ 0 → a + b + c = 0 →
      (∀ x y z : fin n → α, x ∈ A → y ∈ A → z ∈ A → a • x + b • y + c • z = 0 → x = y ∧ x = z) →
      ↑A.card ≤ B * C^n

theorem cap_set_problem : ∃ B : ℝ,
  ∀ {n : ℕ} {A : finset (fin n → ℤ/3ℤ)},
    (∀ x y z : fin n → ℤ/3ℤ, x ∈ A → y ∈ A → z ∈ A → x + y + z = 0 → x = y ∧ x = z) →
    ↑A.card ≤ B * ((((3 : ℝ) / 8)^3 * (207 + 33*real.sqrt 33))^(1/3 : ℝ))^n

theorem cap_set_problem_specific (n : ℕ) {A : finset (fin n → ℤ/3ℤ)}
  (hxyz : ∀ x y z : fin n → ℤ/3ℤ, x ∈ A → y ∈ A → z ∈ A → x + y + z = 0 → x = y ∧ x = z) :
  ↑A.card ≤ 3 * ((((3 : ℝ) / 8)^3 * (207 + 33*real.sqrt 33))^(1/3 : ℝ))^n
```

A fun fact for anyone interested — as of 2019, this problem has actually been formalized in Lean.

## Back to the point of the talk

So what is the polynomial method?

- A proof technique that often involves turning a combinatorics problem into a polynomial, then using various lemmas to find out where the polynomial vanishes, and using that to prove something about the original combinatorics problem.

If we wanted to make a tool that helped mathematicians solve problems using the polynomial method, what should that tool be? Some ideas in order from most to least realistic...

- A **Coq/Lean tactic** that attempts using various lemmas (vanishing, interpolation, rigidity) that usually end up being helpful in polynomial method proofs?
- A piece of **AI that sorts through conjectures** and proposes which problems might be amenable to being solved by this method?
- A piece of **AI that figures out how to transform combinatorics conjectures** into problems about polynomials?

And now back to the question of the talk — is there something interesting to do with this information?