Discrete Mathematical Models

Lecture 15

Kane Townsend

Semester 2, 2024

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI = B(AC)$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI = B(AC) = (BA)C$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so
$$B = BI = B(AC) = (BA)C = IC$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI = B(AC) = (BA)C = IC = C.$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then BA = I and AC = I and so

$$B = BI = B(AC) = (BA)C = IC = C.$$

How can we compute (the unique) A^{-1} when it does exist?

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI = B(AC) = (BA)C = IC = C.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(A) \neq 0$ and in this case

$$\boxed{A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI = B(AC) = (BA)C = IC = C.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(A) \neq 0$ and in this case

$$\boxed{A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(I_2)$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $\mathrm{BA} = \mathrm{I}$ and $\mathrm{AC} = \mathrm{I}$ and so

$$\mathrm{B} = \mathrm{BI} = \mathrm{B(AC)} = \mathrm{(BA)C} = \mathrm{IC} = \mathrm{C}.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(\mathrm{A}) \neq 0$ and in this case

$$\boxed{\mathrm{A}^{-1} = \frac{1}{\det(\mathrm{A})} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(\mathrm{I}_2) = \det(\mathrm{AA}^{-1})$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $BA = I$ and $AC = I$ and so

$$B = BI = B(AC) = (BA)C = IC = C.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(A) \neq 0$ and in this case

$$\boxed{A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(I_2) = \det(AA^{-1}) = \det(A)\det(A^{-1}),$$

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $\mathrm{BA} = \mathrm{I}$ and $\mathrm{AC} = \mathrm{I}$ and so

$$\mathrm{B} = \mathrm{BI} = \mathrm{B(AC)} = \mathrm{(BA)C} = \mathrm{IC} = \mathrm{C}.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(\mathrm{A}) \neq 0$ and in this case

$$\boxed{\mathrm{A}^{-1} = \frac{1}{\det(\mathrm{A})} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(\mathrm{I}_2) = \det(\mathrm{AA}^{-1}) = \det(\mathrm{A}) \det(\mathrm{A}^{-1}),$$

so $\det(\mathrm{A})$ cannot be zero.

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $\mathrm{BA} = \mathrm{I}$ and $\mathrm{AC} = \mathrm{I}$ and so

$$\mathrm{B} = \mathrm{BI} = \mathrm{B(AC)} = \mathrm{(BA)C} = \mathrm{IC} = \mathrm{C}.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(\mathrm{A}) \neq 0$ and in this case

$$\boxed{\mathrm{A}^{-1} = \frac{1}{\det(\mathrm{A})} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(\mathrm{I}_2) = \det(\mathrm{AA}^{-1}) = \det(\mathrm{A}) \det(\mathrm{A}^{-1}),$$

so $\det(\mathrm{A})$ cannot be zero. But if $\det(\mathrm{A}) \neq 0$ then multiplying out shows that $\mathrm{AA}^{-1} = \mathrm{A}^{-1}\mathrm{A} = \mathrm{I}$ when A^{-1} is given by the formula.

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $\mathrm{BA} = \mathrm{I}$ and $\mathrm{AC} = \mathrm{I}$ and so

$$\mathrm{B} = \mathrm{BI} = \mathrm{B}(\mathrm{AC}) = (\mathrm{BA})\mathrm{C} = \mathrm{IC} = \mathrm{C}.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(\mathrm{A}) \neq 0$ and in this case

$$\boxed{\mathrm{A}^{-1} = \frac{1}{\det(\mathrm{A})} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(\mathrm{I}_2) = \det(\mathrm{AA}^{-1}) = \det(\mathrm{A}) \det(\mathrm{A}^{-1}),$$

so $\det(\mathrm{A})$ cannot be zero. But if $\det(\mathrm{A}) \neq 0$ then multiplying out shows that $\mathrm{AA}^{-1} = \mathrm{A}^{-1}\mathrm{A} = \mathrm{I}$ when A^{-1} is given by the formula.

What about $n > 2$?

Calculating Inverses

A matrix A can have at most one inverse, because if B and C are both inverses then $\mathrm{BA} = \mathrm{I}$ and $\mathrm{AC} = \mathrm{I}$ and so

$$\mathrm{B} = \mathrm{BI} = \mathrm{B(AC)} = \mathrm{(BA)C} = \mathrm{IC} = \mathrm{C}.$$

How can we compute (the unique) A^{-1} when it does exist?

Theorem: A matrix $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ has an inverse if and only if $\det(\mathrm{A}) \neq 0$ and in this case

$$\boxed{\mathrm{A}^{-1} = \frac{1}{\det(\mathrm{A})} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \quad \textit{e.g.} \begin{pmatrix} 1 & -2 \\ 3 & 2 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} 2 & 2 \\ -3 & 1 \end{pmatrix}$$

Proof: If A has an inverse then

$$1 = \det(\mathrm{I}_2) = \det(\mathrm{AA}^{-1}) = \det(\mathrm{A}) \det(\mathrm{A}^{-1}),$$

so $\det(\mathrm{A})$ cannot be zero. But if $\det(\mathrm{A}) \neq 0$ then multiplying out shows that $\mathrm{AA}^{-1} = \mathrm{A}^{-1}\mathrm{A} = \mathrm{I}$ when A^{-1} is given by the formula.

What about $n > 2$? See Math1013 or Math1115.

Interesting Examples

Back to population dynamics

As a final example involving matrix multiplication and matrix inverses, we return to the simple ecosystem model

$$\forall n \in \mathbb{N} \quad \begin{cases} x_{n+1} = 4x_n - y_n, \\ y_{n+1} = y_n + 2x_n, \end{cases}$$

where x_n, y_n are the populations of two species after n time steps.

Back to population dynamics

As a final example involving matrix multiplication and matrix inverses, we return to the simple ecosystem model

$$\forall n \in \mathbb{N} \quad \begin{cases} x_{n+1} = 4x_n - y_n, \\ y_{n+1} = y_n + 2x_n, \end{cases}$$

where x_n, y_n are the populations of two species after n time steps.
We can rewrite this in the form

$$\forall n \in \mathbb{N} \quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

Back to population dynamics

As a final example involving matrix multiplication and matrix inverses, we return to the simple ecosystem model

$$\forall n \in \mathbb{N} \quad \begin{cases} x_{n+1} = 4x_n - y_n, \\ y_{n+1} = y_n + 2x_n, \end{cases}$$

where x_n, y_n are the populations of two species after n time steps.
We can rewrite this in the form

$$\forall n \in \mathbb{N} \quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

This is an implicit definition of a sequence of vectors. We will use mathematical induction to establish an explicit formula, stated and proved on the next slide.

Back to population dynamics

As a final example involving matrix multiplication and matrix inverses, we return to the simple ecosystem model

$$\forall n \in \mathbb{N} \quad \begin{cases} x_{n+1} = 4x_n - y_n, \\ y_{n+1} = y_n + 2x_n, \end{cases}$$

where x_n, y_n are the populations of two species after n time steps.
We can rewrite this in the form

$$\forall n \in \mathbb{N} \quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

This is an implicit definition of a sequence of vectors. We will use mathematical induction to establish an explicit formula, stated and proved on the next slide. First two preliminary results

R1: $\begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$ $\qquad \begin{bmatrix} \text{prove by multiplying} \\ \text{out the RHS} \end{bmatrix}$

Back to population dynamics

As a final example involving matrix multiplication and matrix inverses, we return to the simple ecosystem model

$$\forall n \in \mathbb{N} \quad \begin{cases} x_{n+1} = 4x_n - y_n, \\ y_{n+1} = y_n + 2x_n, \end{cases}$$

where x_n, y_n are the populations of two species after n time steps.
We can rewrite this in the form

$$\forall n \in \mathbb{N} \quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

This is an implicit definition of a sequence of vectors. We will use mathematical induction to establish an explicit formula, stated and proved on the next slide. First two preliminary results

R1: $\begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$ $\begin{bmatrix}\text{prove by multiplying} \\ \text{out the RHS}\end{bmatrix}$

R2: $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} = \dfrac{1}{2-1} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$ $\begin{bmatrix}\text{formula for} \\ \text{inverse of} \\ 2\times 2 \text{ matrix}\end{bmatrix}$

Claim: $\forall n \in \mathbb{N}^\star$ $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$

Claim: $\forall \boldsymbol{n} \in \mathbb{N}^\star \quad \begin{pmatrix} \boldsymbol{x_n} \\ \boldsymbol{y_n} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{\boldsymbol{n}} & 0 \\ 0 & 2^{\boldsymbol{n}} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_0 \\ \boldsymbol{y}_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

Claim: $\forall \boldsymbol{n} \in \mathbb{N}^\star \quad \begin{pmatrix} \boldsymbol{x_n} \\ \boldsymbol{y_n} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{\boldsymbol{n}} & 0 \\ 0 & 2^{\boldsymbol{n}} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_0 \\ \boldsymbol{y}_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS.}$$

Claim: $\forall \boldsymbol{n} \in \mathbb{N}^\star \quad \begin{pmatrix} \boldsymbol{x_n} \\ \boldsymbol{y_n} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{\boldsymbol{n}} & 0 \\ 0 & 2^{\boldsymbol{n}} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_0 \\ \boldsymbol{y}_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{aligned}
\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS.}
\end{aligned}$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n + 1$.

Claim: $\forall \boldsymbol{n} \in \mathbb{N}^{\star}$ $$\begin{pmatrix} \boldsymbol{x_n} \\ \boldsymbol{y_n} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{\boldsymbol{n}} & 0 \\ 0 & 2^{\boldsymbol{n}} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_0 \\ \boldsymbol{y}_0 \end{pmatrix}$$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS}. \end{aligned}$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n+1$. Then, using the implicit definition, preliminary results R1 and R2, and the inductive assumption,

Claim: $\forall n \in \mathbb{N}^\star$ $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS.}$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n + 1$. Then, using the implicit definition, preliminary results R1 and R2, and the inductive assumption,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Claim: $\forall \boldsymbol{n} \in \mathbb{N}^\star$ $$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS}.$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n + 1$. Then, using the implicit definition, preliminary results R1 and R2, and the inductive assumption,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Claim: $\forall \boldsymbol{n} \in \mathbb{N}^\star \quad \begin{pmatrix} \boldsymbol{x_n} \\ \boldsymbol{y_n} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{\boldsymbol{n}} & 0 \\ 0 & 2^{\boldsymbol{n}} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_0 \\ \boldsymbol{y}_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS}.$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n + 1$. Then, using the implicit definition, preliminary results R1 and R2, and the inductive assumption,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

Claim: $\forall n \in \mathbb{N}^\star$ $\quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS}.$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n+1$. Then, using the implicit definition, preliminary results R1 and R2, and the inductive assumption,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{n+1} & 0 \\ 0 & 2^{n+1} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

and hence the formula also holds for $n+1$.

Claim: $\forall n \in \mathbb{N}^\star$ $\quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$

Proof:

Basis step: When $n = 0$ the RHS becomes (using R2)

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \text{LHS}.$$

Inductive step: Assume the explicit formula holds up to and including some particular n, and consider the case $n+1$. Then, using the implicit definition, preliminary results R1 and R2, and the inductive assumption,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3^{n+1} & 0 \\ 0 & 2^{n+1} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

and hence the formula also holds for $n+1$.

Fibonacci Sequence

Recall the Fibonacci sequence $(F_n)_{n\geq 0} = (1, 1, 2, 3, 5, 8, 13, 21, ...)$

It has implicit formula, $F_0 = 1, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}, \forall n \geq 2$.

Fibonacci Sequence

Recall the Fibonacci sequence $(F_n)_{n\geq 0} = (1, 1, 2, 3, 5, 8, 13, 21, ...)$

It has implicit formula, $F_0 = 1, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}, \forall n \geq 2$.

For all $n \geq 1$ we have:

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$$

Fibonacci Sequence

Recall the Fibonacci sequence $(F_n)_{n\geq 0} = (1, 1, 2, 3, 5, 8, 13, 21, ...)$

It has implicit formula, $F_0 = 1, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}, \forall n \geq 2$.

For all $n \geq 1$ we have:

$$\begin{aligned}\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \\ &= \tfrac{1}{\sqrt{5}} \begin{pmatrix} \varphi & -\varphi^{-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \varphi & 0 \\ 0 & -\varphi^{-1} \end{pmatrix} \begin{pmatrix} 1 & \varphi^{-1} \\ -1 & \varphi \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}\end{aligned}$$

Fibonacci Sequence

Recall the Fibonacci sequence $(F_n)_{n\geq 0} = (1, 1, 2, 3, 5, 8, 13, 21, ...)$

It has implicit formula, $F_0 = 1, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}, \forall n \geq 2$.

For all $n \geq 1$ we have:

$$\begin{aligned}
\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \\
&= \frac{1}{\sqrt{5}} \begin{pmatrix} \varphi & -\varphi^{-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \varphi & 0 \\ 0 & -\varphi^{-1} \end{pmatrix} \begin{pmatrix} 1 & \varphi^{-1} \\ -1 & \varphi \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \\
&= \frac{1}{\sqrt{5}} \begin{pmatrix} \varphi & -\varphi^{-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \varphi^n & 0 \\ 0 & (-\varphi)^{-n} \end{pmatrix} \begin{pmatrix} 1 & \varphi^{-1} \\ -1 & \varphi \end{pmatrix} \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}
\end{aligned}$$

where $\varphi = \frac{1+\sqrt{5}}{2}$. We can extract an explicit formula for the Fibonacci sequence!

C1: Counting

Cardinality

This section is mostly about calculating the number of objects of some specified type; for example counting all five digit numbers with no repeated digits. Counting like this can be viewed as finding the number of members of some set, also known as finding the *size* of the set.

Cardinality

This section is mostly about calculating the number of objects of some specified type; for example counting all five digit numbers with no repeated digits. Counting like this can be viewed as finding the number of members of some set, also known as finding the *size* of the set.

For a finite set A, this 'size' or 'cardinality' is just the number of members of A. However it can be defined formally as follows:

Cardinality

This section is mostly about calculating the number of objects of some specified type; for example counting all five digit numbers with no repeated digits. Counting like this can be viewed as finding the number of members of some set, also known as finding the *size* of the set.

For a finite set A, this 'size' or 'cardinality' is just the number of members of A. However it can be defined formally as follows:

Let A be a set. Suppose there exists a bijection (one-to-one correspondence) from A to a subset of the natural numbers of the form $\{1, 2, ..., n\}$ for some $n \in \mathbb{N}$. Then the **cardinality**, or **size** of the set A, written $|A|$, is n. Thus $|A| = n$.

Cardinality

This section is mostly about calculating the number of objects of some specified type; for example counting all five digit numbers with no repeated digits. Counting like this can be viewed as finding the number of members of some set, also known as finding the *size* of the set.

For a finite set A, this 'size' or 'cardinality' is just the number of members of A. However it can be defined formally as follows:

Let A be a set. Suppose there exists a bijection (one-to-one correspondence) from A to a subset of the natural numbers of the form $\{1, 2, ..., n\}$ for some $n \in \mathbb{N}$. Then the **cardinality**, or **size** of the set A, written $|A|$, is n. Thus $|A| = n$.

Intervals

Example: numbers in an interval

What is the cardinality of the set of natural numbers in an interval?

Example: $S = \{150, 151, 152, ..., 160\}$

Subtract 149 from each:
$$\begin{array}{ccccc} 150 & 151 & 152 & ... & 160 \\ \downarrow & \downarrow & \downarrow & ... & \downarrow \\ 1 & 2 & 3 & ... & 11 \end{array}$$

We have made a bijection to the set $\{1, 2, 3, ..., 11\}$, so $|S| = 11$.

Example: numbers in an interval, generalized

Let $S = \{a, a+1, a+2, ..., b\} \subseteq \mathbb{N}$

A nice bijection subtracts '$a - 1$' from each element of S. We have

$$\begin{array}{ccccc} a & a+1 & a+2 & \cdots & b \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ 1 & 2 & 3 & \cdots & b-a+1 \end{array}$$

Therefore $|S| = b - a + 1$.

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

150 mod $7 = 3$ so the lowest number is $150 + 2 = 152$.

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

150 mod $7 = 3$ so the lowest number is $150 + 2 = 152$.

330 mod $7 = 1$ so the highest number is $330 - 3 = 327$.

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

150 mod $7 = 3$ so the lowest number is $150 + 2 = 152$.

330 mod $7 = 1$ so the highest number is $330 - 3 = 327$.

Now use the following composition of bijections:

$$\begin{array}{lccccc} & 152 & 159 & 166 & \cdots & 327 \\ \text{subtract 5:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ & 147 & 154 & 161 & \cdots & 322 \end{array}$$

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

150 mod $7 = 3$ so the lowest number is $150 + 2 = 152$.

330 mod $7 = 1$ so the highest number is $330 - 3 = 327$.

Now use the following composition of bijections:

$$\begin{array}{rccccc} & 152 & 159 & 166 & \cdots & 327 \\ \text{subtract 5:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ & 147 & 154 & 161 & \cdots & 322 \\ \text{divide by 7:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ & 21 & 22 & 23 & \cdots & 46 \end{array}$$

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

150 mod $7 = 3$ so the lowest number is $150 + 2 = 152$.

330 mod $7 = 1$ so the highest number is $330 - 3 = 327$.

Now use the following composition of bijections:

$$\begin{array}{rccccc}
 & 152 & 159 & 166 & \cdots & 327 \\
\text{subtract 5:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
 & 147 & 154 & 161 & \cdots & 322 \\
\text{divide by 7:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
 & 21 & 22 & 23 & \cdots & 46 \\
\text{subtract 20:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
 & 1 & 2 & 3 & \cdots & 26
\end{array}$$

A slightly harder but similar example

How many numbers from 150 to 330 inclusive are congruent to 5 mod 7?

150 mod $7 = 3$ so the lowest number is $150 + 2 = 152$.

330 mod $7 = 1$ so the highest number is $330 - 3 = 327$.

Now use the following composition of bijections:

$$
\begin{array}{rccccc}
 & 152 & 159 & 166 & \cdots & 327 \\
\text{subtract 5:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
 & 147 & 154 & 161 & \cdots & 322 \\
\text{divide by 7:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
 & 21 & 22 & 23 & \cdots & 46 \\
\text{subtract 20:} & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
 & 1 & 2 & 3 & \cdots & 26
\end{array}
$$

Since the composition of bijections is a bijection, the answer is 26.

Countable sets

Finite and infinite sets

The **cardinality of the empty set** is defined to be 0. Thus $|\emptyset| = 0$.

Finite and infinite sets

The **cardinality of the empty set** is defined to be 0. Thus $|\emptyset| = 0$.

Any set S with cardinality $|S| = n \in \mathbb{N}^\star$ it is said to be **finite**.

Finite and infinite sets

The **cardinality of the empty set** is defined to be 0. Thus $|\emptyset| = 0$.

Any set S with cardinality $|S| = n \in \mathbb{N}^\star$ it is said to be **finite**.

Any set S that is not finite is said to be **infinite**. We write $|S| = \infty$.

Finite and infinite sets

The **cardinality of the empty set** is defined to be 0. Thus $|\emptyset| = 0$.

Any set S with cardinality $|S| = n \in \mathbb{N}^\star$ it is said to be **finite**.

Any set S that is not finite is said to be **infinite**. We write $|S| = \infty$.

Examples:

Finite Sets	Infinite Sets
$\{1, 2, 3\}$	$\mathbb{N}$ ... natural numbers
{red, orange, yellow, green, blue, purple}	$\mathbb{Z}$ ... integers
$\{b$: b is a book in the Hancock library$\}$	$\mathbb{Q}$ ... rational numbers
$\{s$: s is a star in the Milky Way Galaxy$\}$	$\mathbb{R}$ ... real numbers
$\{\}$	$\mathcal{P}(\mathbb{R})$ ... power set of $\mathbb{R}$

Countability

A set S is called **countable** when there is a bijection from S to a subset of the set $\mathbb{N}$ of natural numbers.
Examples:

Any *finite* set is countable.

Countability

A set S is called **countable** when there is a bijection from S to a subset of the set $\mathbb{N}$ of natural numbers.
Examples:

Any *finite* set is countable.

The *empty set* is countable (because $\emptyset \subseteq \mathbb{N}$).

Countability

A set S is called **countable** when there is a bijection from S to a subset of the set $\mathbb{N}$ of natural numbers. Examples:

Any *finite* set is countable.

The *empty set* is countable (because $\emptyset \subseteq \mathbb{N}$).

The set of all primes is countable (because $\subseteq \mathbb{N}$).

$\mathbb{N}$ itself is countable (because $\mathbb{N} \subseteq \mathbb{N}$).

Countability

A set S is called **countable** when there is a bijection from S to a subset of the set $\mathbb{N}$ of natural numbers.
Examples:

Any *finite* set is countable.

The *empty set* is countable (because $\emptyset \subseteq \mathbb{N}$).

The set of all primes is countable (because $\subseteq \mathbb{N}$).

$\mathbb{N}$ itself is countable (because $\mathbb{N} \subseteq \mathbb{N}$).

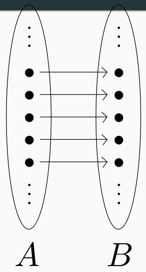
The sets $\mathbb{N}$ and $\mathbb{P}$ are each both countable and infinite.
Such sets are called **countably infinite**.

Comparing cardinalities

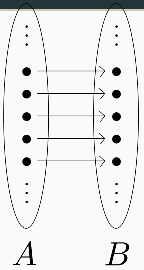
Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.

Comparing cardinalities

Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.



Comparing cardinalities



Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.

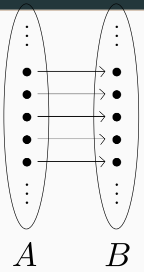
Remember that for $\phi : A \to B$ to be a bijection:

- no two arrows point to the same element of B, *i.e.*

$$\forall x, y \in A \;\; x \neq y \implies \phi(x) \neq \phi(y).$$

Comparing cardinalities

Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.

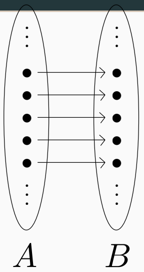


Remember that for $\phi : A \to B$ to be a bijection:

- no two arrows point to the same element of B, *i.e.*
$$\forall x, y \in A \;\; x \neq y \implies \phi(x) \neq \phi(y).$$
- each element of B must have an arrow pointing to it: *i.e.*
$$\forall b \in B \; \exists a \in A \;\; \phi(a) = b.$$

Comparing cardinalities

Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.



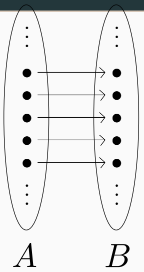
Remember that for $\phi : A \to B$ to be a bijection:

- no two arrows point to the same element of B, *i.e.*
$$\forall x, y \in A \;\; x \neq y \implies \phi(x) \neq \phi(y).$$
- each element of B must have an arrow pointing to it: *i.e.*
$$\forall b \in B \; \exists a \in A \;\; \phi(a) = b.$$

Also remember that $\phi : A \to B$ is a bijection if and only if it has an inverse $\phi^{-1} : B \to A$.

Comparing cardinalities

Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.



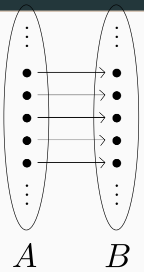
Remember that for $\phi : A \to B$ to be a bijection:

- no two arrows point to the same element of B, *i.e.*
$$\forall x, y \in A \;\; x \neq y \implies \phi(x) \neq \phi(y).$$
- each element of B must have an arrow pointing to it: *i.e.*
$$\forall b \in B \; \exists a \in A \;\; \phi(a) = b.$$

Also remember that $\phi : A \to B$ is a bijection if and only if it has an inverse $\phi^{-1} : B \to A$.
Since the inverse is also a bijection, we say that A and B have the same cardinality if and only if there is a bijection between them.

Comparing cardinalities

Generalising from the case of finite sets, we say that two sets A and B have **the same cardinality**, written $|A| = |B|$, provided that there exists a bijection (one-to-one correspondence) from A to B.



Remember that for $\phi : A \to B$ to be a bijection:

- no two arrows point to the same element of B, *i.e.*
$$\forall x, y \in A \;\; x \neq y \implies \phi(x) \neq \phi(y).$$
- each element of B must have an arrow pointing to it: *i.e.*
$$\forall b \in B \; \exists a \in A \;\; \phi(a) = b.$$

Also remember that $\phi : A \to B$ is a bijection if and only if it has an inverse $\phi^{-1} : B \to A$.
Since the inverse is also a bijection, we say that A and B have the same cardinality if and only if there is a bijection between them. (i.e. we don't have to specify the direction of the function).

Examples of sets with the same cardinality

1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.

Examples of sets with the same cardinality

1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.

But actually the two sets have the **same** cardinality

Examples of sets with the same cardinality

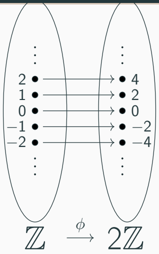
1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.

But actually the two sets have the **same** cardinality, because the function $\quad \phi : \mathbb{Z} \to 2\mathbb{Z} : \quad \phi(z) = 2z \quad$ is (clearly) a bijection.

Examples of sets with the same cardinality

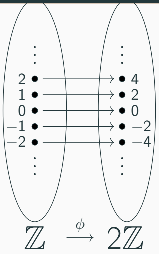
1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.

But actually the two sets have the **same** cardinality, because the function $\quad \phi : \mathbb{Z} \to 2\mathbb{Z} : \quad \phi(z) = 2z \quad$ is (clearly) a bijection.



Examples of sets with the same cardinality

1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.
But actually the two sets have the **same** cardinality, because the function $\phi : \mathbb{Z} \to 2\mathbb{Z} : \quad \phi(z) = 2z$ is (clearly) a bijection.

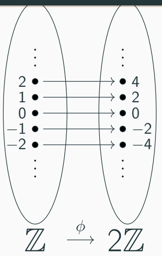


2 By tweaking the function ϕ a little we can establish the perhaps more surprising fact that $\mathbb{Z}$ also has the same cardinality as $\mathbb{N}$.

Examples of sets with the same cardinality

1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.

But actually the two sets have the **same** cardinality, because the function $\phi : \mathbb{Z} \to 2\mathbb{Z} : \quad \phi(z) = 2z$ is (clearly) a bijection.



2 By tweaking the function ϕ a little we can establish the perhaps more surprising fact that $\mathbb{Z}$ also has the same cardinality as $\mathbb{N}$.

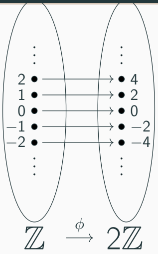
The modified version of ϕ is

$$\phi : \mathbb{Z} \to \mathbb{N} : \quad \phi(z) = \begin{cases} 2z & \text{if } z > 0 \\ 1 - 2z & \text{if } z \leq 0 \end{cases}$$

Examples of sets with the same cardinality

1 You might expect the set $\mathbb{Z}$ of integers to have a 'bigger' cardinality than the set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers, since there are 'twice as many' integers as even integers.

But actually the two sets have the **same** cardinality, because the function $\phi : \mathbb{Z} \to 2\mathbb{Z} : \quad \phi(z) = 2z$ is (clearly) a bijection.

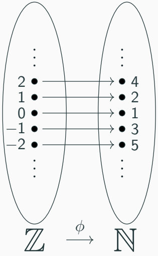


2 By tweaking the function ϕ a little we can establish the perhaps more surprising fact that $\mathbb{Z}$ also has the same cardinality as $\mathbb{N}$.

The modified version of ϕ is

$$\phi : \mathbb{Z} \to \mathbb{N} : \quad \phi(z) = \begin{cases} 2z & \text{if } z > 0 \\ 1 - 2z & \text{if } z \leq 0 \end{cases}$$

It not difficult to see that this is a bijection.



All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.

All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.
In other words, S has the same cardinality as some infinite subset of $\mathbb{N}$.

All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.

In other words, S has the same cardinality as some infinite subset of $\mathbb{N}$.

However

Any infinite subset S of $\mathbb{N}$ has the same cardinality as $\mathbb{N}$ itself.

All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.
In other words, S has the same cardinality as some infinite subset of $\mathbb{N}$.
However

Any infinite subset S of $\mathbb{N}$ has the same cardinality as $\mathbb{N}$ itself.

Proof: Since every bijection has an inverse, it is enough to establish a bijection $\phi : \mathbb{N} \to S$.

All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.
In other words, S has the same cardinality as some infinite subset of $\mathbb{N}$.
However

Any infinite subset S of $\mathbb{N}$ has the same cardinality as $\mathbb{N}$ itself.

Proof: Since every bijection has an inverse, it is enough to establish a bijection $\phi : \mathbb{N} \to S$. This can be done recursively as follows:

$$\begin{aligned} \phi(1) &= \text{least member of } S \\ \phi(2) &= \text{least member of } S \setminus \{\phi(1)\} \quad (2^{\text{nd}} \text{ least member}) \\ \forall n \in \mathbb{N} \ \ \phi(n+1) &= \text{least member of } S \setminus \{\phi(1), \ldots, \phi(n)\}. \end{aligned}$$

All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.
In other words, S has the same cardinality as some infinite subset of $\mathbb{N}$.
However

Any infinite subset S of $\mathbb{N}$ has the same cardinality as $\mathbb{N}$ itself.

Proof: Since every bijection has an inverse, it is enough to establish a bijection $\phi : \mathbb{N} \to S$. This can be done recursively as follows:

$$\begin{aligned}
\phi(1) &= \text{least member of } S \\
\phi(2) &= \text{least member of } S \setminus \{\phi(1)\} \quad (2^{\text{nd}} \text{ least member}) \\
\forall n \in \mathbb{N} \;\; \phi(n+1) &= \text{least member of } S \setminus \{\phi(1), \ldots, \phi(n)\}.
\end{aligned}$$

Note: It follows from the result above (and its proof) that proving that an arbitrary infinite set S (not necessarily a subset of $\mathbb{N}$) is countably infinite amounts to showing that it can be '**well-ordered**'.

All countably infinite sets have the same cardinality

Recall that we call a set S countably infinite if (and only if) it is infinite and there is a bijection from S to a subset of $\mathbb{N}$.
In other words, S has the same cardinality as some infinite subset of $\mathbb{N}$.
However

Any infinite subset S of $\mathbb{N}$ has the same cardinality as $\mathbb{N}$ itself.

Proof: Since every bijection has an inverse, it is enough to establish a bijection $\phi : \mathbb{N} \to S$. This can be done recursively as follows:

$$\begin{aligned} \phi(1) &= \text{least member of } S \\ \phi(2) &= \text{least member of } S \backslash \{\phi(1)\} \quad (2^{\text{nd}} \text{ least member}) \\ \forall n \in \mathbb{N} \;\; \phi(n+1) &= \text{least member of } S \backslash \{\phi(1), \ldots, \phi(n)\}. \end{aligned}$$

Note: It follows from the result above (and its proof) that proving that an arbitrary infinite set S (not necessarily a subset of $\mathbb{N}$) is countably infinite amounts to showing that it can be '**well-ordered**'. This means that it is possible to order the elements of S in some (perhaps ingenious) way so that S and every subset of S has a 'least' member.

Not all infinite sets have the same cardinality

The most surprising fact we will see is that $\mathbb{Q}$ is countable. This is shown by describing a bijection from $\mathbb{N}$ to $\mathbb{Q}$. Since every bijection has an inverse that is a bijection, this suffices to show that there exists a bijection from $\mathbb{Q}$ to $\mathbb{N}$.

However, $\mathbb{R}$, the set of real numbers, is uncountable. This is proven by showing there is no surjection (and hence no bijection) from $\mathbb{N}$ to $\mathbb{R}$. It follows that there is no bijection from $\mathbb{R}$ to $\mathbb{N}$.

So we have

$$|\mathbb{N}| = |\mathbb{N}^\star| = |\mathbb{Z}| = |\mathbb{Q}|$$

but

$$|\mathbb{N}| \neq |\mathbb{R}|.$$

These observations, first made by Georg Cantor (1845-1918), were a breakthrough in mathematical thinking about infinite sets. We will have a look at the proofs next week!

Principles of counting

How do we count?

How do we count? We have a collection of counting principles. When we need to count some objects, we analyse those objects until we carefully match the situation to one of the situations in which a counting principle applies.

What makes counting hard? Matching your scenario to one of the scenarios described in a counting principle takes care, as the scenarios described in the counting principles sound similar unless you read carefully.

What is your best strategy? Understand the scenarios described in the counting principles. In particular, carefully notice how the scenarios are different. Then, when you have to count something and you think that a counting principle applies, **state which counting principle you are using and explain carefully (write it out) how you know that the situation you have is like the scenario described in the counting principle**.

The structures we count

We have already discussed sets, n-tuples, lists and sequences. In a set, order is unimportant and for elements in a set there is no notion of "how many times" the element is in the set. Lists, n-tuples and sequences are different ways to talks about the same thing—order matters and elements can appear more than once unless explicitly excluded by the language. We need one more structure, one that recognises multiplicty (how many times an element appears) but not order (there is no first element, second element etc)....

Multisets

A multiset is a ‘set’ with multiple copies of elements allowed and acknowledged.

Multisets

A multiset is a 'set' with multiple copies of elements allowed and acknowledged. An example is $\{c, b, a, c, a\}$, which has 2 a's, 1 b and 2 c's.

As for ordinary sets, order is irrelevant: $\{c, b, a, c, a\} = \{a, a, b, c, c\}$.

But the multiplicities **do** matter.

Formally, a **size-r multiset** is a set S together with a 'multiplicity function' $m : S \to \mathbb{N}$, where,

$$\forall s \in S \quad m(s) = \text{number of copies of } s \quad \text{and} \qquad r = \textstyle\sum_{s \in S} m(s).$$

So, for example, $\{c, b, a, c, a\}$ has size $r = 2 + 1 + 2 = 5$.

Principles of counting

Bijections preserve cardinality If A and B are finite sets and there exists a bijection $f : A \to B$, then $|A| = |B|$.
TO USE THIS PRINCIPLE: Count something easier, and exhibit a bijection between the set you which to count and the set you have counted.

The Pigeonhole Principle If $k + 1$ or more pigeons occupy k pigeonholes, then at least one pigeonhole must contain two or more pigeons.

The Generalised Pigeonhole Principle If N objects are classified in k disjoint categories, then at least one category must contain $\lceil \frac{N}{k} \rceil$ objects. ($\lceil \frac{N}{k} \rceil$ means the least integer that is greater than or equal to $\frac{N}{k}$)

Permutations There are $n!$ ways to arrange n distinct objects in a list.

r-**Permutations** There are

$$P(n, r) = \frac{n!}{(n-r)!}$$

ways to select and order r out of n distinct objects.

Combinations There are

$$C(n, r) = \binom{n}{r} = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}$$

ways to choose a set of r objects from a set of n objects (that is, to select r out of n distinct objects when the order in which objects are selected in not important). The notation $\binom{n}{r}$ is read "n choose r."

Principles of counting

Multisets (Stars and Bars) There are $\binom{r+n-1}{r}$ size-r multisets with members from a set of size n. That is, there are $\binom{r+n-1}{r}$ ways to arrange a list of r stars and $n-1$ bars.

Inclusion-Exclusion If A and B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$.

The Sum Rule If A is a finite set and $\{A_1, A_2, \ldots, A_m\}$ is a partition of A, then $|A| = |A_1| + |A_2| + \cdots + |A_m|$.

The Product Rule If $A_1, A_2, \ldots, A_m$ are finite sets, then $|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \times |A_2| \times \cdots \times |A_m|$.

Example 1

Prove the following: If A is a non-empty finite set, then $|\mathcal{P}(A)| = 2^{|A|}$.

Example 1

Prove the following: If A is a non-empty finite set, then $|\mathcal{P}(A)| = 2^{|A|}$.

IDEA: A subset of A corresponds to making one of two choices for each element of A: include it in the subset or not. These choices could be recorded as a bit-string. So elements of $\mathcal{P}(A)$ can be counted by counting bit-strings...

Proof: Let A be a non-empty finite set. Let $n = |A|$. Let B be the set of n-bit strings. When representing integers, the smallest element of B represents 0 and the largest represents $2^n - 1$; it follows that $|B| = 2^n$. Since **bijections preserve cardinality**, to prove the result, it is enough to exhibit a bijection from B to $\mathcal{P}(A)$. Let $f : A \to \{1, 2, \ldots, n\}$ be a bijection. Let $g : B \to \mathcal{P}(A)$ be the function defined by the rule $b_1 b_2 \ldots b_n \mapsto \{a \in A \mid b_{f(a)} = 1\}$. We leave the reader to verify that g is a bijection. $\square$

An example illustrating the functions in Example 1

Let $A = \{\text{cat}, \text{dog}, \text{chicken}\}$. Then $n = 3$ and

$$B = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Let $f : A \to \{1, 2, 3\}$ be the function defined by

$$f(\text{cat}) = 1, f(\text{dog}) = 2, f(\text{chicken}) = 3.$$

Then

$$g(011) = \{\text{dog}, \text{chicken}\}$$
$$g(101) = \{\text{cat}, \text{chicken}\}$$
$$g(000) = \emptyset$$
$$g(100) = \{\text{cat}\}$$