Counting

Gadadhar Misra
Department of Mathematics,
Indian Institute of Science

It’s festive season, and you want to pack gifts for all your friends.

It's festive season, and you want to pack gifts for all your friends.

You have access to a storeroom that has an infinite supply of five kinds of gifts:

It's festive season, and you want to pack gifts for all your friends.

You have access to a storeroom that has an infinite supply of five kinds of gifts:

...that we will refer to as

G_1, G_2, G_3, G_4, G_5

You can form a GIFT PACK by picking some subset of

$$\{G_1, G_2, G_3, G_4, G_5\}$$

For example,

$$\mathfrak{G}_1 = \{G_1, G_3\}$$

is one gift pack, while

$$\mathfrak{G}_2 = \{G_1, G_2, G_4\}$$

is another.

How many different giftpacks can you form?

Naturally, you intend to make different gift packs for your different friends, depending on their personalities.

A Twist in the Story...

The storeroom comes with a guard.

The storeroom comes with a guard.

The storeroom comes with a guard.

A Compromise...

Turns out the guard is mathematically inclined, because he proclaims:

Turns out the guard is mathematically inclined, because he proclaims:

"I'll allow you to take five giftpacks and any others that you can form by...

...a linear combination of the indicator vectors of the giftpacks you have chosen."

What is an indicator vector?

What is an indicator vector?

It is a vector that keeps track of what gifts go into your gift packs.

What is an indicator vector?

It is a vector that keeps track of what gifts go into your gift packs.

An indicator vector of a giftpack $\mathfrak{G}$ is a string with five positions, formed with numbers $\{0, 1\}$, where:

What is an indicator vector?

It is a vector that keeps track of what gifts go into your gift packs.

An indicator vector of a giftpack $\mathfrak{G}$ is a string with five positions, formed with numbers $\{0, 1\}$, where:

the first position has number 1 if the first gift is in the gift pack, and 0 otherwise,

What is an indicator vector?

It is a vector that keeps track of what gifts go into your gift packs.

An indicator vector of a giftpack $\mathfrak{G}$ is a string with five positions, formed with numbers $\{0, 1\}$, where:

the first position has number 1 if the first gift is in the gift pack, and 0 otherwise,

the second position has number 1 if the second gift is in the gift pack, and 0 otherwise,

What is an indicator vector?

It is a vector that keeps track of what gifts go into your gift packs.

An indicator vector of a giftpack $\mathfrak{G}$ is a string with five positions, formed with numbers $\{0, 1\}$, where:

the first position has number 1 if the first gift is in the gift pack, and 0 otherwise,

the second position has number 1 if the second gift is in the gift pack, and 0 otherwise,

and so on.





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

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

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

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

$$(1 \qquad\qquad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0, 0, 1, 1, 0) +_2 (1, 0, 1, 1, 1)$$

$$(1 \qquad\qquad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0, 0, 1, 1, 0) +_2 (1, 0, 1, 1, 1)$$

$$(1, 0 \qquad\quad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0, 0, 1, 1, 0) +_2 (1, 0, 1, 1, 1)$$

$$(1, 0 \qquad\quad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0, 0, 1, 1, 0) +_2 (1, 0, 1, 1, 1)$$

$$(1, 0, 0 \qquad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0, 0, 1, 1, 0) +_2 (1, 0, 1, 1, 1)$$

$$(1, 0, 0 \qquad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

$$(1,0,0,0\quad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

$$(1,0,0,0\quad)$$

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0, 0, 1, 1, 0) +_2 (1, 0, 1, 1, 1)$$

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

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

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

What is a linear combination of indicator vectors?

Just take two vectors and add them point-wise — modulo two.

$$(0,0,1,1,0) +_2 (1,0,1,1,1)$$

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


Only five gift packs and linear combinations of them...


...that should be enough to get hold of all 32!

Can you figure out how?

Consider the simplest giftpacks, those with one gift each:

Consider the simplest giftpacks, those with one gift each:

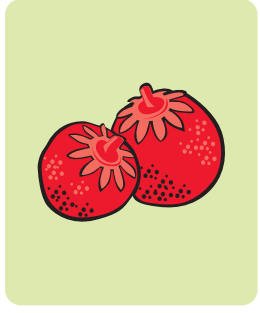
$$(1, 0, 0, 0, 0)$$

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

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

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

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



Because you can use these vectors to *generate* any of the others, these vectors are called...

Because you can use these vectors to *generate* any of the others, these vectors are called...

The Basis Vectors.

Incidentally, you could have also asked for the following giftpacks:

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

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

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

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

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

Incidentally, you could have also asked for the following giftpacks:

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

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

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

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

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

and every other giftpack can be obtained as a linear combination of these five.

Incidentally, you could have also asked for the following giftpacks:

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

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

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

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

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

and every other giftpack can be obtained as a linear combination of these five.

(Exercise: convince yourself of the above!)

A more interesting exercise: If the guard only allowed you four vectors instead of five, can you find four vectors with which you can generate all 32 giftpacks?

Consider a collection of vectors:

$$\{v_1, v_2, v_3, \ldots, v_n\}$$

Consider a collection of vectors:

$$\{v_1, v_2, v_3, \ldots, v_n\}$$

They are called LINEARLY INDEPENDENT if none of them can be generated by the rest.

Consider a collection of vectors:

$$\{v_1, v_2, v_3, \ldots, v_n\}$$

They are called LINEARLY INDEPENDENT if none of them can be generated by the rest.

What is quite interesting is that...

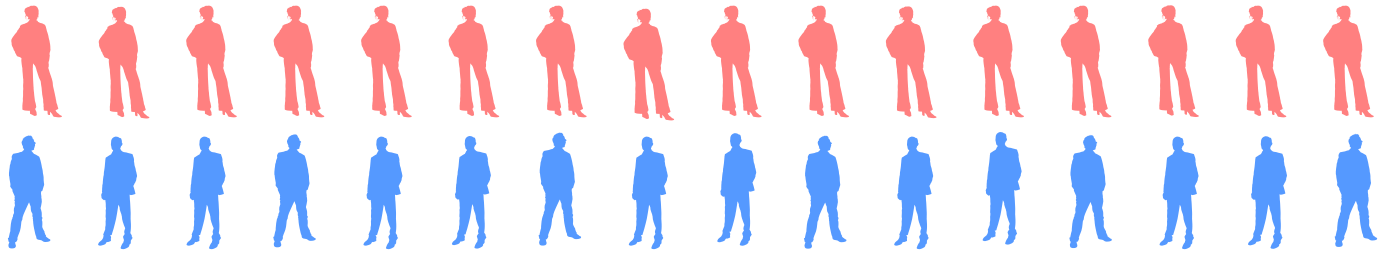
If the basis has p vectors,

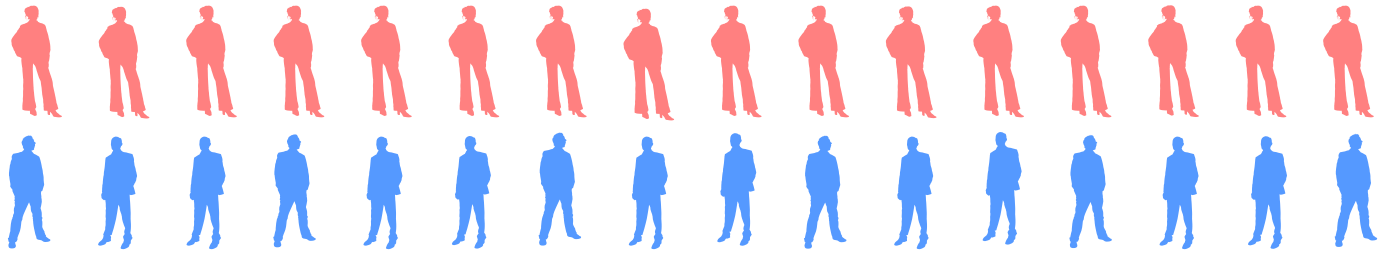
ANY collection of linearly independent vectors can have at most p vectors.

In the giftpack setting, this means that

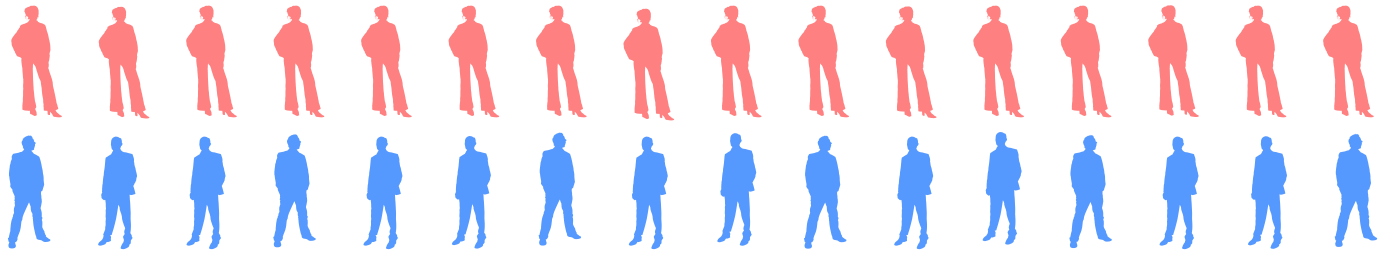
ANY collection of linearly independent vectors can have at most five vectors.

Welcome to Eventown

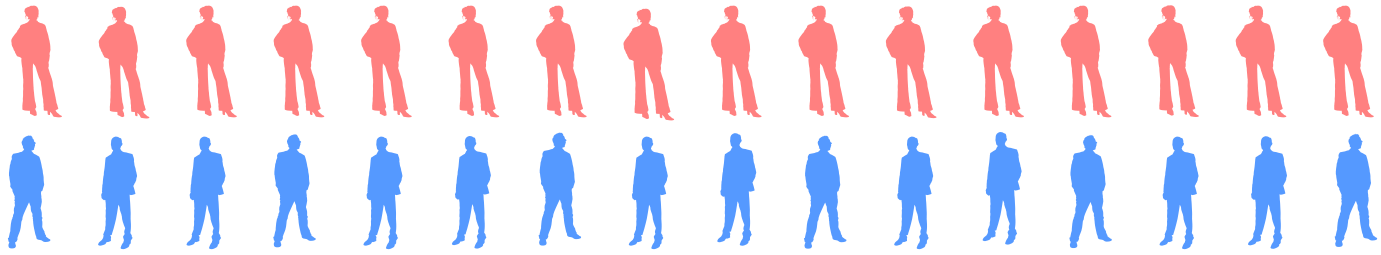




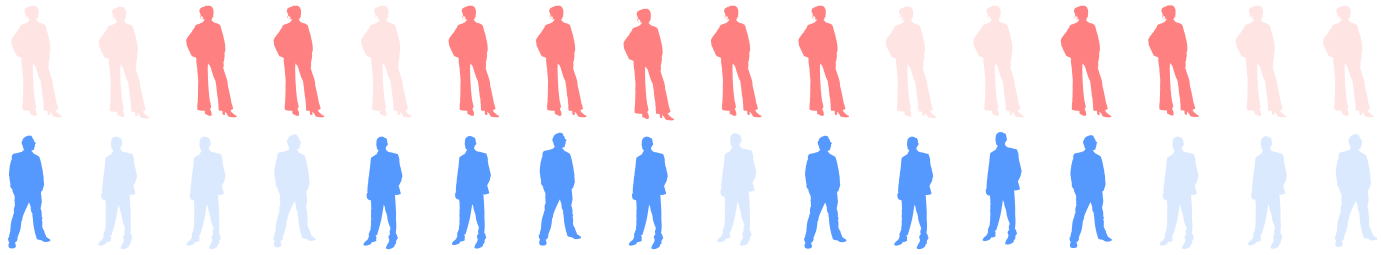
Sixteen couples live happily in Eventown.



Inhabitants of Eventown can form groups that are called *clubs*.

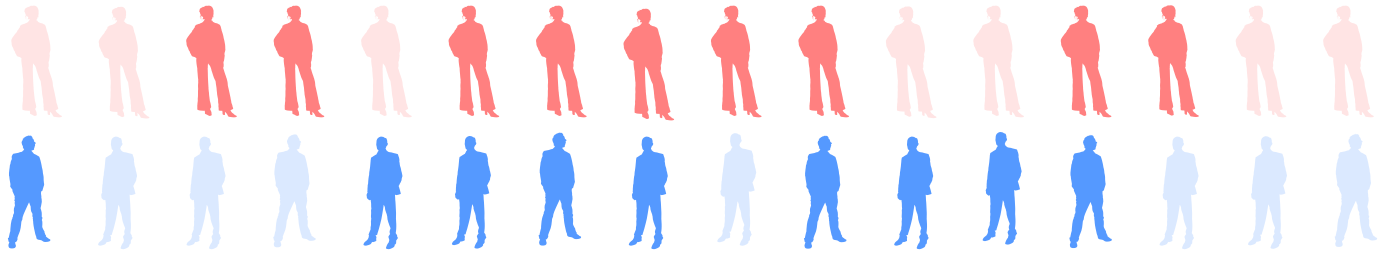


Club formation, however, is subject to some regulations.



Club formation, however, is subject to some regulations.

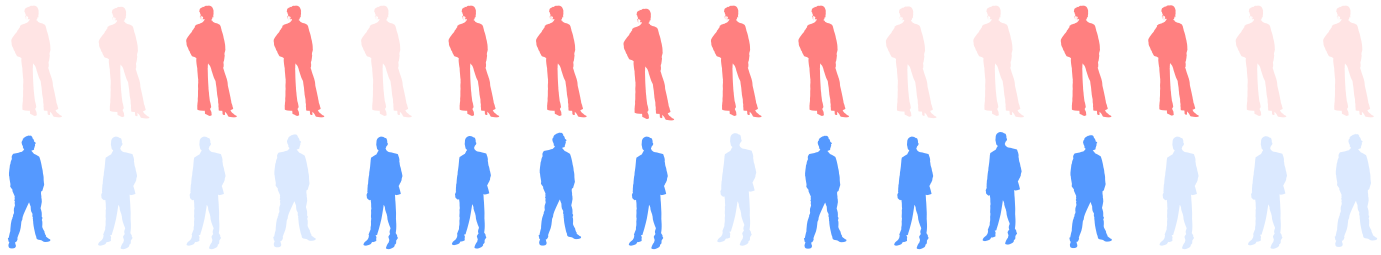
Every club should have an even number of members.



Club formation, however, is subject to some regulations.

Every club should have an even number of members.

No two clubs should have the same set of members.

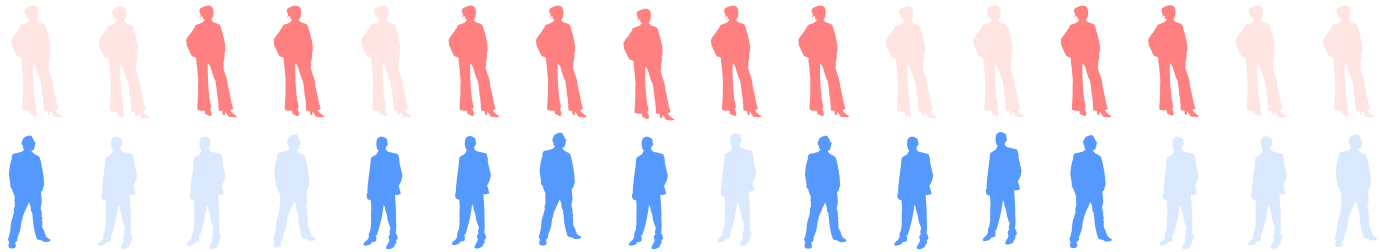


Club formation, however, is subject to some regulations.

Every club should have an even number of members.

No two clubs should have the same set of members.

Between any two clubs, the number of common members is even.



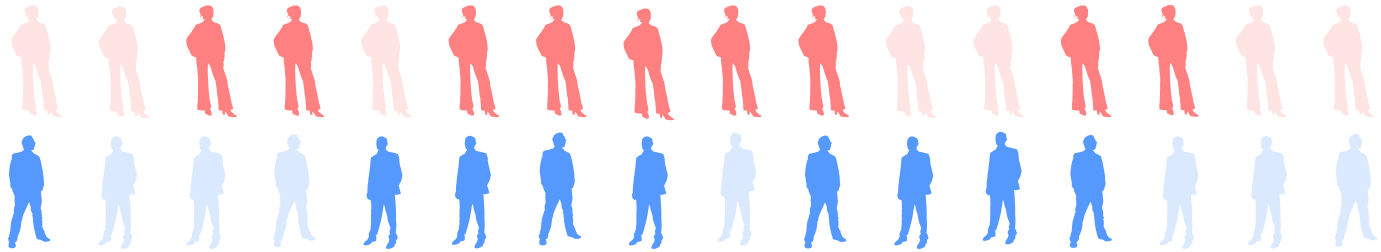
Club formation, however, is subject to some regulations.

Every club should have an even number of members.

No two clubs should have the same set of members.

Between any two clubs, the number of common members is even.

Members of Eventown want to form as many clubs as possible.



Club formation, however, is subject to some regulations.

Every club should have an even number of members.

No two clubs should have the same set of members.

Between any two clubs, the number of common members is even.

How many can you form given the regulations here?

A Simple Strategy...

A Simple Strategy...

Couples join clubs “together”.

Consider a couple A and B.

Given any club $\mathfrak{C}$:

Consider a couple A and B.

Given any club $\mathfrak{C}$:

Either A and B *both* belong to $\mathfrak{C}$, or

Consider a couple A and B.

Given any club $\mathfrak{C}$:

Either A and B *both* belong to $\mathfrak{C}$, or

Neither A *nor* B belong to $\mathfrak{C}$.

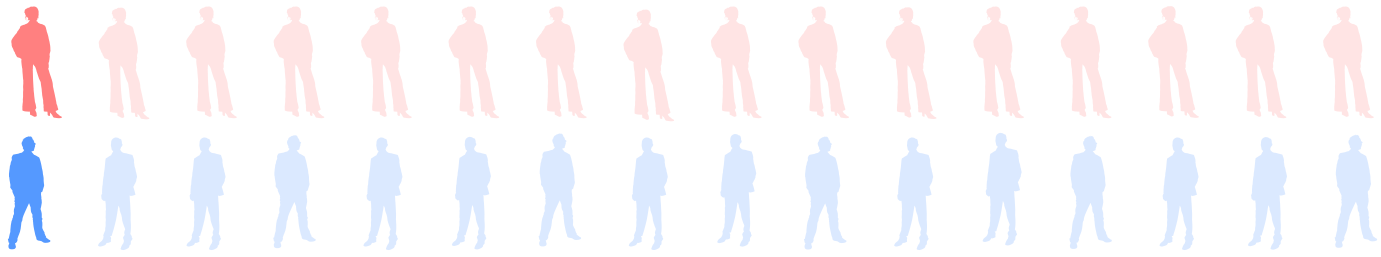
Consider a couple A and B.

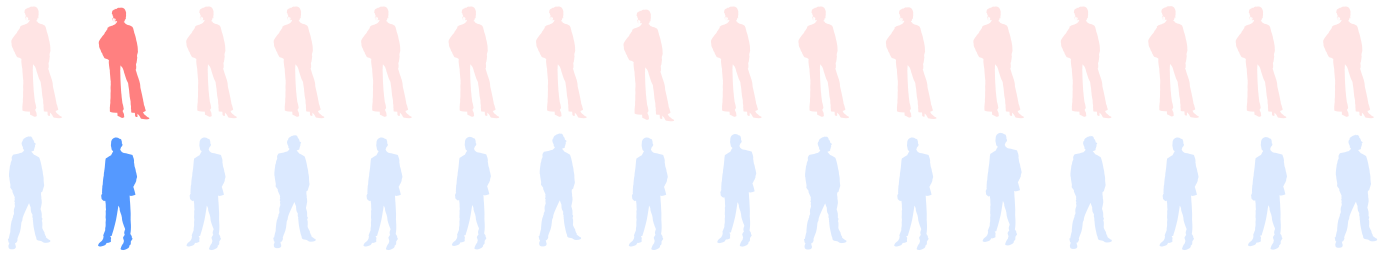
Given any club $\mathfrak{C}$:

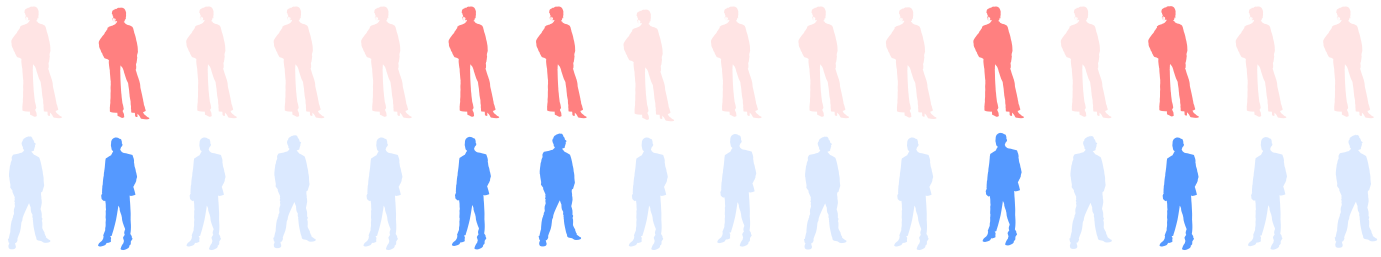
Either A and B *both* belong to $\mathfrak{C}$, or

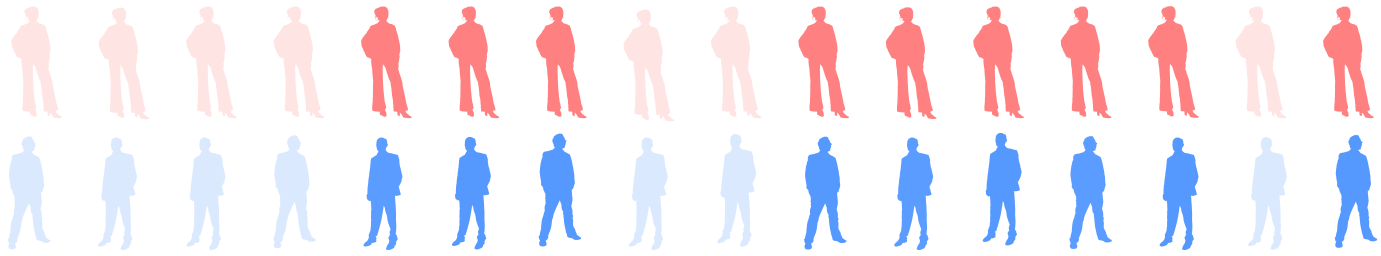
Neither A *nor* B belong to $\mathfrak{C}$.

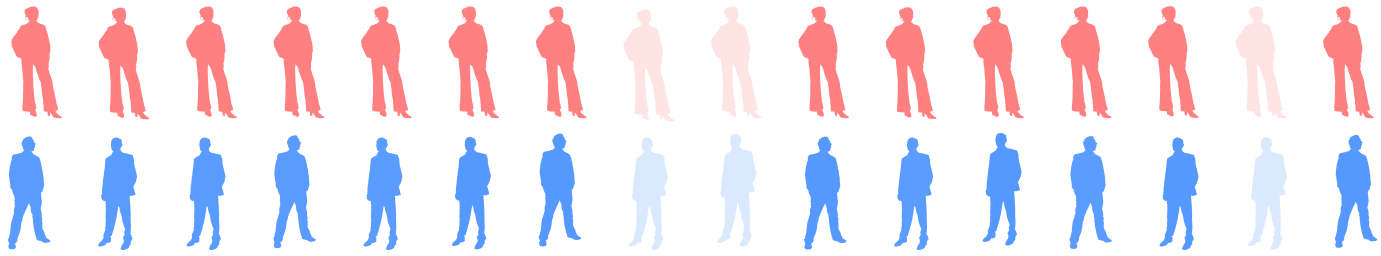
Given this strategy, how many clubs have we formed in Eventown?

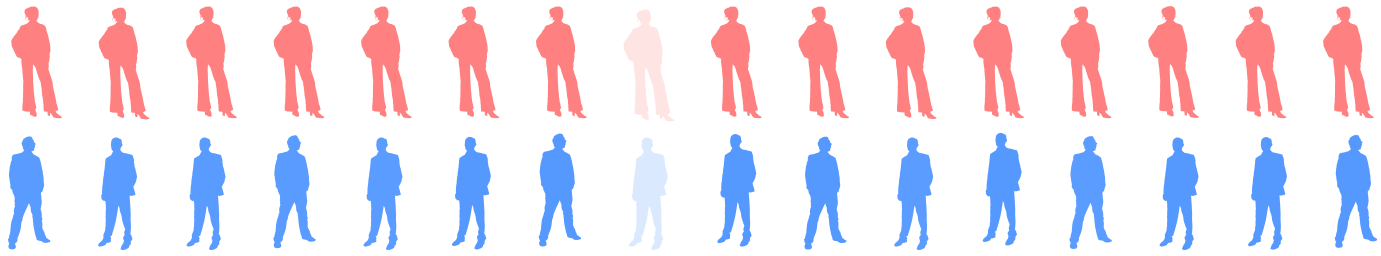


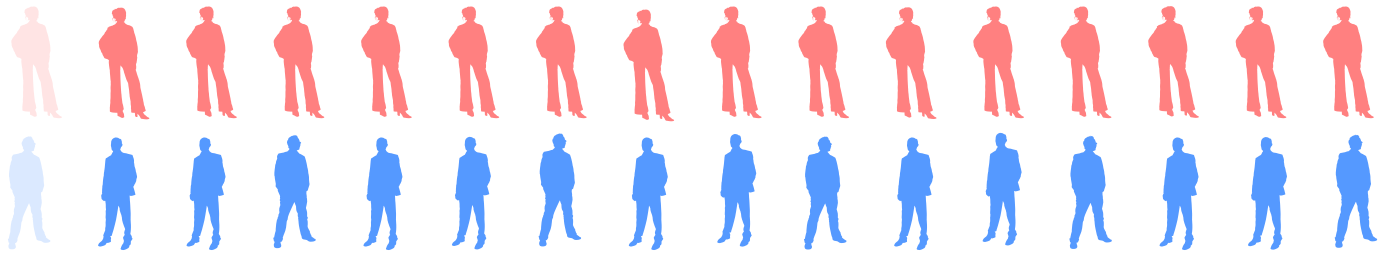


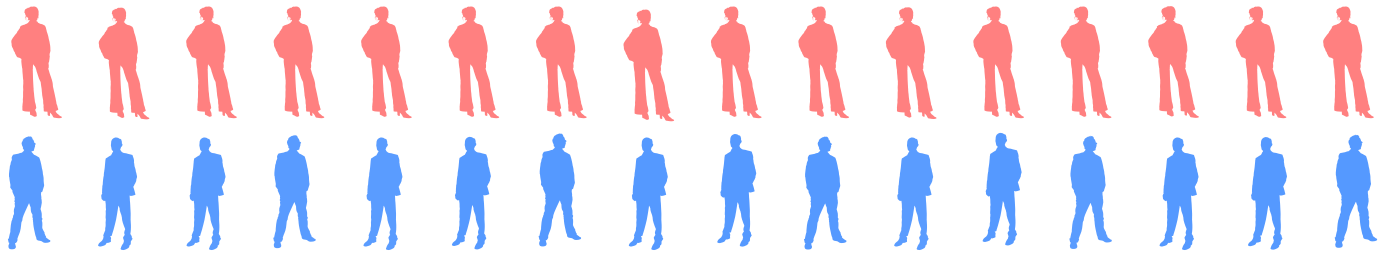












To count the total number of clubs, consider the *indicator string* of a club $\mathfrak{C}$.

To count the total number of clubs, consider the *indicator string* of a club $\mathfrak{C}$.

The $\mathfrak{i}^{\mathfrak{th}}$ bit of the string is a 1 if the $\mathfrak{i}^{\mathfrak{th}}$ couple belong to the club, and 0 otherwise.

For example,

1000000000000001

represents the club that has the first and last couple, and

1111111111111111

represents the club that has all couples as its members.

So the total number of clubs corresponds *exactly* to the total number of strings of length sixteen, each of whose letters can be either a 0 or a 1.

So the total number of clubs corresponds *exactly* to the total number of strings of length sixteen, each of whose letters can be either a 0 or a 1.

The total number of such strings is

$$2^{16} = 65,536.$$

So the total number of clubs corresponds *exactly* to the total number of strings of length sixteen, each of whose letters can be either a 0 or a 1.

The total number of such strings is

$$2^{16} = 65,536.$$

Exercise: Can you come up with a strategy to form even more clubs?

Now the management of Eventown decides this is one club too many.

Now the management of Eventown decides this is one club too many.

So in an attempt to prune down the number of possible clubs, the law is thus updated:

Now the management of Eventown decides this is one club too many.

So in an attempt to prune down the number of possible clubs, the law is thus updated:

Every club should have an ~~even~~ odd number of members.

No two clubs should have the same set of members.

Between any two clubs, the number of common members is even.

Now the management of Eventown decides this is one club too many.

So in an attempt to prune down the number of possible clubs, the law is thus updated:

Every club should have an ~~even~~ odd number of members.

No two clubs should have the same set of members.

Between any two clubs, the number of common members is even.

Members of Eventown still want to form as many clubs as possible.

Now the management of Eventown decides this is one club too many.

So in an attempt to prune down the number of possible clubs, the law is thus updated:

Every club should have an ~~even~~ odd number of members.

No two clubs should have the same set of members.

Between any two clubs, the number of common members is even.

Members of Eventown still want to form as many clubs as possible.
How many can you form given the new regulations?

Here's an easy way to form 32 clubs:

Here's an easy way to form 32 clubs:

Each inhabitant belongs to a club that has only himself as the member.

Here's an easy way to form 32 clubs:

Each inhabitant belongs to a club that has only himself as the member.

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

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

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

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

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

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

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

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

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

$$\vdots \quad \vdots$$

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

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

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

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

$$\vdots\ \vdots$$

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

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

In this example, clearly:

In this example, clearly:

all clubs are distinct,

In this example, clearly:

all clubs are distinct,

the intersection is always even because its always empty,

In this example, clearly:

all clubs are distinct,

the intersection is always even because its always empty,

and each club has an odd number of members because each club has just one person.

Notice, also, that these vectors form a basis for the set of indicator vectors of clubs - the indicator vector of *any* club can be generated using just these 32 vectors:

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

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

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

$$\vdots\ \vdots$$

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

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

So remember that we have a collection of 32 basis vectors.

Here's another easy way to form 32 clubs:

Here's another easy way to form 32 clubs:

For each inhabitant X, we create a club that has everyone except for X as its members.

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

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

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

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

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

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

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

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

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

$$\vdots\ \vdots$$

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

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

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

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

$$\vdots\ \vdots$$

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

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

In this example, clearly:

In this example, clearly:

all clubs are distinct,

In this example, clearly:

all clubs are distinct,

each club has an odd number of members because each club has all but one inhabitant from Eventown (and that's 31 people),

In this example, clearly:

all clubs are distinct,

each club has an odd number of members because each club has all but one inhabitant from Eventown (and that's 31 people),

and the intersection is always even because it contains all but two members of Eventown (that's 30 people).

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

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

Exercise: Can you come up with more ways of forming 32 clubs?

Exercise: Can you come up with more ways of forming 32 clubs?

(Harder) Exercise: In how many ways can you form 32 clubs?

(Harder) Exercise: In how many ways can you form 32 clubs?

Non-Exercise: Can you form *more* than 32 clubs?

Non-Exercise: Can you form *more* than 32 clubs?

The answer is no.

Non-Exercise: Can you form *more* than 32 clubs?

The answer is no. And we'll see why.

Apart from knowing how to do linear combinations, we'll need to learn one more operation on indicator vectors:

the inner product.

Let $u = (u_1, u_2, \ldots, u_k)$ and $v = (v_1, v_2, \ldots, v_k)$ be two vectors.

Let $u = (u_1, u_2, \ldots, u_k)$ and $v = (v_1, v_2, \ldots, v_k)$ be two vectors.

Then the inner product of u and v is given by:

Let $u = (u_1, u_2, \ldots, u_k)$ and $v = (v_1, v_2, \ldots, v_k)$ be two vectors.

Then the inner product of u and v is given by:

$$u \cdot v = u_1 v_1 + u_2 v_2 + \cdots u_k v_k (\mathrm{mod} 2).$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 \qquad\qquad\qquad\qquad\qquad\qquad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 \qquad\qquad\qquad\qquad\qquad\qquad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 \qquad\qquad\qquad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 \qquad\qquad\qquad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 + 1 \qquad\qquad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 + 1 \qquad\qquad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 + 1 + 1 \quad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 + 1 + 1 \quad) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 + 1 + 1 + 0) \bmod 2$$

$$(0, 0, 1, 1, 0) \cdot (1, 0, 1, 1, 1)$$

$$(0 + 0 + 1 + 1 + 0) \bmod 2$$

$$(0,0,1,1,0) \cdot (1,0,1,1,1)$$

$$(0+0+1+1+0) \bmod 2 = 0$$

Observation: If u is an indicator vector of a club with an odd number of members, then

$$u \cdot u = 1.$$

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

.

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

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

.

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

$$(1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+0+1+0+0+1+1+1+1) \bmod 2$$

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

.

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

$$(1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+0+1+0+0+1+1+1+1) \bmod 2$$

Since there are odd number of members, there are an odd number of ones, so this sum comes out to be 1 (modulo 2).

Observation: If u and v are indicator vectors of clubs with an even number of common members, then

$$u \cdot v = 0.$$

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

.

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

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

.

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

Only points of intersection "survive" in the inner product:

$$(1+1+1+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+1+1+1) \bmod 2$$

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

.

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

Only points of intersection "survive" in the inner product:

$$(1+1+1+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+1+1+1) \bmod 2$$

Since there are an even number of common members, there are an even number of ones, so this sum comes out to be 0 (modulo 2).

Proof strategy....

Consider indicator vectors of clubs formed under the new rules.

Consider indicator vectors of clubs formed under the new rules.

Show that none of them can be generated from the rest, that is, they are linearly independent.

Consider indicator vectors of clubs formed under the new rules.

Show that none of them can be generated from the rest, that is, they are linearly independent.

This implies there cannot be more than 32 of them, because we have a basis of size 32.

Consider indicator vectors of clubs formed under the new rules.

Show that none of them can be generated from the rest, that is, they are linearly independent.

This implies there cannot be more than 32 of them, because we have a basis of size 32.

Proof: By contradiction.

Proof: By contradiction.

Suppose $\{v_1, v_2, \ldots, v_m\}$
is the collection of the indicator vectors of clubs formed under the new rules.

Proof: By contradiction.

Suppose $\{v_1, v_2, \ldots, v_m\}$
is the collection of the indicator vectors of clubs formed under the new rules.

Suppose (WLOG) v_1 can be generated from the rest, that is, can be written as a sum of some of the remaining vectors:

$$v_1 = v_{i_1} + v_{i_2} + \cdots + v_{i_r}.$$

$$v_1 = v_{i_1} + v_{i_2} + \cdots + v_{i_r}.$$

$$v_1 = v_{i_1} + v_{i_2} + \cdots + v_{i_r}.$$

Let's take inner product on both sides with v_1:

$$v_1 \cdot v_1 = (v_{i_1} \cdot v_1) + (v_{i_2} \cdot v_1) + \cdots + (v_{i_r} \cdot v_1).$$

$$v_1 = v_{i_1} + v_{i_2} + \cdots + v_{i_r}.$$

Let's take inner product on both sides with v_1:

$$v_1 \cdot v_1 = (v_{i_1} \cdot v_1) + (v_{i_2} \cdot v_1) + \cdots + (v_{i_r} \cdot v_1).$$

Then, by our first observation, the left-hand side is 1, and by our second observation, each term on the right hand size is 0

$$v_1 = v_{i_1} + v_{i_2} + \cdots + v_{i_r}.$$

Let's take inner product on both sides with v_1:

$$v_1 \cdot v_1 = (v_{i_1} \cdot v_1) + (v_{i_2} \cdot v_1) + \cdots + (v_{i_r} \cdot v_1).$$

Then, by our first observation, the left-hand side is 1, and by our second observation, each term on the right hand size is 0

$$1 = 0$$

$$v_1 = v_{i_1} + v_{i_2} + \cdots + v_{i_r}.$$

Let's take inner product on both sides with v_1:

$$v_1 \cdot v_1 = (v_{i_1} \cdot v_1) + (v_{i_2} \cdot v_1) + \cdots + (v_{i_r} \cdot v_1).$$

Then, by our first observation, the left-hand side is 1, and by our second observation, each term on the right hand size is 0

$$1 = 0$$

This is the end of the world, so this must mean that v_1 cannot be generated from the rest of the vectors (and this is true of any vector in the collection).

Therefore: no more than 32 clubs given the new regulations!

Therefore: no more than 32 clubs given the new regulations!

Exercise: Figure out where this proof breaks down if you try to mimic it with the old regulations.