Review

Now...

Induction

$$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$$

Induction

$$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$$

Thm: For all $n \geq 1$, $8|3^{2n} - 1$.

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n)$.

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n)$.

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.

Induction Step: Prove $P(n+1)$

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8|3^{2n} - 1$.

Induction on n.

Base: $8|3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.

Induction Step: Prove $P(n+1)$

$3^{2n+2} - 1 =$

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n)$.

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.

Induction Step: Prove $P(n+1)$

$3^{2n+2} - 1 = 9(3^{2n}) - 1$

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$3^{2n+2} - 1 = 9(3^{2n}) - 1$ (by induction hypothesis)

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2} - 1 &= 9(3^{2n}) - 1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1) - 1 \end{aligned}$$

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n)$.

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2} - 1 &= 9(3^{2n}) - 1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1) - 1 \\ &= 72d + 8 \end{aligned}$$

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8|3^{2n} - 1$.

Induction on n.

Base: $8|3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2} - 1 &= 9(3^{2n}) - 1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1) - 1 \\ &= 72d + 8 \\ &= 8(9d+1) \end{aligned}$$

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n)$.

Thm: For all $n \geq 1$, $8|3^{2n} - 1$.

Induction on n.

Base: $8|3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2} - 1 &= 9(3^{2n}) - 1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1) - 1 \\ &= 72d + 8 \\ &= 8(9d+1) \end{aligned}$$

Divisible by 8.

Induction

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n).$

Thm: For all $n \geq 1$, $8|3^{2n}-1$.

Induction on n.

Base: $8|3^2-1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n}-1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2}-1 &= 9(3^{2n})-1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1)-1 \\ &= 72d+8 \\ &= 8(9d+1) \end{aligned}$$

Divisible by 8.

$\square$

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list

Stable Marriage: a study in definitions and WOP.

n-men, *n*-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Stable Marriage: a study in definitions and WOP.

n-men, *n*-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs?

Stable Marriage: a study in definitions and WOP.

n-men, *n*-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? *n*.

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? n.
People in pair are **partners** in pairing.

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? n.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Marriage: a study in definitions and WOP.

n-men, *n*-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? *n*.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? n.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? n.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.
Pairing with no rogue couples.

Stable Marriage: a study in definitions and WOP.

n-men, *n*-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? *n*.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.
Pairing with no rogue couples.

Does stable pairing exist?

Stable Marriage: a study in definitions and WOP.

n-men, *n*-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? *n*.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.
Pairing with no rogue couples.

Does stable pairing exist?

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? n.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.
Pairing with no rogue couples.

Does stable pairing exist?

No, for roommates problem.

TMA.

Traditional Marriage Algorithm:

TMA.

Traditional Marriage Algorithm:

Each Day:

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject."

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\implies$ any future man on string is better.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\Longrightarrow$ any future man on string is better.

Stability:

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\Longrightarrow$ any future man on string is better.

Stability: No rogue couple.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\implies$ any future man on string is better.

Stability: No rogue couple.
rogue couple (M,W)

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\implies$ any future man on string is better.

Stability: No rogue couple.
rogue couple (M,W)
$\implies$ M proposed to W

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\Longrightarrow$ any future man on string is better.

Stability: No rogue couple.
rogue couple (M,W)
$\Longrightarrow$ M proposed to W
$\Longrightarrow$ W ended up with someone she liked better than M.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\Longrightarrow$ any future man on string is better.

Stability: No rogue couple.
rogue couple (M,W)
$\Longrightarrow$ M proposed to W
$\Longrightarrow$ W ended up with someone she liked better than M.
Not rogue couple!

...Graphs...

$$G = (V, E)$$

...Graphs...

$G = (V, E)$
V - set of vertices.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:
If there is a path between them.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:
If there is a path between them.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:
If there is a path between them.

Connected Component: maximal set of connected vertices.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:
If there is a path between them.

Connected Component: maximal set of connected vertices.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:
If there is a path between them.

Connected Component: maximal set of connected vertices.

Connected Graph: one connected component.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Proof Idea: Even degree.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Proof Idea: Even degree.

Recurse on connected components.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Proof Idea: Even degree.

Recurse on connected components.

Put together.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Proof Idea: Even degree.

Recurse on connected components.

Put together.

Property: walk visits every component.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Proof Idea: Even degree.

Recurse on connected components.

Put together.

Property: walk visits every component.

Proof Idea: Original graph connected.

Graph Algorithm: Eulerian Tour

Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:

Take a walk using each edge at most once.

Property: return to starting point.

Proof Idea: Even degree.

Recurse on connected components.

Put together.

Property: walk visits every component.

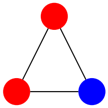
Proof Idea: Original graph connected.

Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

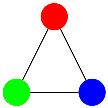
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



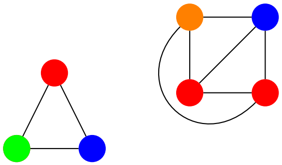
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



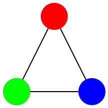
Graph Coloring.

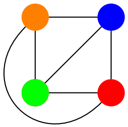
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Graph Coloring.

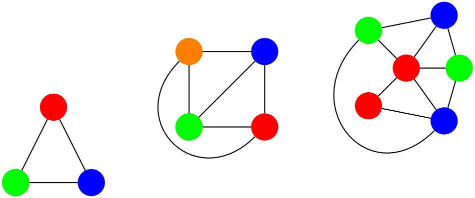
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.





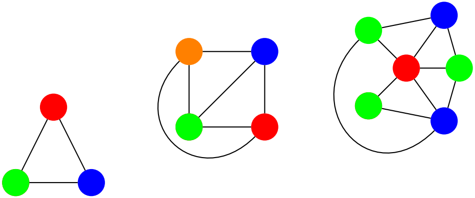
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



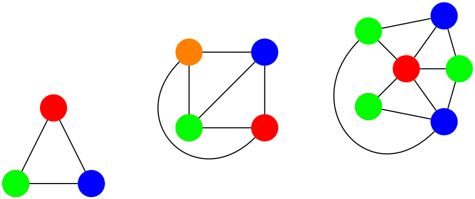
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



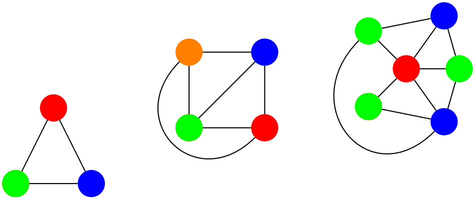
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Graph Coloring.

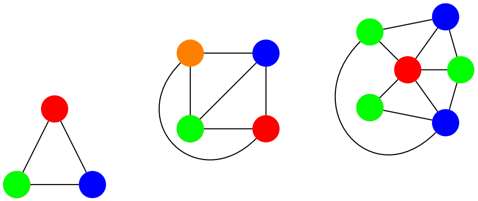
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.

Graph Coloring.

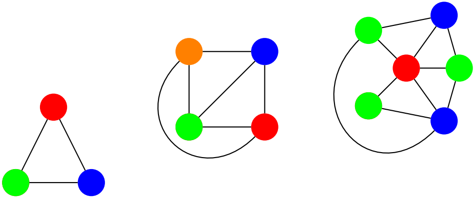
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.
Fewer colors than number of vertices.

Graph Coloring.

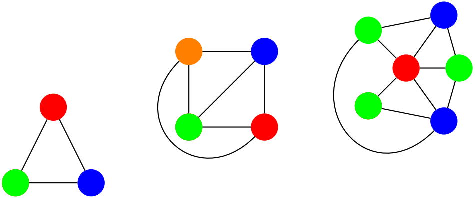
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Graph Coloring.

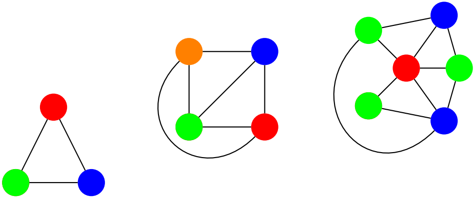
Given $G = (V,E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

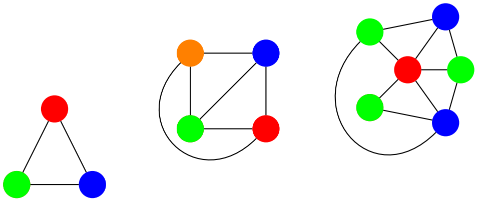


Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Interesting things to do.

Graph Coloring.

Given $G = (V,E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

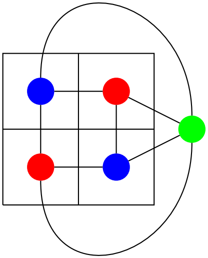


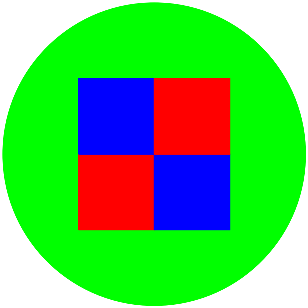
Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Interesting things to do. Algorithm!

Planar graphs and maps.

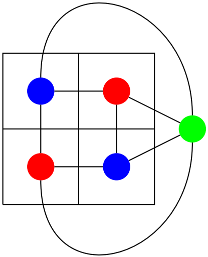
Planar graph coloring $\equiv$ map coloring.

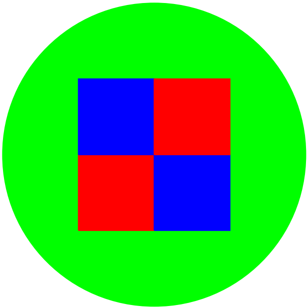




Planar graphs and maps.

Planar graph coloring $\equiv$ map coloring.





Four color theorem is about planar graphs!

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v}$

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v}$

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...
and only five colors are used.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

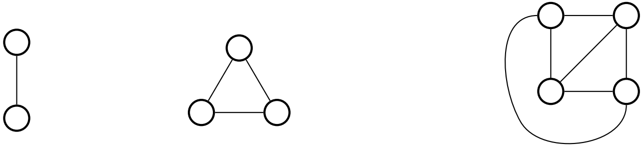
Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

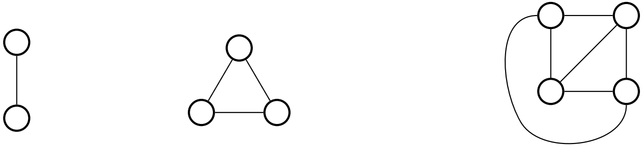
There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...
and only five colors are used. □

Graph Types: Complete Graph.

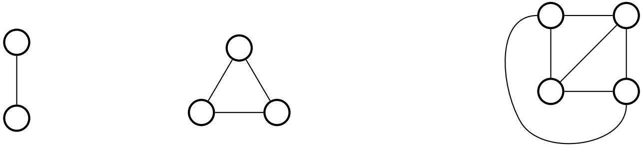


Graph Types: Complete Graph.



K_n, $|V| = n$

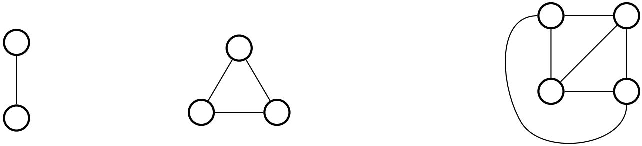
Graph Types: Complete Graph.



K_n, $|V| = n$

every edge present.

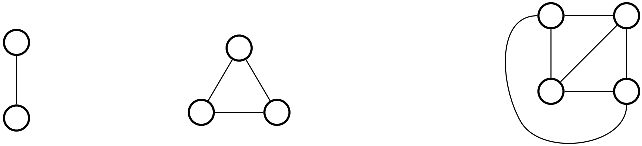
Graph Types: Complete Graph.



K_n, $|V| = n$

every edge present.
degree of vertex?

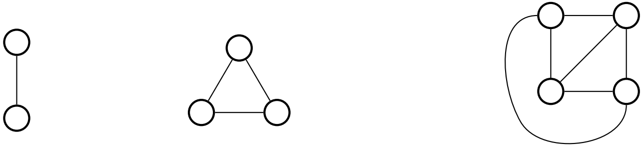
Graph Types: Complete Graph.



K_n, $|V| = n$

every edge present.
degree of vertex? $|V| - 1$.

Graph Types: Complete Graph.

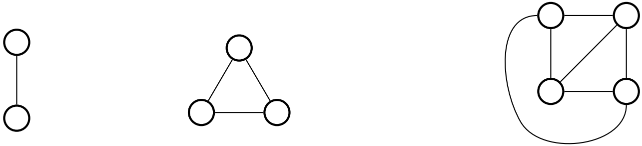


K_n, $|V| = n$

every edge present.
degree of vertex? $|V| - 1$.

Very connected.

Graph Types: Complete Graph.

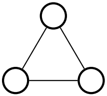


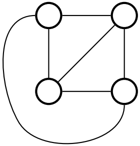
K_n, $|V| = n$

every edge present.
degree of vertex? $|V| - 1$.

Very connected.
Lots of edges:

Graph Types: Complete Graph.



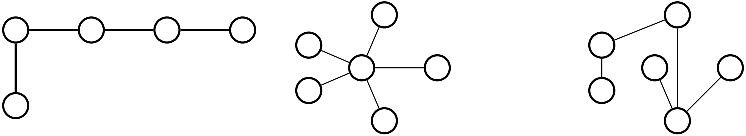


K_n, $|V| = n$

every edge present.
degree of vertex? $|V| - 1$.

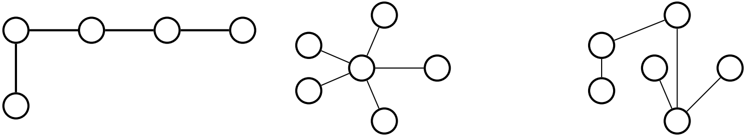
Very connected.
Lots of edges: $n(n-1)/2$.

Trees.



Definitions:

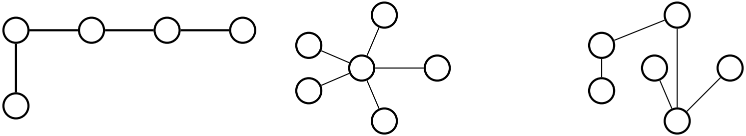
Trees.



Definitions:

A connected graph without a cycle.

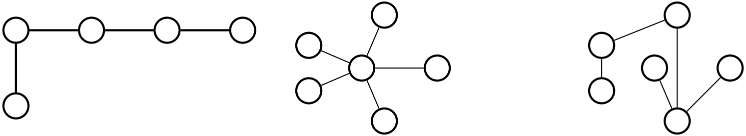
Trees.



Definitions:

A connected graph without a cycle.
A connected graph with $|V| - 1$ edges.

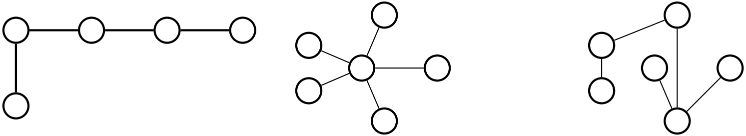
Trees.



Definitions:

A connected graph without a cycle.
A connected graph with $|V| - 1$ edges.
A connected graph where any edge removal disconnects it.

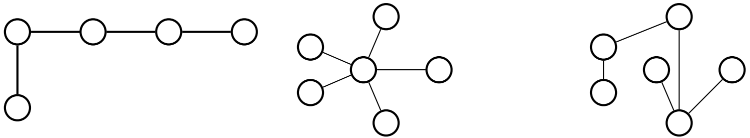
Trees.



Definitions:

A connected graph without a cycle.
A connected graph with $|V|-1$ edges.
A connected graph where any edge removal disconnects it.
An acyclic graph where any edge addition creates a cycle.

Trees.

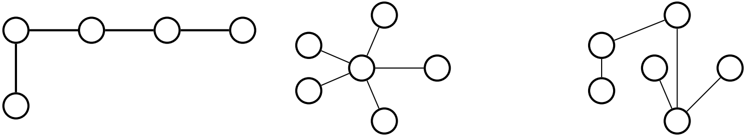


Definitions:

A connected graph without a cycle.
A connected graph with $|V| - 1$ edges.
A connected graph where any edge removal disconnects it.
An acyclic graph where any edge addition creates a cycle.

Minimally connected, minimum number of edges to connect.

Trees.



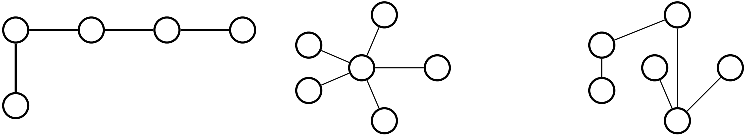
Definitions:

A connected graph without a cycle.
A connected graph with $|V| - 1$ edges.
A connected graph where any edge removal disconnects it.
An acyclic graph where any edge addition creates a cycle.

Minimally connected, minimum number of edges to connect.

Property:

Trees.



Definitions:

A connected graph without a cycle.
A connected graph with $|V|-1$ edges.
A connected graph where any edge removal disconnects it.
An acyclic graph where any edge addition creates a cycle.
Minimally connected, minimum number of edges to connect.

Property:
Can remove a single node and break into components of size at most $|V|/2$.

Hypercube

Hypercubes.

Hypercube

Hypercubes. Really connected.

Hypercube

Hypercubes. Really connected. $|V| \log |V|$ edges!

Hypercube

Hypercubes. Really connected. $|V| \log |V|$ edges!
Also represents bit-strings nicely.

Hypercube

Hypercubes. Really connected. $|V| \log |V|$ edges!
Also represents bit-strings nicely.

Hypercube

Hypercubes. Really connected. $|V| \log |V|$ edges!
Also represents bit-strings nicely.

$G = (V, E)$

Hypercube

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

$G=(V,E)$
$|V|=\{0,1\}^n$,

Hypercube

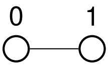
Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

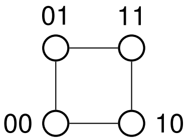
$G = (V, E)$
$|V| = \{0,1\}^n$,
$|E| = \{(x,y) | x$ and y differ in one bit position.$\}$

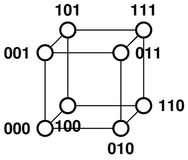
Hypercube

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

$G = (V, E)$
$|V| = \{0, 1\}^n$,
$|E| = \{(x, y) | x$ and y differ in one bit position.$\}$







...Modular Arithmetic...

Arithmetic modulo *m*.

Elements of equivalence classes of integers.

...Modular Arithmetic...

Arithmetic modulo m.

Elements of equivalence classes of integers.

$\{0, \ldots, m-1\}$

...Modular Arithmetic...

Arithmetic modulo m.

Elements of equivalence classes of integers.

$\{0, \ldots, m-1\}$

and integer $i \equiv a \pmod{m}$

...Modular Arithmetic...

Arithmetic modulo m.
- Elements of equivalence classes of integers.
  - $\{0,\ldots,m-1\}$
  - and integer $i \equiv a \pmod{m}$
    - if $i = a + km$ for integer k.

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0,\ldots,m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0, \ldots, m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

...Modular Arithmetic...

Arithmetic modulo m.
  Elements of equivalence classes of integers.
    $\{0,\ldots,m-1\}$
    and integer $i \equiv a \pmod{m}$
      if $i = a + km$ for integer k.
       or if the remainder of i divided by m is a.

Can do calculations by taking remainders
  at the beginning,

...Modular Arithmetic...

Arithmetic modulo m.
 Elements of equivalence classes of integers.
  $\{0,\ldots,m-1\}$
  and integer $i \equiv a \pmod{m}$
   if $i = a + km$ for integer k.
    or if the remainder of i divided by m is a.

Can do calculations by taking remainders
 at the beginning,
  in the middle

...Modular Arithmetic...

Arithmetic modulo m.
  Elements of equivalence classes of integers.
    $\{0,\ldots,m-1\}$
    and integer $i \equiv a \pmod{m}$
      if $i = a + km$ for integer k.
        or if the remainder of i divided by m is a.

Can do calculations by taking remainders
  at the beginning,
    in the middle
      or at the end.

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0,\ldots,m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58 + 32 = 90 = 6 \pmod{7}$

...Modular Arithmetic...

Arithmetic modulo m.

Elements of equivalence classes of integers.

$\{0,\ldots,m-1\}$

and integer $i \equiv a \pmod{m}$

if $i = a + km$ for integer k.

or if the remainder of i divided by m is a.

Can do calculations by taking remainders

at the beginning,

in the middle

or at the end.

$58+32 = 90 = 6 \pmod{7}$

$58+32 = 2+4 = 6 \pmod{7}$

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0, \ldots, m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58 + 32 = 90 = 6 \pmod{7}$
$58 + 32 = 2 + 4 = 6 \pmod{7}$
$58 + 32 = 2 + -3 = -1 = 6 \pmod{7}$

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0, \ldots, m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58 + 32 = 90 = 6 \pmod{7}$
$58 + 32 = 2 + 4 = 6 \pmod{7}$
$58 + 32 = 2 + -3 = -1 = 6 \pmod{7}$

...Modular Arithmetic...

Arithmetic modulo m.

Elements of equivalence classes of integers.

$\{0, \ldots, m-1\}$

and integer $i \equiv a \pmod{m}$

if $i = a + km$ for integer k.

or if the remainder of i divided by m is a.

Can do calculations by taking remainders

at the beginning,

in the middle

or at the end.

$58 + 32 = 90 = 6 \pmod{7}$

$58 + 32 = 2 + 4 = 6 \pmod{7}$

$58 + 32 = 2 + -3 = -1 = 6 \pmod{7}$

Negative numbers work the way you are used to.

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0,\ldots,m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58+32=90=6 \pmod{7}$
$58+32=2+4=6 \pmod{7}$
$58+32=2+-3=-1=6 \pmod{7}$

Negative numbers work the way you are used to.
$-3=0-3=7-3=4 \pmod{7}$

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0, \ldots, m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58 + 32 = 90 = 6 \pmod{7}$
$58 + 32 = 2 + 4 = 6 \pmod{7}$
$58 + 32 = 2 + -3 = -1 = 6 \pmod{7}$

Negative numbers work the way you are used to.
$-3 = 0 - 3 = 7 - 3 = 4 \pmod{7}$

...Modular Arithmetic...

Arithmetic modulo m.
  Elements of equivalence classes of integers.
    $\{0, \ldots, m-1\}$
    and integer $i \equiv a \pmod{m}$
      if $i = a + km$ for integer k.
        or if the remainder of i divided by m is a.

Can do calculations by taking remainders
  at the beginning,
    in the middle
        or at the end.

$58 + 32 = 90 = 6 \pmod{7}$
$58 + 32 = 2 + 4 = 6 \pmod{7}$
$58 + 32 = 2 + -3 = -1 = 6 \pmod{7}$

Negative numbers work the way you are used to.
  $-3 = 0 - 3 = 7 - 3 = 4 \pmod{7}$

Additive inverses are intuitively negative numbers.

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$?

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod{7}$? 5

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod{7}$? 5
$5^{-1} \pmod{7}$?

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique?

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod{7}$? 5
$5^{-1} \pmod{7}$? 3

Inverse Unique? Yes.

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$
$ax = bx = 1 \pmod n$

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$
$ax = bx = 1 \pmod n$
$axb = bxb = b \pmod n$

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.

Proof: a and b inverses of $x \pmod n$

$ax = bx = 1 \pmod n$
$axb = bxb = b \pmod n$
$a = b \pmod n$.

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$
$ax = bx = 1 \pmod n$
$axb = bxb = b \pmod n$
$a = b \pmod n$.

$3^{-1} \pmod 6$?

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod{7}$? 5
$5^{-1} \pmod{7}$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod{n}$
$ax = bx = 1 \pmod{n}$
$axb = bxb = b \pmod{n}$
$a = b \pmod{n}$.

$3^{-1} \pmod{6}$? No, no, no....

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.

Proof: a and b inverses of $x \pmod n$

$ax = bx = 1 \pmod n$

$axb = bxb = b \pmod n$

$a = b \pmod n$.

$3^{-1} \pmod 6$? No, no, no....

$\{3(1), 3(2), 3(3), 3(4), 3(5)\}$

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod{7}$? 5
$5^{-1} \pmod{7}$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod{n}$

$ax = bx = 1 \pmod{n}$
$axb = bxb = b \pmod{n}$
$a = b \pmod{n}$.

$3^{-1} \pmod{6}$? No, no, no....

$\{3(1), 3(2), 3(3), 3(4), 3(5)\}$
$\{3, 6, 3, 6, 3\}$

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$
$ax = bx = 1 \pmod n$
$axb = bxb = b \pmod n$
$a = b \pmod n$.

$3^{-1} \pmod 6$? No, no, no....

$\{3(1), 3(2), 3(3), 3(4), 3(5)\}$
$\{3, 6, 3, 6, 3\}$

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$
$ax = bx = 1 \pmod n$
$axb = bxb = b \pmod n$
$a = b \pmod n$.

$3^{-1} \pmod 6$? No, no, no....

$\{3(1), 3(2), 3(3), 3(4), 3(5)\}$
$\{3, 6, 3, 6, 3\}$

See,

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.

Proof: a and b inverses of $x \pmod n$

$ax = bx = 1 \pmod n$
$axb = bxb = b \pmod n$
$a = b \pmod n$.

$3^{-1} \pmod 6$? No, no, no....

$\{3(1), 3(2), 3(3), 3(4), 3(5)\}$
$\{3, 6, 3, 6, 3\}$

See,... no inverse!

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x, m) = 1$.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y)$

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm!

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y,x-y) = gcd(y,x \pmod y)$.

Give recursive Algorithm! Base Case?

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x, y)

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y,x-y) = gcd(y,x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y,x-y) = gcd(y,x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax+by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse!

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm$

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y,x-y) = gcd(y,x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax+by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax+bm = ax \pmod m$.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm = ax \pmod{m}$.

Idea: egcd.

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y,x-y) = gcd(y,x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm = ax \pmod m$.

Idea: egcd.
gcd produces 1

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm = ax \pmod m$.

Idea: egcd.
gcd produces 1
by adding and subtracting multiples of x and y

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm = ax \pmod{m}$.

Idea: egcd.
gcd produces 1
by adding and subtracting multiples of x and y

Example: $p = 7$, $q = 11$.

Example: $p = 7$, $q = 11$.

$N = 77$.

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$

Example: $p = 7$, $q = 11$.

$N = 77.$
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$7(0) + 60(1) \quad = \quad 60$$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0)+60(1) &= 60 \\ 7(1)+60(0) &= 7 \end{aligned}$$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0) + 60(1) &= 60 \\ 7(1) + 60(0) &= 7 \\ 7(-8) + 60(1) &= 4 \end{aligned}$$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned}
7(0) + 60(1) &= 60 \\
7(1) + 60(0) &= 7 \\
7(-8) + 60(1) &= 4 \\
7(9) + 60(-1) &= 3
\end{aligned}$$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0) + 60(1) &= 60 \\ 7(1) + 60(0) &= 7 \\ 7(-8) + 60(1) &= 4 \\ 7(9) + 60(-1) &= 3 \\ 7(-17) + 60(2) &= 1 \end{aligned}$$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned}
7(0) + 60(1) &= 60 \\
7(1) + 60(0) &= 7 \\
7(-8) + 60(1) &= 4 \\
7(9) + 60(-1) &= 3 \\
7(-17) + 60(2) &= 1
\end{aligned}$$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0) + 60(1) &= 60 \\ 7(1) + 60(0) &= 7 \\ 7(-8) + 60(1) &= 4 \\ 7(9) + 60(-1) &= 3 \\ 7(-17) + 60(2) &= 1 \end{aligned}$$

Confirm:

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0) + 60(1) &= 60 \\ 7(1) + 60(0) &= 7 \\ 7(-8) + 60(1) &= 4 \\ 7(9) + 60(-1) &= 3 \\ 7(-17) + 60(2) &= 1 \end{aligned}$$

Confirm: $-119 + 120 = 1$

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned}
7(0) + 60(1) &= 60 \\
7(1) + 60(0) &= 7 \\
7(-8) + 60(1) &= 4 \\
7(9) + 60(-1) &= 3 \\
7(-17) + 60(2) &= 1
\end{aligned}$$

Confirm: $-119 + 120 = 1$

$d = e^{-1} = -17 = 43 = \pmod{60}$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function:

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.

Invertible function: one-to-one.

$T \subseteq S$ since $0 \notin T$.

p is prime.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \not\in T$.
p is prime.
$\implies T = S$.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \not\in T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \not\in T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \not\in T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Each of $2, \ldots (p-1)$ has an inverse modulo p,

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Each of $2, \ldots (p-1)$ has an inverse modulo p,
mulitply by inverses to get...

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.

Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Each of $2, \ldots (p-1)$ has an inverse modulo p,
mulitply by inverses to get...

$$a^{(p-1)} \equiv 1 \mod p.$$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.

Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Each of $2, \ldots (p-1)$ has an inverse modulo p,
mulitply by inverses to get...

$$a^{(p-1)} \equiv 1 \mod p.$$

□

RSA

RSA:

RSA

RSA:

$N = p, q$

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.

RSA

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1)) = 1$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

RSA

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1)) = 1$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and $q \implies$ theorem!

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and q $\implies$ theorem!

$x^{ed} - x$

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and q $\implies$ theorem!

$x^{ed} - x = x^{k(p-1)(q-1)+1} - x$

RSA

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1)) = 1$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:

$x^{ed} - x$ is divisible by p and q $\implies$ theorem!

$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and $q \implies$ theorem!

$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$

If x is divisible by p, the product is.

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and q $\implies$ theorem!

$$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$$

If x is divisible by p, the product is.
Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and $q \implies$ theorem!

$$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$$

If x is divisible by p, the product is.
Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.
$\implies (x^{k(q-1)})^{p-1} - 1$ divisible by p.

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and $q \implies$ theorem!

$$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$$

If x is divisible by p, the product is.
Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.
$\implies (x^{k(q-1)})^{p-1} - 1$ divisible by p.

Similarly for q.

RSA

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1)) = 1$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:

$x^{ed} - x$ is divisible by p and $q \implies$ theorem!

$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$

If x is divisible by p, the product is.

Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.

$\implies (x^{k(q-1)})^{p-1} - 1$ divisible by p.

Similarly for q. □

RSA, Public Key, and Signatures.

RSA, Public Key, and Signatures.

RSA:

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

RSA, Public Key, and Signatures.

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

RSA, Public Key, and Signatures.

RSA:

$N = p,q$

e with $\gcd(e,(p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

RSA, Public Key, and Signatures.

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1))$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.

RSA, Public Key, and Signatures.

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

RSA, Public Key, and Signatures.

RSA:
$N = p,q$
e with $\gcd(e,(p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

RSA, Public Key, and Signatures.

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K), k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

$E(D(C,k),K) = (C^d)^e = C \pmod{N}$

Fermat/RSA

$3^6 \pmod{7}$?

Fermat/RSA

$3^6 \pmod 7$? 1.

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$?

Fermat/RSA

$3^6 \pmod 7$? 1.   Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$?

Fermat/RSA

$3^6 \pmod 7$? 1.   Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$?

Fermat/RSA

$3^6 \pmod 7$? 1.   Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
  $21 = (3)(7)$

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p - 1)(q - 1) = (2)(6) = 12$

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p-1)(q-1) = (2)(6) = 12$
$gcd(2, 12) = 1$, $x^{(p-1)(q-1)} = 1 \pmod{pq}$

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p-1)(q-1) = (2)(6) = 12$
$gcd(2, 12) = 1$, $x^{(p-1)(q-1)} = 1 \pmod{pq}$ $2^{12} = 1 \pmod{21}$.

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p-1)(q-1) = (2)(6) = 12$
$gcd(2,12) = 1$, $x^{(p-1)(q-1)} = 1 \pmod{pq}$ $2^{12} = 1 \pmod{21}$.

$2^14 \pmod{21}$?

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p-1)(q-1) = (2)(6) = 12$
$gcd(2,12) = 1$, $x^{(p-1)(q-1)} = 1 \pmod{pq}$ $2^{12} = 1 \pmod{21}$.

$2^14 \pmod{21}$? 4.

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p - 1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p-1)(q-1) = (2)(6) = 12$
$gcd(2,12) = 1$, $x^{(p-1)(q-1)} = 1 \pmod{pq}$ $2^{12} = 1 \pmod{21}$.

$2^14 \pmod{21}$? 4. Technically $4 \pmod{21}$.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S **and** T**,** $|S \cup T| = |S| + |T|$

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)!$

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit. $|S| = 10^9$

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S **and** T**,** $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S **and** T**,**
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.$|S| = 10^9$

T = phone numbers with 7 as second digit.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.$|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S **and** T**,** $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S **and** T**,**
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.$|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

$S \cap T$ = phone numbers with 7 as first and second digit.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.$|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

$S \cap T$ = phone numbers with 7 as first and second digit. $|S \cap T| = 10^8$.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit. $|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

$S \cap T$ = phone numbers with 7 as first and second digit. $|S \cap T| = 10^8$.

Answer: $|S| + |T| - |S \cap T| = 10^9 + 10^9 - 10^8$.

Counting.

First Rule: Enumerate objects with sequence of choices.

Counting.

First Rule: Enumerate objects with sequence of choices.
  Number of Objects: $n_1 \times n_2 \ldots$.

Counting.

First Rule: Enumerate objects with sequence of choices.

Number of Objects: $n_1 \times n_2 \ldots$.

Example: Poker deals.

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
Example: Poker hands. Orderings of ANAGRAM.

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.

Counting.

First Rule: Enumerate objects with sequence of choices.
 Number of Objects: $n_1 \times n_2 \ldots$.
 Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
 Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.
 Example: Hands with joker, hands without.

Counting.

First Rule: Enumerate objects with sequence of choices.
  Number of Objects: $n_1 \times n_2 \ldots$.
  Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
  Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.
  Example: Hands with joker, hands without.

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.
Example: Hands with joker, hands without.

Inclusion/Exclusion: For arbtrary sets A, B.

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.
Example: Hands with joker, hands without.

Inclusion/Exclusion: For arbtrary sets A, B.
$|A \cup B| = |A| + |B| - |A \cap B|$

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.
Example: Hands with joker, hands without.

Inclusion/Exclusion: For arbtrary sets A, B.
$|A \cup B| = |A| + |B| - |A \cap B|$
Example: 10 digit numbers with 9 in the first or second digit.

Counting.

First Rule: Enumerate objects with sequence of choices.
Number of Objects: $n_1 \times n_2 \ldots$.
Example: Poker deals.

Second Rule: Divide out if by ordering of same objects.
Example: Poker hands. Orderings of ANAGRAM.

Sum Rule: If sets of objects disjoint add sizes.
Example: Hands with joker, hands without.

Inclusion/Exclusion: For arbtrary sets A, B.
$|A \cup B| = |A| + |B| - |A \cap B|$
Example: 10 digit numbers with 9 in the first or second digit.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$?

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element,

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.
Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.
Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.
Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

So, $\binom{n}{k-1} + \binom{n}{k}$

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

So, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

So, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. □

Uncountability/Undecidability.

Integers are countable.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why?

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Halt is undecidable.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Halt is undecidable.

Why?

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Halt is undecidable.

Why? Diagonalization.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Halt is undecidable.

Why? Diagonalization.

Reductions **from** Halt give more undecidable problems.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Halt is undecidable.

Why? Diagonalization.

Reductions **from** Halt give more undecidable problems.

Reductions use program for problem A to solve HALT.

Uncountability/Undecidability.

Integers are countable.

Reals are not.

Why? Diagonalization.

Halt is undecidable.

Why? Diagonalization.

Reductions **from** Halt give more undecidable problems.

Reductions use program for problem A to solve HALT.

Concept 1: can call program A
Concept 2:One can modify text of input program (to HALT).

CS70: Review of Probability.

Probability Review

CS70: Review of Probability.

Probability Review

CS70: Review of Probability.

Probability Review

1. True or False

CS70: Review of Probability.

Probability Review

1. True or False
2. Some Key Results

CS70: Review of Probability.

Probability Review

1. True or False
2. Some Key Results
3. Quiz 1: G

CS70: Review of Probability.

Probability Review

1. True or False
2. Some Key Results
3. Quiz 1: G
4. Quiz 2: PG

CS70: Review of Probability.

Probability Review

1. True or False
2. Some Key Results
3. Quiz 1: G
4. Quiz 2: PG
5. Quiz 3: R

CS70: Review of Probability.

Probability Review

1. True or False
2. Some Key Results
3. Quiz 1: G
4. Quiz 2: PG
5. Quiz 3: R
6. Common Mistakes

CS70: Review of Probability.

Probability Review

1. True or False
2. Some Key Results
3. Quiz 1: G
4. Quiz 2: PG
5. Quiz 3: R
6. Common Mistakes

True or False

- Ω and A are independent.

True or False

- Ω and A are independent. True

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$.

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$.

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$.

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$.

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\Longrightarrow$ $var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$. True

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies \frac{X_1 + \cdots + X_n - nE[X_1]}{n\sigma(X_1)} \to \mathcal{N}(0,1)$.

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies \frac{X_1 + \cdots + X_n - nE[X_1]}{n\sigma(X_1)} \to \mathcal{N}(0, 1)$. False: $\sqrt{n}$

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies \frac{X_1 + \cdots + X_n - nE[X_1]}{n\sigma(X_1)} \to \mathcal{N}(0,1)$. False: $\sqrt{n}$
- $X = Expo(\lambda) \implies Pr[X > 5 | X > 3] = Pr[X > 2]$.

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies \frac{X_1 + \cdots + X_n - nE[X_1]}{n\sigma(X_1)} \to \mathcal{N}(0, 1)$. False: $\sqrt{n}$
- $X = Expo(\lambda) \implies Pr[X > 5 | X > 3] = Pr[X > 2]$. True:

True or False

- Ω and A are independent. True
- $Pr[A \cap B] = Pr[A] + Pr[B] - Pr[A \cup B]$. True
- $Pr[A \setminus B] \geq Pr[A] - Pr[B]$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies var(\frac{X_1 + \cdots + X_n}{n}) = var(X_1)$. False: $\times \frac{1}{n}$
- $Pr[|X - a| \geq b] \leq \frac{E[(X-a)^2]}{b^2}$. True
- $X_1, \ldots, X_n$ i.i.d. $\implies \frac{X_1 + \cdots + X_n - nE[X_1]}{n\sigma(X_1)} \to \mathcal{N}(0,1)$. False: $\sqrt{n}$
- $X = Expo(\lambda) \implies Pr[X > 5 | X > 3] = Pr[X > 2]$. True:

  $$\frac{\exp\{-\lambda 5\}}{\exp\{-\lambda 3\}} = \exp\{-\lambda 2\}.$$

Correct or not?

Correct or not?

When $n \gg 1$, one has

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ.

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ.

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes
- If $0.3 < \sigma < 3$, then

  $$[A_n - 0.6\frac{1}{\sqrt{n}}, A_n + 0.6\frac{1}{\sqrt{n}}] = 95\%\text{-CI for } \mu.$$

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes
- If $0.3 < \sigma < 3$, then

  $[A_n - 0.6\frac{1}{\sqrt{n}}, A_n + 0.6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. No

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes
- If $0.3 < \sigma < 3$, then

  $[A_n - 0.6\frac{1}{\sqrt{n}}, A_n + 0.6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. No
- If $0.3 < \sigma < 3$, then

  $[A_n - 6\frac{1}{\sqrt{n}}, A_n + 6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ.

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes
- If $0.3 < \sigma < 3$, then

  $[A_n - 0.6\frac{1}{\sqrt{n}}, A_n + 0.6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. No
- If $0.3 < \sigma < 3$, then

  $[A_n - 6\frac{1}{\sqrt{n}}, A_n + 6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes

Correct or not?

When $n \gg 1$, one has

- $[A_n - 2\sigma\frac{1}{n}, A_n + 2\sigma\frac{1}{n}] = 95\%$-CI for μ. No
- $[A_n - 2\sigma\frac{1}{\sqrt{n}}, A_n + 2\sigma\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes
- If $0.3 < \sigma < 3$, then

  $[A_n - 0.6\frac{1}{\sqrt{n}}, A_n + 0.6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. No
- If $0.3 < \sigma < 3$, then

  $[A_n - 6\frac{1}{\sqrt{n}}, A_n + 6\frac{1}{\sqrt{n}}] = 95\%$-CI for μ. Yes

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$;

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \varepsilon] \rightarrow 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$;

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \rightarrow 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \rightarrow 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$;

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \varepsilon] \to 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X, Y)}{var(X)}(X - E[X]).$

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \varepsilon] \to 0,$

[8] $E[(Y - E[Y|X])h(X)] = 0.$

- WLLN (7)
- MMSE (6)

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$;

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X, Y)}{var(X)}(X - E[X])$.

[6] $\sum_y yPr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \varepsilon] \rightarrow 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \to 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property (8)

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X, Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \to 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property (8)
- Chebyshev

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \varepsilon] \to 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property (8)
- Chebyshev (2)

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \to 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property (8)
- Chebyshev (2)
- LLSE

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y yPr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \rightarrow 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property (8)
- Chebyshev (2)
- LLSE (5)

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$;

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \rightarrow 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

- WLLN (7)
- MMSE (6)
- Projection property (8)
- Chebyshev (2)
- LLSE (5)
- Markov's inequality

Match Items

[1] $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$

[2] $Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}$

[3] $Pr[X \geq a] \leq \min_{\theta > 0} \frac{E[e^{\theta X}]}{e^{\theta a}}$

[4] $g(\cdot)$ convex $\Rightarrow E[g(X)] \geq g(E[X])$

[5] $E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X])$.

[6] $\sum_y y Pr[Y = y | X = x]$

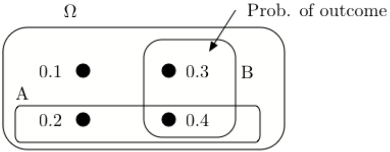
[7] $Pr[|\frac{X_1 + \cdots + X_n}{n} - E[X_1]| \geq \epsilon] \to 0$,

[8] $E[(Y - E[Y|X])h(X)] = 0$.

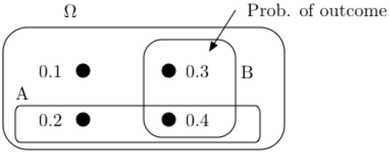
- WLLN (7)
- MMSE (6)
- Projection property (8)
- Chebyshev (2)
- LLSE (5)
- Markov's inequality (1)

Quiz 1: G

Quiz 1: G

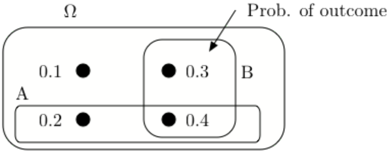


Quiz 1: G



1. What is $P[A|B]$?

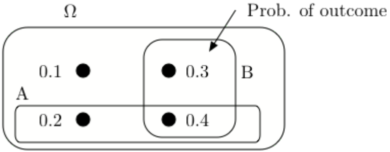
Quiz 1: G



1. What is $P[A|B]$?

   $Pr[A|B] =$

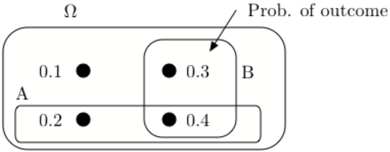
Quiz 1: G



1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} =$

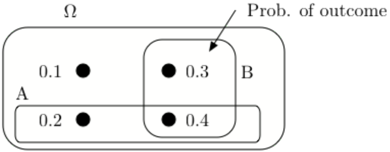
Quiz 1: G



1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

Quiz 1: G

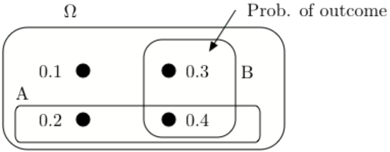


1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

2. What is $Pr[B|A]$?

Quiz 1: G



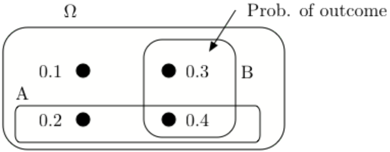
1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

2. What is $Pr[B|A]$?

   $Pr[B|A] =$

Quiz 1: G



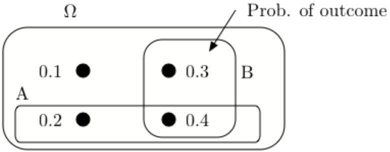
1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

2. What is $Pr[B|A]$?

   $Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]} =$

Quiz 1: G



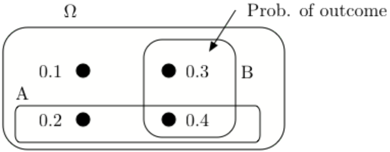
1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

2. What is $Pr[B|A]$?

   $Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]} = \frac{0.4}{0.6}$

Quiz 1: G



1. What is $P[A|B]$?

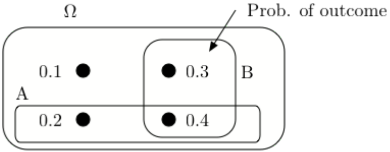
   $$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$$

2. What is $Pr[B|A]$?

   $$Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]} = \frac{0.4}{0.6}$$

3. Are A and B positively correlated?

Quiz 1: G



1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

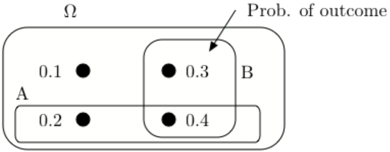
2. What is $Pr[B|A]$?

   $Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]} = \frac{0.4}{0.6}$

3. Are A and B positively correlated?

   No.

Quiz 1: G



1. What is $P[A|B]$?

   $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{0.4}{0.7}$

2. What is $Pr[B|A]$?

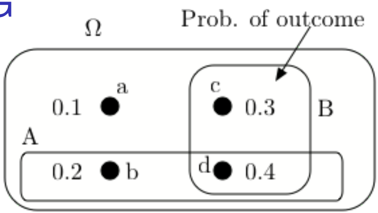
   $Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]} = \frac{0.4}{0.6}$

3. Are A and B positively correlated?

   No. $Pr[A \cap B] = 0.4 < Pr[A]Pr[B] = 0.6 \times 0.7$.

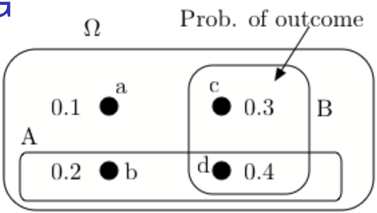
Quiz 1: G

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

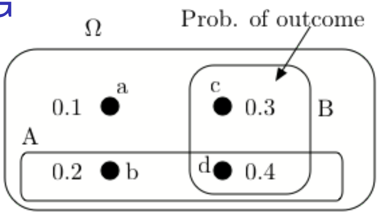
Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

Quiz 1: G

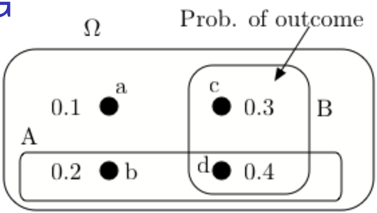


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$E[Y|X=0] \quad =$$

Quiz 1: G

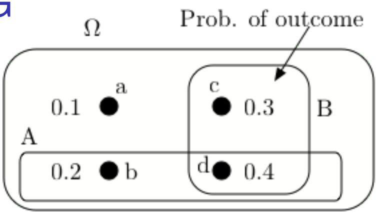


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$E[Y|X=0] = 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0]$$

Quiz 1: G



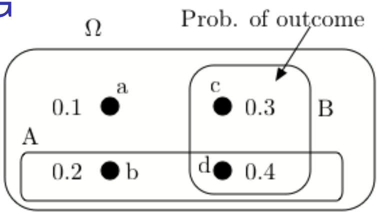
ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$E[Y|X=0] = 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0]$$

$$=$$

Quiz 1: G

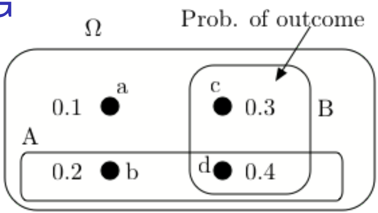


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$\begin{aligned} E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\ &= 2 \times \frac{0.3}{0.4} = \end{aligned}$$

Quiz 1: G

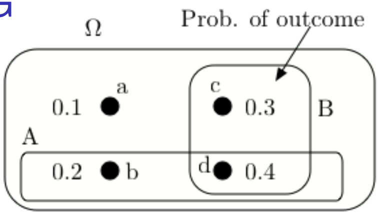


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5
\end{aligned}
$$

Quiz 1: G

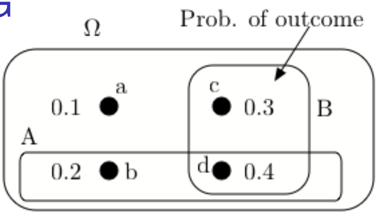


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$E[Y|X=0] = 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0]$$
$$= 2 \times \frac{0.3}{0.4} = 1.5$$
$$E[Y|X=1] =$$

Quiz 1: G

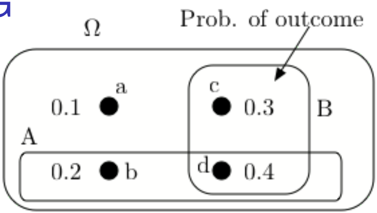


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1]
\end{aligned}
$$

Quiz 1: G

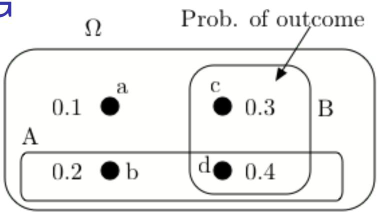


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&=
\end{aligned}
$$

Quiz 1: G

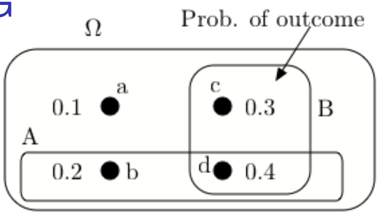


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&= 2 \times \frac{0.4}{0.6} =
\end{aligned}
$$

Quiz 1: G

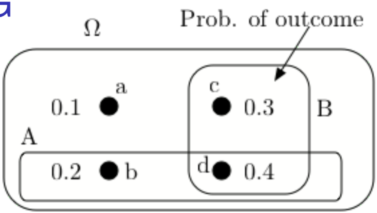


ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&= 2 \times \frac{0.4}{0.6} = 1.33
\end{aligned}$$

Quiz 1: G



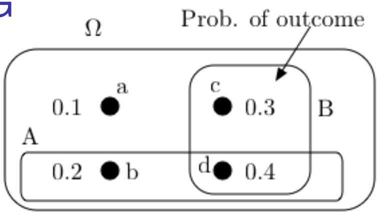
ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&= 2 \times \frac{0.4}{0.6} = 1.33
\end{aligned}
$$

5. What is $cov(X, Y)$?

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

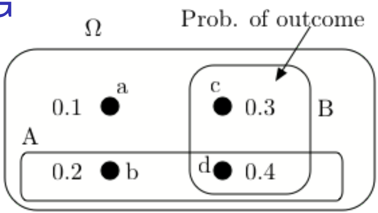
4. What is $E[Y|X]$?

$$\begin{aligned} E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\ &= 2 \times \frac{0.3}{0.4} = 1.5 \\ E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\ &= 2 \times \frac{0.4}{0.6} = 1.33 \end{aligned}$$

5. What is $cov(X, Y)$?

   $cov(X, Y) =$

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

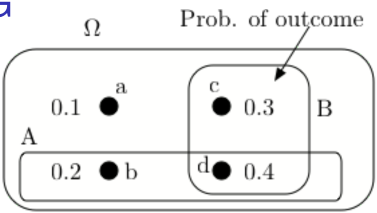
4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&= 2 \times \frac{0.4}{0.6} = 1.33
\end{aligned}
$$

5. What is $cov(X, Y)$?

$cov(X,Y) = E[XY] - E[X]E[Y] =$

Quiz 1: G



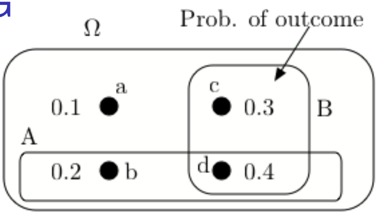
ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$\begin{aligned} E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\ &= 2 \times \frac{0.3}{0.4} = 1.5 \\ E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\ &= 2 \times \frac{0.4}{0.6} = 1.33 \end{aligned}$$

5. What is $cov(X, Y)$?
$cov(X, Y) = E[XY] - E[X]E[Y] = 0.8 - 0.6 \times 1.4 =$

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

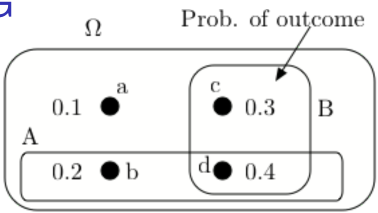
4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&= 2 \times \frac{0.4}{0.6} = 1.33
\end{aligned}
$$

5. What is $cov(X, Y)$?

$cov(X,Y) = E[XY] - E[X]E[Y] = 0.8 - 0.6 \times 1.4 = -0.04$

Quiz 1: G



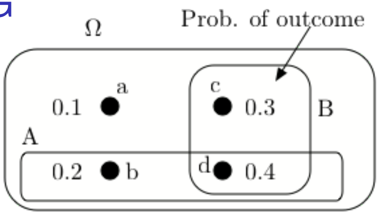
ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$\begin{aligned} E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\ &= 2 \times \frac{0.3}{0.4} = 1.5 \\ E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\ &= 2 \times \frac{0.4}{0.6} = 1.33 \end{aligned}$$

5. What is $cov(X, Y)$?
   $cov(X,Y) = E[XY] - E[X]E[Y] = 0.8 - 0.6 \times 1.4 = -0.04$
6. What is $L[Y|X]$?

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$\begin{aligned} E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\ &= 2 \times \frac{0.3}{0.4} = 1.5 \\ E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\ &= 2 \times \frac{0.4}{0.6} = 1.33 \end{aligned}$$

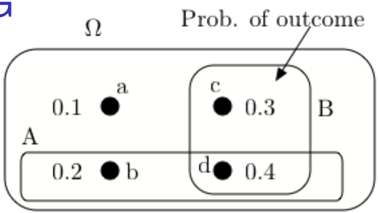
5. What is $cov(X, Y)$?

   $cov(X,Y) = E[XY] - E[X]E[Y] = 0.8 - 0.6 \times 1.4 = -0.04$

6. What is $L[Y|X]$?

   $L[Y|X] =$

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$
\begin{aligned}
E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\
&= 2 \times \frac{0.3}{0.4} = 1.5 \\
E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\
&= 2 \times \frac{0.4}{0.6} = 1.33
\end{aligned}
$$

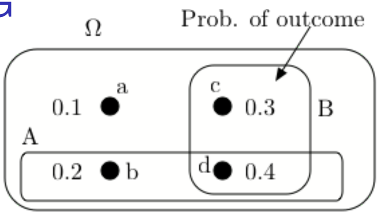
5. What is $cov(X, Y)$?

   $cov(X, Y) = E[XY] - E[X]E[Y] = 0.8 - 0.6 \times 1.4 = -0.04$

6. What is $L[Y|X]$?

   $L[Y|X] = E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X]) =$

Quiz 1: G



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

4. What is $E[Y|X]$?

$$\begin{aligned} E[Y|X=0] &= 0 \times Pr[Y=0|X=0] + 2 \times Pr[Y=2|X=0] \\ &= 2 \times \frac{0.3}{0.4} = 1.5 \\ E[Y|X=1] &= 0 \times Pr[Y=0|X=1] + 2 \times Pr[Y=2|X=1] \\ &= 2 \times \frac{0.4}{0.6} = 1.33 \end{aligned}$$

5. What is $cov(X, Y)$?

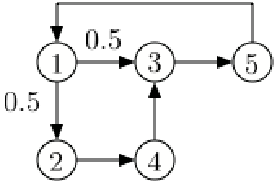
   $cov(X,Y) = E[XY] - E[X]E[Y] = 0.8 - 0.6 \times 1.4 = -0.04$

6. What is $L[Y|X]$?

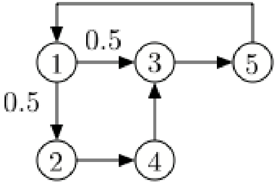
   $L[Y|X] = E[Y] + \frac{cov(X,Y)}{var(X)}(X - E[X]) = 1.4 + \frac{-0.04}{0.6 \times 0.4}(X - 0.6)$

Quiz 1: G

Quiz 1: G

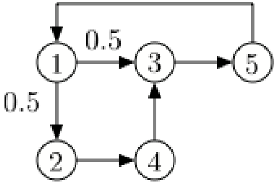


Quiz 1: G



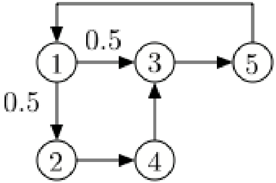
7. Is this Markov chains irreducible?

Quiz 1: G



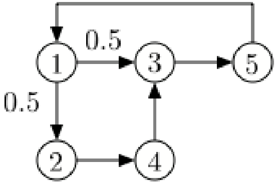
7. Is this Markov chains irreducible? Yes.

Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

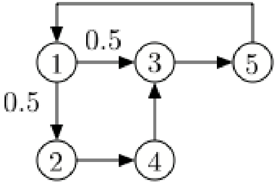
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No.

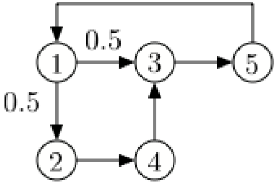
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are

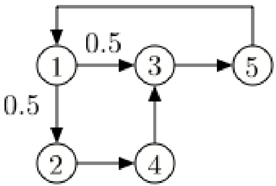
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$:

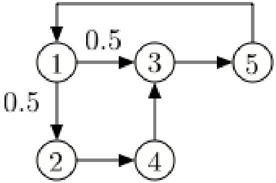
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!

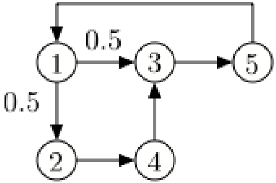
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0?

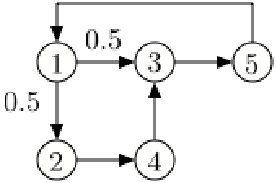
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!

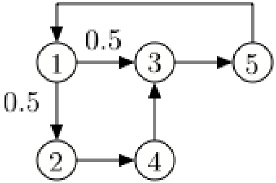
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$?

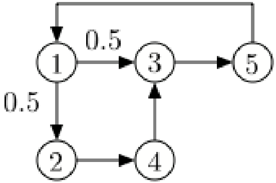
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!

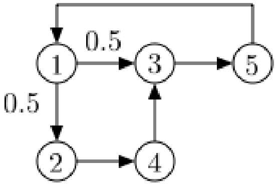
Quiz 1: G



7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

Quiz 1: G

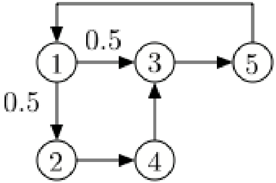


7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

    Let $a = \pi(1)$.

Quiz 1: G

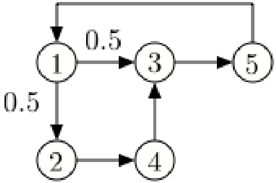


7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

    Let $a = \pi(1)$. Then $a = \pi(5)$,

Quiz 1: G

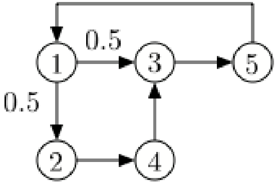


7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

    Let $a = \pi(1)$. Then $a = \pi(5), \pi(2) = 0.5a$,

Quiz 1: G

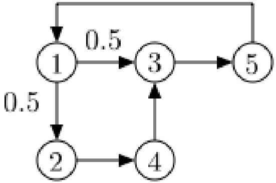


7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

    Let $a = \pi(1)$. Then $a = \pi(5), \pi(2) = 0.5a, \pi(4) = \pi(2) = 0.5a,$

Quiz 1: G

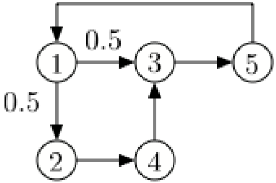


7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

    Let $a = \pi(1)$. Then $a = \pi(5), \pi(2) = 0.5a, \pi(4) = \pi(2) = 0.5a, \pi(3) = 0.5\pi(1) + \pi(4) = a$.

Quiz 1: G

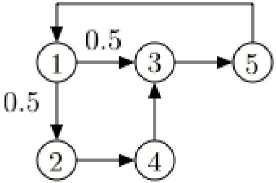


7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

    Let $a = \pi(1)$. Then $a = \pi(5), \pi(2) = 0.5a, \pi(4) = \pi(2) = 0.5a, \pi(3) = 0.5\pi(1) + \pi(4) = a$. Thus, $\pi = [a, 0.5a, a, 0.5a, a] = [1, 0.5, 1, 0.5, 1]a$, so $a =$

Quiz 1: G



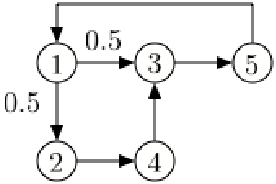
7. Is this Markov chains irreducible? Yes.
8. Is this Markov chain periodic?

   No. The return times to 3 are $\{3, 5, ..\}$: coprime!
9. Does π_n converge to a value independent of π_0? Yes!
10. Does $\frac{1}{n}\sum_{m=1}^{n-1} 1\{X_m = 3\}$ converge as $n \to \infty$? Yes!
11. Calculate π.

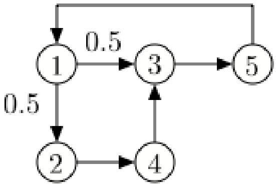
    Let $a = \pi(1)$. Then $a = \pi(5), \pi(2) = 0.5a, \pi(4) = \pi(2) = 0.5a, \pi(3) = 0.5\pi(1) + \pi(4) = a$. Thus,
    $\pi = [a, 0.5a, a, 0.5a, a] = [1, 0.5, 1, 0.5, 1]a$, so $a = 1/4$.

Quiz 1: G

Quiz 1: G

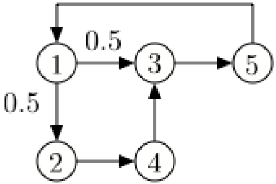


Quiz 1: G



12. Write the first step equations for calculating the mean time from 1 to 4.

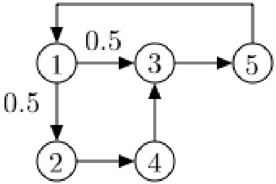
Quiz 1: G



12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$

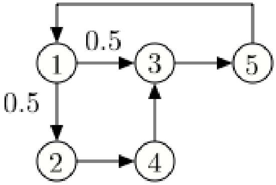
Quiz 1: G



12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$

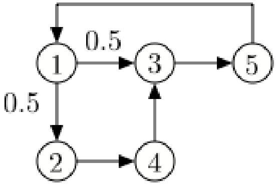
Quiz 1: G



12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$
$$\beta(3) = 1 + \beta(5)$$

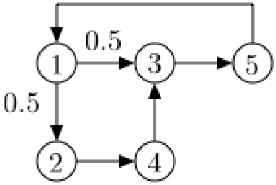
Quiz 1: G



12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$
$$\beta(3) = 1 + \beta(5)$$
$$\beta(5) = 1 + \beta(1).$$

Quiz 1: G

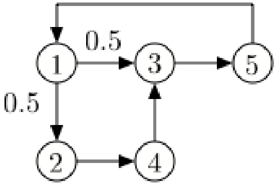


12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$
$$\beta(3) = 1 + \beta(5)$$
$$\beta(5) = 1 + \beta(1).$$

13. Solve these equations.

Quiz 1: G



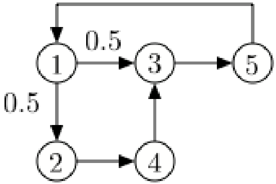
12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$
$$\beta(3) = 1 + \beta(5)$$
$$\beta(5) = 1 + \beta(1).$$

13. Solve these equations.

$$\beta(1) \quad = \quad 1 + 0.5 \times 1 + 0.5 \times (1 + (1 + \beta(1)))$$

Quiz 1: G



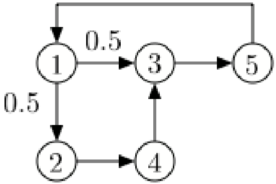
12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$
$$\beta(3) = 1 + \beta(5)$$
$$\beta(5) = 1 + \beta(1).$$

13. Solve these equations.

$$\begin{aligned}\beta(1) &= 1 + 0.5 \times 1 + 0.5 \times (1 + (1 + \beta(1))) \\ &= 2.5 + 0.5\beta(1).\end{aligned}$$

Quiz 1: G



12. Write the first step equations for calculating the mean time from 1 to 4.

$$\beta(1) = 1 + 0.5\beta(2) + 0.5\beta(3)$$
$$\beta(2) = 1$$
$$\beta(3) = 1 + \beta(5)$$
$$\beta(5) = 1 + \beta(1).$$

13. Solve these equations.

$$\begin{aligned} \beta(1) &= 1 + 0.5 \times 1 + 0.5 \times (1 + (1 + \beta(1))) \\ &= 2.5 + 0.5\beta(1). \end{aligned}$$

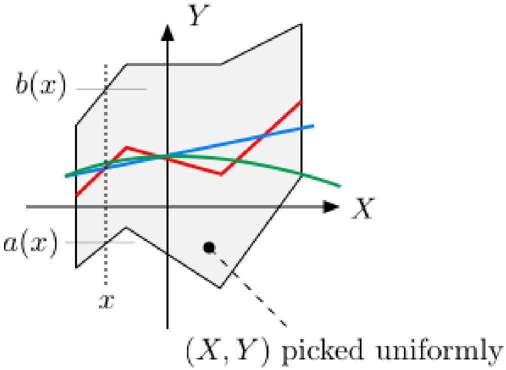
Hence, $\beta(1) = 5$.

Quiz 1: G

14. Which is $E[Y|X]$? Blue, red or green?

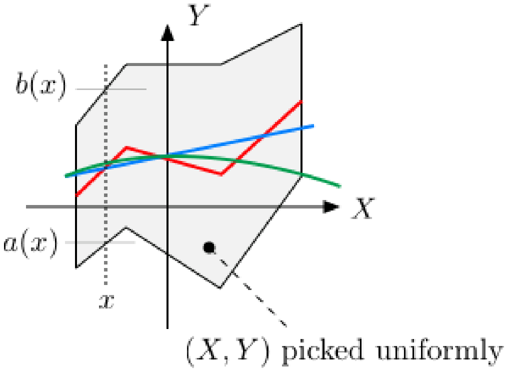
Quiz 1: G

14. Which is $E[Y|X]$? Blue, red or green?



Quiz 1: G

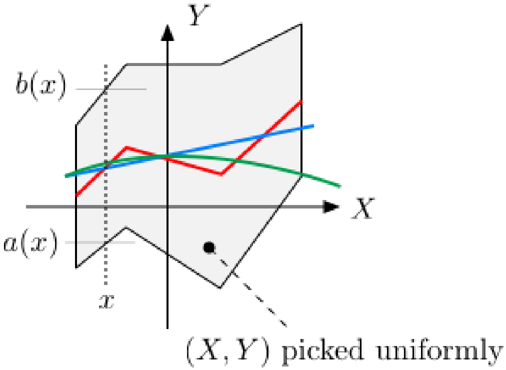
14. Which is $E[Y|X]$? Blue, red or green?



Answer: Red.

Quiz 1: G

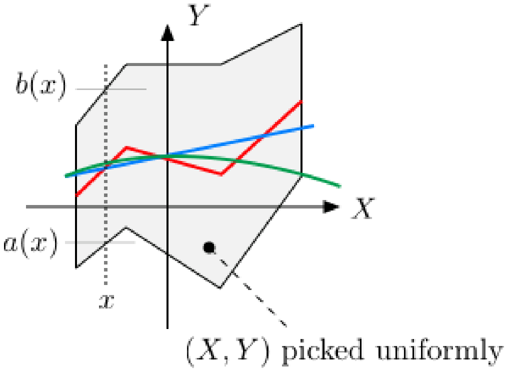
14. Which is $E[Y|X]$? Blue, red or green?



Answer: Red.
Given $X = x, Y = U[a(x), b(x)]$.

Quiz 1: G

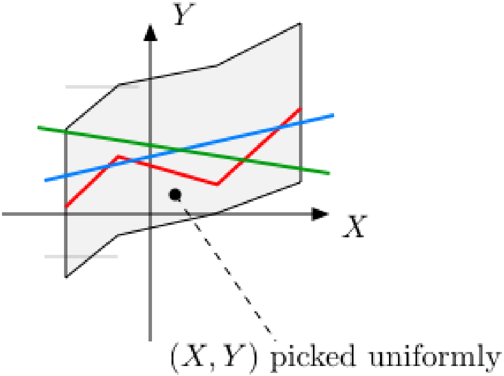
14. Which is $E[Y|X]$? Blue, red or green?



Answer: Red.
Given $X = x, Y = U[a(x), b(x)]$. Thus, $E[Y|X = x] = \frac{a(x)+b(x)}{2}$.

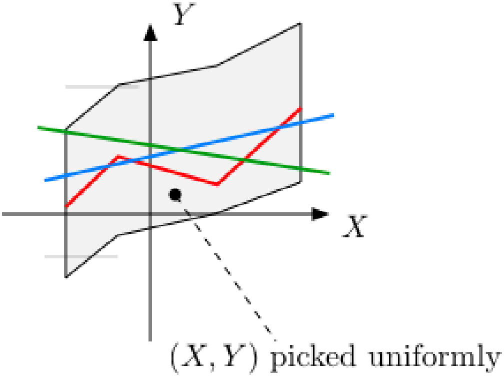
Quiz 1: G

15. Which is $L[Y|X]$? Blue, red or green?



Quiz 1: G

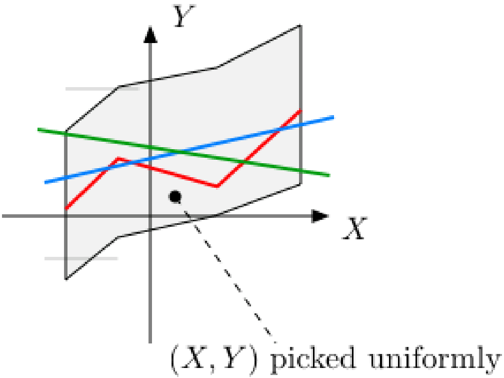
15. Which is $L[Y|X]$? Blue, red or green?



Answer: Blue.

Quiz 1: G

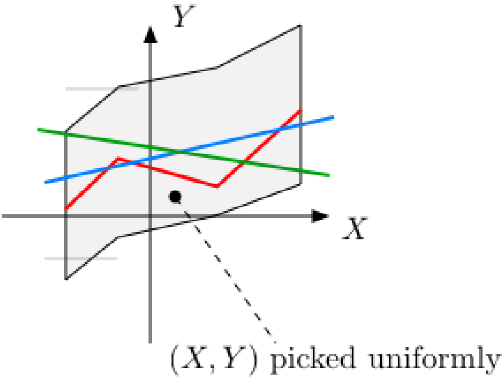
15. Which is $L[Y|X]$? Blue, red or green?



Answer: Blue.
Cannot be red (not a straight line).

Quiz 1: G

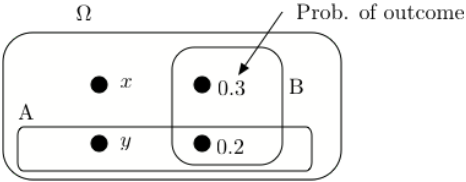
15. Which is $L[Y|X]$? Blue, red or green?



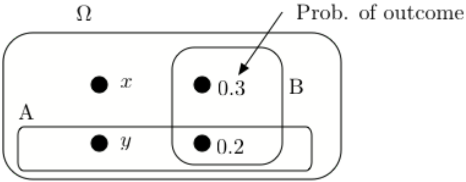
Answer: Blue.
Cannot be red (not a straight line).
Cannot be green: X and Y are clearly positively correlated.

Quiz 2: PG

Quiz 2: PG

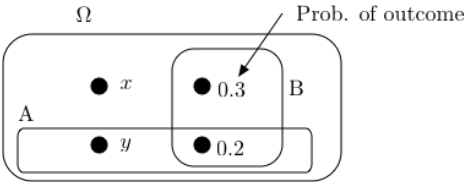


Quiz 2: PG



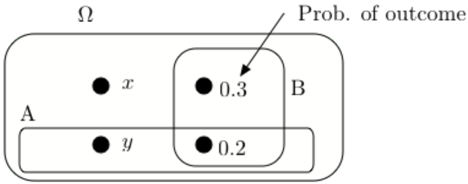
1. Find (x, y) so that A and B are independent.

Quiz 2: PG



1. Find (x, y) so that A and B are independent.
   We need
   $$Pr[A \cap B] = Pr[A]Pr[B]$$

Quiz 2: PG



1. Find (x, y) so that A and B are independent.

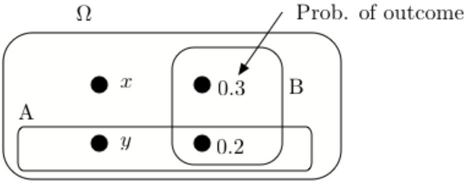
   We need

   $$Pr[A \cap B] = Pr[A]Pr[B]$$

   That is,

   $$0.2 = (y + 0.2) \times 0.5 =$$

Quiz 2: PG



1. Find (x, y) so that A and B are independent.

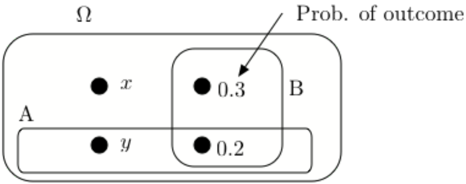
   We need

$$Pr[A \cap B] = Pr[A]Pr[B]$$

   That is,

$$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$

Quiz 2: PG



1. Find (x, y) so that A and B are independent.

   We need

   $$Pr[A \cap B] = Pr[A]Pr[B]$$

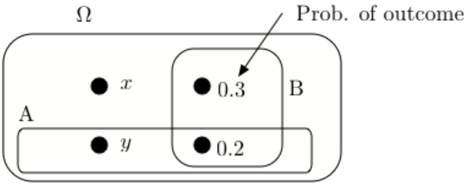
   That is,

   $$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$

   Hence,

   $$y = 0.2$$

Quiz 2: PG



1. Find (x, y) so that A and B are independent.

   We need

   $$Pr[A \cap B] = Pr[A]Pr[B]$$

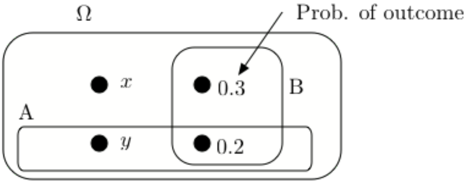
   That is,

   $$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$

   Hence,

   $$y = 0.2 \text{ and } x =$$

Quiz 2: PG



1. Find (x, y) so that A and B are independent.

   We need

   $$Pr[A \cap B] = Pr[A]Pr[B]$$

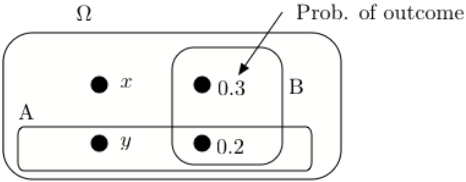
   That is,

   $$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$

   Hence,

   $$y = 0.2 \text{ and } x = 0.3.$$

Quiz 2: PG

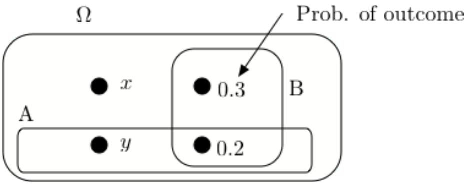


1. Find (x, y) so that A and B are independent.

   We need
   $$Pr[A \cap B] = Pr[A]Pr[B]$$
   That is,
   $$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$
   Hence,
   $$y = 0.2 \text{ and } x = 0.3.$$

2. Find the value of x that maximizes $Pr[B|A]$.

Quiz 2: PG



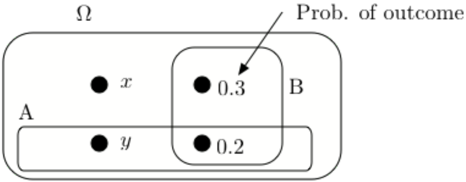
1. Find (x, y) so that A and B are independent.

   We need
   $$Pr[A \cap B] = Pr[A]Pr[B]$$
   That is,
   $$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$
   Hence,
   $$y = 0.2 \text{ and } x = 0.3.$$

2. Find the value of x that maximizes $Pr[B|A]$.

   Obviously, it is $x =$

Quiz 2: PG



1. Find (x, y) so that A and B are independent.

   We need

   $$Pr[A \cap B] = Pr[A]Pr[B]$$

   That is,

   $$0.2 = (y + 0.2) \times 0.5 = 0.5y + 0.1$$

   Hence,

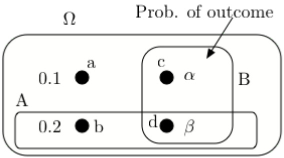
   $$y = 0.2 \text{ and } x = 0.3.$$

2. Find the value of x that maximizes $Pr[B|A]$.

   Obviously, it is $x = 0.5$.

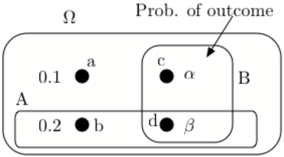
Quiz 2: PG

Quiz 2: PG



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

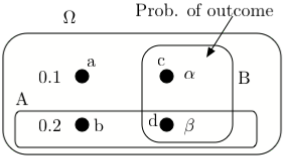
Quiz 2: PG



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

3. Find α so that X and Y are independent.

Quiz 2: PG



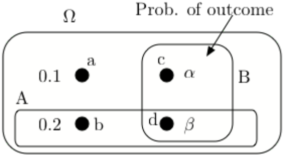
ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

3. Find α so that X and Y are independent.

   We need

$$Pr[X = 0, Y = 0] = Pr[X = 0]Pr[Y = 0]$$

Quiz 2: PG



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

3. Find α so that X and Y are independent.

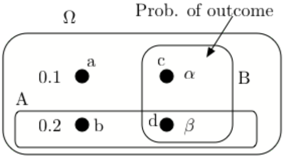
   We need

$$Pr[X=0, Y=0] = Pr[X=0]Pr[Y=0]$$

   That is,

$$0.1 = (0.1+\alpha)\times(0.1+0.2) =$$

Quiz 2: PG



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

3. Find α so that X and Y are independent.

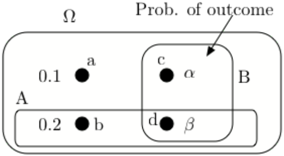
   We need

   $$Pr[X=0,Y=0]=Pr[X=0]Pr[Y=0]$$

   That is,

   $$0.1=(0.1+\alpha)\times(0.1+0.2)=0.03+0.3\alpha$$

Quiz 2: PG



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

3. Find α so that X and Y are independent.

We need

$$Pr[X=0, Y=0] = Pr[X=0]Pr[Y=0]$$

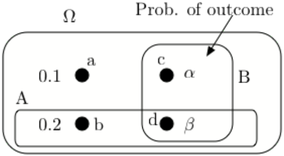
That is,

$$0.1 = (0.1+\alpha) \times (0.1+0.2) = 0.03 + 0.3\alpha$$

Hence,

$$\alpha = 0.233$$

Quiz 2: PG



ω	$X(\omega)$	$Y(\omega)$
a	0	0
b	1	0
c	0	2
d	1	2

3. Find α so that X and Y are independent.

   We need

$$Pr[X=0, Y=0] = Pr[X=0]Pr[Y=0]$$

   That is,

$$0.1 = (0.1+\alpha)\times(0.1+0.2) = 0.03+0.3\alpha$$

   Hence,

$$\alpha = 0.233$$

Quiz 2: PG

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7.

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6.

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1

Quiz 2: PG

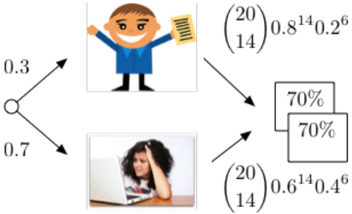
4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2.

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?

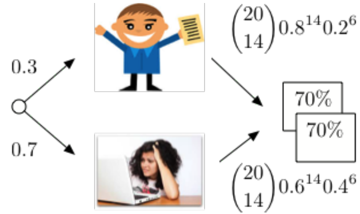
Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?



Quiz 2: PG

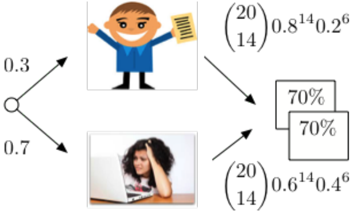
4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?



$p := Pr[\text{great}|\text{scores}] =$

Quiz 2: PG

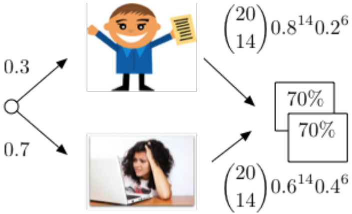
4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?



$$p := Pr[\text{great}|\text{scores}] = \frac{0.3\binom{20}{14}0.8^{14}0.2^{6}}{0.3\binom{20}{14}0.8^{14}0.2^{6} + 0.7\binom{20}{14}0.6^{14}0.4^{6}}$$

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?

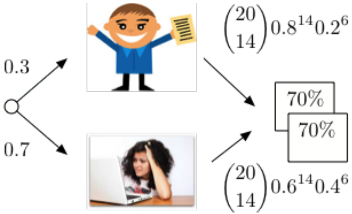


$$p := Pr[\text{great}|\text{scores}] = \frac{0.3\binom{20}{14}0.8^{14}0.2^6}{0.3\binom{20}{14}0.8^{14}0.2^6 + 0.7\binom{20}{14}0.6^{14}0.4^6}$$

$$= \frac{(0.3)0.8^{14}0.2^6}{(0.3)0.8^{14}0.2^6 + (0.7)0.6^{14}0.4^6}$$

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?

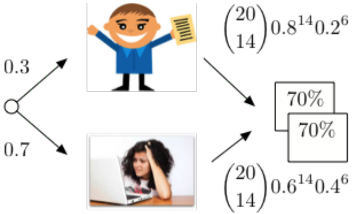


$$p := Pr[\text{great}|\text{scores}] = \frac{0.3\binom{20}{14}0.8^{14}0.2^6}{0.3\binom{20}{14}0.8^{14}0.2^6 + 0.7\binom{20}{14}0.6^{14}0.4^6}$$

$$= \frac{(0.3)0.8^{14}0.2^6}{(0.3)0.8^{14}0.2^6 + (0.7)0.6^{14}0.4^6} \approx 0.27$$

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?



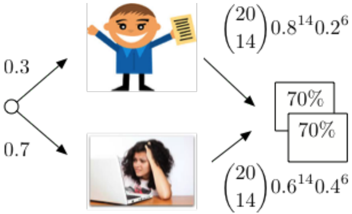
$$p := Pr[\text{great}|\text{scores}] = \frac{0.3\binom{20}{14}0.8^{14}0.2^{6}}{0.3\binom{20}{14}0.8^{14}0.2^{6} + 0.7\binom{20}{14}0.6^{14}0.4^{6}}$$

$$= \frac{(0.3)0.8^{14}0.2^{6}}{(0.3)0.8^{14}0.2^{6} + (0.7)0.6^{14}0.4^{6}} \approx 0.27$$

Expected score $=$

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?



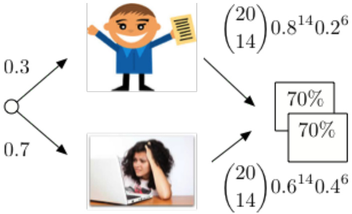
$$p := Pr[\text{great}|\text{scores}] = \frac{0.3\binom{20}{14}0.8^{14}0.2^{6}}{0.3\binom{20}{14}0.8^{14}0.2^{6} + 0.7\binom{20}{14}0.6^{14}0.4^{6}}$$

$$= \frac{(0.3)0.8^{14}0.2^{6}}{(0.3)0.8^{14}0.2^{6} + (0.7)0.6^{14}0.4^{6}} \approx 0.27$$

Expected score $= p80\% + (1-p)60\% \approx$

Quiz 2: PG

4. A CS70 student is great w.p. 0.3 and good w.p. 0.7. A great student solves each question correctly w.p. 0.8 whereas a good student does it w.p. 0.6. One student got right 70% of the 10 questions on Midterm 1 and 70% of the 10 questions on Midterm 2. What is the expected score of the student on the final?



$$p := Pr[\text{great}|\text{scores}] = \frac{0.3\binom{20}{14}0.8^{14}0.2^{6}}{0.3\binom{20}{14}0.8^{14}0.2^{6} + 0.7\binom{20}{14}0.6^{14}0.4^{6}}$$

$$= \frac{(0.3)0.8^{14}0.2^{6}}{(0.3)0.8^{14}0.2^{6} + (0.7)0.6^{14}0.4^{6}} \approx 0.27$$

Expected score $= p80\% + (1-p)60\% \approx 65\%.$

Quiz 2: PG

Quiz 2: PG

5. You roll a balanced six-sided die 20 times.

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\frac{X - 70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$

where

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then
$$\frac{X - 70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$
where
$$\sigma^2 = var(X_1) =$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\frac{X - 70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$

where

$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then
$$\frac{X-70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$
where
$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx 2.9$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\frac{X-70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$

where

$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx 2.9 = 1.7^2.$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\frac{X - 70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$

where

$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx 2.9 = 1.7^2.$$

Now,

$$Pr[X > 85] \quad = \quad Pr[X - 70 > 15]$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then
$$\frac{X-70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$
where
$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx 2.9 = 1.7^2.$$
Now,
$$\begin{aligned} Pr[X > 85] &= Pr[X - 70 > 15] \\ &= Pr[\frac{X-70}{1.7 \times 4.5} > \frac{15}{1.7 \times 4.5}] \end{aligned}$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\frac{X - 70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$

where

$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx 2.9 = 1.7^2.$$

Now,

$$\begin{aligned} Pr[X > 85] &= Pr[X - 70 > 15] \\ &= Pr[\frac{X-70}{1.7 \times 4.5} > \frac{15}{1.7 \times 4.5}] \\ &= Pr[\frac{X-70}{1.7 \times 4.5} > 2] \end{aligned}$$

Quiz 2: PG

5. You roll a balanced six-sided die 20 times. Use CLT to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\frac{X - 70}{\sigma\sqrt{20}} \approx \mathcal{N}(0,1)$$

where

$$\sigma^2 = var(X_1) = (1/6)\sum_{m=1}^{6} m^2 - (3.5)^2 \approx 2.9 = 1.7^2.$$

Now,

$$\begin{aligned} Pr[X > 85] &= Pr[X - 70 > 15] \\ &= Pr[\frac{X-70}{1.7 \times 4.5} > \frac{15}{1.7 \times 4.5}] \\ &= Pr[\frac{X-70}{1.7 \times 4.5} > 2] \approx 2.5\%. \end{aligned}$$

Quiz 2: PG

Quiz 2: PG

6. You roll a balanced six-sided die 20 times.

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$Pr[X > 85] \quad = \quad Pr[X - 70 > 15]$$

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$Pr[X > 85] \quad = \quad Pr[X - 70 > 15] \leq Pr[|X - 70| > 15]$$

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\begin{aligned} Pr[X > 85] &= Pr[X - 70 > 15] \leq Pr[|X - 70| > 15] \\ &\leq \frac{var(X)}{15^2}. \end{aligned}$$

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\begin{aligned} Pr[X > 85] &= Pr[X - 70 > 15] \leq Pr[|X - 70| > 15] \\ &\leq \frac{var(X)}{15^2}. \end{aligned}$$

Now,

$$var(X) = 20 var(X_1) = 20 \times 2.9 = 58.$$

Quiz 2: PG

6. You roll a balanced six-sided die 20 times. Use Chebyshev to upper-bound the probability that the total number of dots exceeds 85.

Let $X = X_1 + \cdots + X_{20}$ be the total number of dots.
Then

$$\begin{aligned} Pr[X > 85] &= Pr[X - 70 > 15] \leq Pr[|X - 70| > 15] \\ &\leq \frac{var(X)}{15^2}. \end{aligned}$$

Now,

$$var(X) = 20 var(X_1) = 20 \times 2.9 = 58.$$

Hence,

$$Pr[X > 85] \leq \frac{58}{15^2} \approx 0.26.$$

Quiz 2: PG

Quiz 2: PG

7. Let X, Y, Z be i.i.d. *Expo*(1).

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$.

Quiz 2: PG

7. Let X, Y, Z be i.i.d. *Expo*(1). Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$L[X|V] =$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1,$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$

$$E[X] = 1, E[V] =$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X + 2Y + 3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X + 2Y + 3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$
$$cov(X,V) =$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$
$$cov(X,V) = var(X) =$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$
$$cov(X,V) = var(X) = 1$$
$$var(V) =$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X + 2Y + 3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$
$$cov(X,V) = var(X) = 1$$
$$var(V) = 1 + 4 + 9 = 14.$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X + 2Y + 3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$
$$cov(X,V) = var(X) = 1$$
$$var(V) = 1 + 4 + 9 = 14.$$

   Hence,

$$L[X|V] = 1 + \frac{1}{14}(V - 6).$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$\begin{aligned} L[X|V] &= E[X] + \frac{cov(X,V)}{var(V)}(V - E[V]) \\ E[X] &= 1, E[V] = 6 \\ cov(X,V) &= var(X) = 1 \\ var(V) &= 1+4+9 = 14. \end{aligned}$$

   Hence,

$$L[X|V] = 1 + \frac{1}{14}(V-6).$$

8. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $E[X+Z|X+Y]$.

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$
\begin{aligned}
L[X|V] &= E[X] + \frac{cov(X,V)}{var(V)}(V - E[V]) \\
E[X] &= 1, E[V] = 6 \\
cov(X,V) &= var(X) = 1 \\
var(V) &= 1+4+9 = 14.
\end{aligned}
$$

   Hence,

$$L[X|V] = 1 + \frac{1}{14}(V-6).$$

8. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $E[X+Z|X+Y]$.

$$E[X+Z|X+Y] \quad = \quad E[X|X+Y] + E[Z]$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X + 2Y + 3Z$. One finds

$$
\begin{aligned}
L[X|V] &= E[X] + \frac{cov(X,V)}{var(V)}(V - E[V]) \\
E[X] &= 1, E[V] = 6 \\
cov(X,V) &= var(X) = 1 \\
var(V) &= 1 + 4 + 9 = 14.
\end{aligned}
$$

   Hence,

$$L[X|V] = 1 + \frac{1}{14}(V - 6).$$

8. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $E[X+Z|X+Y]$.

$$
\begin{aligned}
E[X+Z|X+Y] &= E[X|X+Y] + E[Z] \\
&= \frac{1}{2}(X+Y) + 1.
\end{aligned}
$$

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.
   Let $V = X+2Y+3Z$. One finds

$$
\begin{aligned}
L[X|V] &= E[X] + \frac{cov(X,V)}{var(V)}(V - E[V]) \\
E[X] &= 1, E[V] = 6 \\
cov(X,V) &= var(X) = 1 \\
var(V) &= 1+4+9 = 14.
\end{aligned}
$$

   Hence,

$$L[X|V] = 1 + \frac{1}{14}(V-6).$$

8. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $E[X+Z|X+Y]$.

$$
\begin{aligned}
E[X+Z|X+Y] &= E[X|X+Y] + E[Z] \\
&= \frac{1}{2}(X+Y) + 1.
\end{aligned}
$$

9. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $L[X+Z|X+Y]$.

Quiz 2: PG

7. Let X, Y, Z be i.i.d. $Expo(1)$. Find $L[X|X+2Y+3Z]$.

   Let $V = X + 2Y + 3Z$. One finds

$$L[X|V] = E[X] + \frac{cov(X,V)}{var(V)}(V - E[V])$$
$$E[X] = 1, E[V] = 6$$
$$cov(X,V) = var(X) = 1$$
$$var(V) = 1 + 4 + 9 = 14.$$

   Hence,

$$L[X|V] = 1 + \frac{1}{14}(V - 6).$$

8. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $E[X+Z|X+Y]$.

$$\begin{aligned} E[X+Z|X+Y] &= E[X|X+Y] + E[Z] \\ &= \frac{1}{2}(X+Y) + 1. \end{aligned}$$

9. Let X, Y, Z be i.i.d. $Expo(1)$. Calculate $L[X+Z|X+Y]$.

$$L[X+Z|X+Y] = \frac{1}{2}(X+Y) + 1.$$

Q2: PG

10. You roll a balanced die.

Q2: PG

10. You roll a balanced die.

    You start with $1.00.

Q2: PG

10. You roll a balanced die.

    You start with $1.00.

    Every time you get a 6, your fortune is multiplied by 10.

Q2: PG

10. You roll a balanced die.

    You start with \$1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

Q2: PG

10. You roll a balanced die.

    You start with \$1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

Q2: PG

10. You roll a balanced die.

    You start with \$1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

Q2: PG

10. You roll a balanced die.

    You start with \$1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

We have $X_1 = 1$.

Q2: PG

10. You roll a balanced die.

    You start with \$1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

We have $X_1 = 1$. Also,

$$E[X_{n+1}|X_n] \quad = \quad X_n \times [10\frac{1}{6} + 0.5 \times \frac{5}{6}]$$

Q2: PG

10. You roll a balanced die.

    You start with $1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

We have $X_1 = 1$. Also,

$$\begin{aligned} E[X_{n+1}|X_n] &= X_n \times [10\frac{1}{6} + 0.5 \times \frac{5}{6}] \\ &= \rho X_n, \rho = 10\frac{1}{6} + 0.5 \times \frac{5}{6} \end{aligned}$$

Q2: PG

10. You roll a balanced die.

    You start with \$1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

We have $X_1 = 1$. Also,

$$\begin{aligned} E[X_{n+1}|X_n] &= X_n \times [10\frac{1}{6} + 0.5 \times \frac{5}{6}] \\ &= \rho X_n, \rho = 10\frac{1}{6} + 0.5 \times \frac{5}{6} \approx 2.1. \end{aligned}$$

Q2: PG

10. You roll a balanced die.

    You start with $1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

We have $X_1 = 1$. Also,

$$\begin{aligned} E[X_{n+1}|X_n] &= X_n \times [10\frac{1}{6} + 0.5 \times \frac{5}{6}] \\ &= \rho X_n, \rho = 10\frac{1}{6} + 0.5 \times \frac{5}{6} \approx 2.1. \end{aligned}$$

Hence,

$$E[X_{n+1}] = \rho E[X_n], n \geq 1.$$

Q2: PG

10. You roll a balanced die.

    You start with $1.00.

    Every time you get a 6, your fortune is multiplied by 10.

    Every time you do not get a 6, your fortune is divided by 2.

    Let X_n be your fortune at the start of step n,

    Calculate $E[X_n]$.

We have $X_1 = 1$. Also,

$$\begin{aligned} E[X_{n+1}|X_n] &= X_n \times [10\frac{1}{6} + 0.5 \times \frac{5}{6}] \\ &= \rho X_n, \rho = 10\frac{1}{6} + 0.5 \times \frac{5}{6} \approx 2.1. \end{aligned}$$

Hence,

$$E[X_{n+1}] = \rho E[X_n], n \geq 1.$$

Thus,

$$E[X_n] = \rho^{n-1}, n \geq 1.$$

Quiz 3: R

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year.

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8.

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective.

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year.

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs?

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb,

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good,

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

$$(a) \qquad p := Pr[G|X \in (0.6, 0.6+\delta)]$$

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

$$(a) \qquad p := Pr[G | X \in (0.6, 0.6 + \delta)]$$

$$= \frac{0.5 Pr[X \in (0.6, 0.6+\delta) | G]}{0.5 Pr[X \in (0.6, 0.6+\delta) | G] + 0.5 Pr[X \in (0.6, 0.6+\delta) | D]}$$

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

$$(a) \qquad p := Pr[G | X \in (0.6, 0.6 + \delta)]$$

$$= \frac{0.5 Pr[X \in (0.6, 0.6 + \delta) | G]}{0.5 Pr[X \in (0.6, 0.6 + \delta) | G] + 0.5 Pr[X \in (0.6, 0.6 + \delta) | D]}$$

$$= \frac{e^{-0.6} \delta}{e^{-0.6} \delta + (0.8)^{-1} e^{-(0.8)^{-1} 0.6} \delta}$$

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

$$(a) \qquad p := Pr[G|X \in (0.6, 0.6 + \delta)]$$

$$= \frac{0.5Pr[X \in (0.6, 0.6 + \delta)|G]}{0.5Pr[X \in (0.6, 0.6 + \delta)|G] + 0.5Pr[X \in (0.6, 0.6 + \delta)|D]}$$

$$= \frac{e^{-0.6}\delta}{e^{-0.6}\delta + (0.8)^{-1}e^{-(0.8)^{-1}0.6}\delta} \approx 0.488.$$

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

$$
\begin{aligned}
(a) \qquad p &:= Pr[G|X \in (0.6, 0.6+\delta)] \\
&= \frac{0.5Pr[X \in (0.6, 0.6+\delta)|G]}{0.5Pr[X \in (0.6, 0.6+\delta)|G] + 0.5Pr[X \in (0.6, 0.6+\delta)|D]} \\
&= \frac{e^{-0.6}\delta}{e^{-0.6}\delta + (0.8)^{-1}e^{-(0.8)^{-1}0.6}\delta} \approx 0.488. \\
(b) \qquad & E[\text{ lifespan of other bulb }] =
\end{aligned}
$$

Quiz 3: R

1. The lifespans of good lightbulbs are exponentially distributed with mean 1 year. Those of defective bulbs are exponentially distributed with mean 0.8. All the bulbs in one batch are equally likely to be good or defective. You test one bulb and note that it burns out after 0.6 year. (a) What is the probability you got a batch of good bulbs? (b) What is the expected lifespan of another bulb in that batch?

   Hint: If $X = Expo(\lambda), f_X(x) = \lambda e^{-\lambda x} 1\{x > 0\}, E[X] = 1/\lambda$.

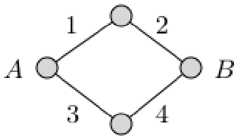
Let X be the lifespan of a bulb, G the event that it is good, and B the event that it is bad.

$$
\begin{aligned}
(a) \qquad p &:= Pr[G | X \in (0.6, 0.6+\delta)] \\
&= \frac{0.5 Pr[X \in (0.6, 0.6+\delta) | G]}{0.5 Pr[X \in (0.6, 0.6+\delta) | G] + 0.5 Pr[X \in (0.6, 0.6+\delta) | D]} \\
&= \frac{e^{-0.6}\delta}{e^{-0.6}\delta + (0.8)^{-1} e^{-(0.8)^{-1} 0.6}\delta} \approx 0.488.
\end{aligned}
$$

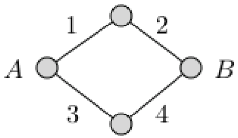
$$
(b) \qquad E[\text{ lifespan of other bulb }] = p \times 1 + (1-p) \times 0.8 \approx 0.9.
$$

Quiz 3: R

Quiz 3: R

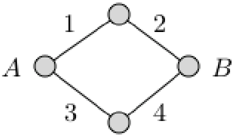


Quiz 3: R



2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

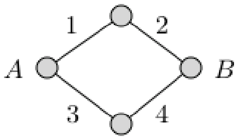
Quiz 3: R



2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Quiz 3: R

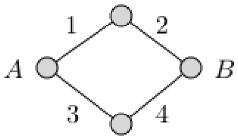


2. In the figure, $1,2,3,4$ are links that fail after i.i.d. times that are $U[0,1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1,\ldots,4$.

Quiz 3: R

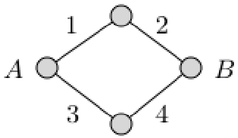


2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with

Quiz 3: R

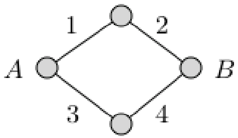


2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with
$Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

Quiz 3: R



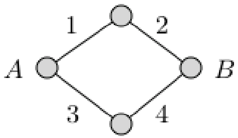
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0,1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$Pr[Y_1 > t] \quad = \quad Pr[X_1 > t]Pr[X_2 > t]$$

Quiz 3: R



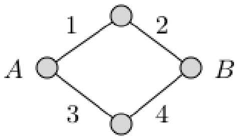
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$Pr[Y_1 > t] = Pr[X_1 > t]Pr[X_2 > t] = (1 - t)^2$$

Quiz 3: R



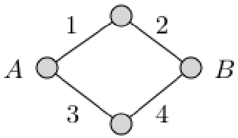
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$\begin{aligned} Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1-t)^2 \\ Pr[Z \leq t] &= Pr[Y_1 \leq t]Pr[Y_2 \leq t] \end{aligned}$$

Quiz 3: R



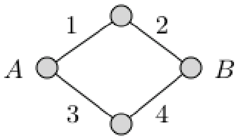
2. In the figure, $1,2,3,4$ are links that fail after i.i.d. times that are $U[0,1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1,\ldots,4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$
\begin{aligned}
Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1-t)^2 \\
Pr[Z \le t] &= Pr[Y_1 \le t]Pr[Y_2 \le t] = (1-(1-t)^2)^2
\end{aligned}
$$

Quiz 3: R



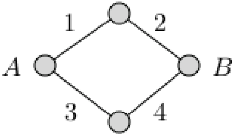
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0,1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$
\begin{aligned}
Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1-t)^2 \\
Pr[Z \leq t] &= Pr[Y_1 \leq t]Pr[Y_2 \leq t] = (1-(1-t)^2)^2 \\
&= (2t - t^2)^2
\end{aligned}
$$

Quiz 3: R



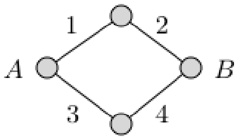
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$\begin{aligned} Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1-t)^2 \\ Pr[Z \le t] &= Pr[Y_1 \le t]Pr[Y_2 \le t] = (1-(1-t)^2)^2 \\ &= (2t - t^2)^2 = 4t^2 - 4t^3 + t^4 \end{aligned}$$

Quiz 3: R



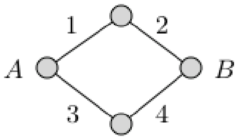
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0,1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$
\begin{aligned}
Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1-t)^2 \\
Pr[Z \leq t] &= Pr[Y_1 \leq t]Pr[Y_2 \leq t] = (1-(1-t)^2)^2 \\
&= (2t - t^2)^2 = 4t^2 - 4t^3 + t^4 \\
f_Z(t) &= 8t - 12t^2 + 4t^3
\end{aligned}
$$

Quiz 3: R



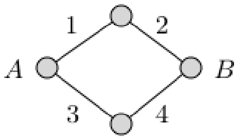
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with
$Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$\begin{aligned}
Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1 - t)^2 \\
Pr[Z \leq t] &= Pr[Y_1 \leq t]Pr[Y_2 \leq t] = (1 - (1 - t)^2)^2 \\
&= (2t - t^2)^2 = 4t^2 - 4t^3 + t^4 \\
f_Z(t) &= 8t - 12t^2 + 4t^3 \\
E[Z] &= \int_0^1 t f_Z(t) dt
\end{aligned}$$

Quiz 3: R



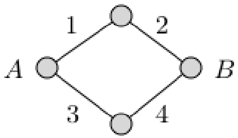
2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0,1]$.

   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

$$
\begin{aligned}
Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1-t)^2 \\
Pr[Z \leq t] &= Pr[Y_1 \leq t]Pr[Y_2 \leq t] = (1-(1-t)^2)^2 \\
&= (2t - t^2)^2 = 4t^2 - 4t^3 + t^4 \\
f_Z(t) &= 8t - 12t^2 + 4t^3 \\
E[Z] &= \int_0^1 t f_Z(t) dt = 8\frac{1}{3} - 12\frac{1}{4} + 4\frac{1}{5}
\end{aligned}
$$

Quiz 3: R



2. In the figure, $1, 2, 3, 4$ are links that fail after i.i.d. times that are $U[0, 1]$.

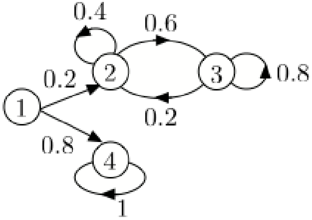
   Find the average time until A and B are disconnected.

Let X_k be the lifespan of link k, for $k = 1, \ldots, 4$.
We are looking for $E[Z]$ where $Z = \max\{Y_1, Y_2\}$ with $Y_1 = \min\{X_1, X_2\}$ and $Y_2 = \min\{X_3, X_4\}$.

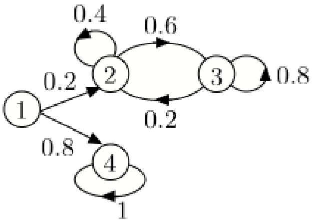
$$
\begin{aligned}
Pr[Y_1 > t] &= Pr[X_1 > t]Pr[X_2 > t] = (1 - t)^2 \\
Pr[Z \leq t] &= Pr[Y_1 \leq t]Pr[Y_2 \leq t] = (1 - (1 - t)^2)^2 \\
&= (2t - t^2)^2 = 4t^2 - 4t^3 + t^4 \\
f_Z(t) &= 8t - 12t^2 + 4t^3 \\
E[Z] &= \int_0^1 t f_Z(t) dt = 8\frac{1}{3} - 12\frac{1}{4} + 4\frac{1}{5} \\
&\approx 0.4667.
\end{aligned}
$$

Quiz 3: R

Quiz 3: R

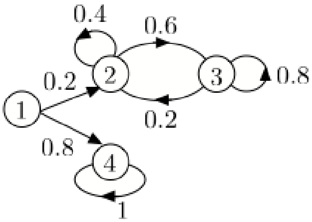


Quiz 3: R



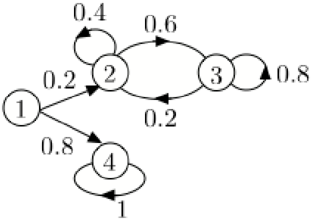
3. We are given π_0.

Quiz 3: R



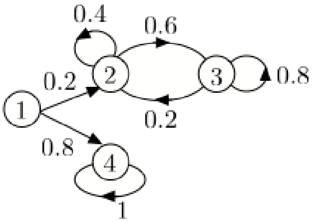
3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.

Quiz 3: R



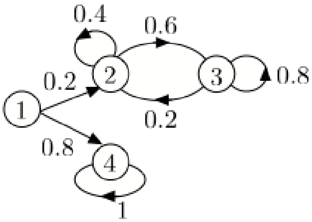
3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.
   With probability $\alpha := 0.2\pi_0(1) + \pi_0(2) + \pi_0(3)$, the MC ends up in $\{2,3\}$.

Quiz 3: R



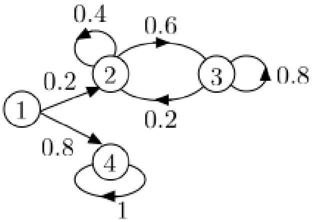
3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.
   With probability $\alpha := 0.2\pi_0(1) + \pi_0(2) + \pi_0(3)$, the MC ends up in $\{2,3\}$.
   With probability $1-\alpha$, it ends up in state 4.

Quiz 3: R



3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.
   With probability $\alpha := 0.2\pi_0(1) + \pi_0(2) + \pi_0(3)$, the MC ends up in $\{2,3\}$.
   With probability $1-\alpha$, it ends up in state 4.
   If it is in $\{2,3\}$, the probability that it is in state 2 converges to

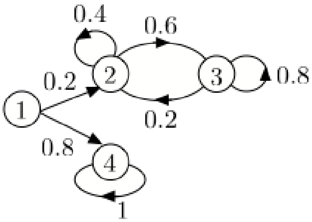
Quiz 3: R



3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.
   With probability $\alpha := 0.2\pi_0(1) + \pi_0(2) + \pi_0(3)$, the MC ends up in $\{2,3\}$.
   With probability $1-\alpha$, it ends up in state 4.
   If it is in $\{2,3\}$, the probability that it is in state 2 converges to

$$\frac{0.2}{0.2+0.6} = 0.25.$$

Quiz 3: R

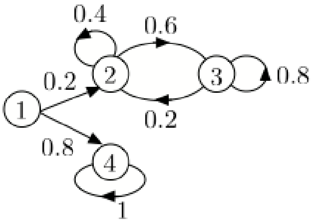


3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.
   With probability $\alpha := 0.2\pi_0(1) + \pi_0(2) + \pi_0(3)$, the MC ends up in $\{2,3\}$.
   With probability $1-\alpha$, it ends up in state 4.
   If it is in $\{2,3\}$, the probability that it is in state 2 converges to

$$\frac{0.2}{0.2+0.6} = 0.25.$$

   Hence, the limiting distribution is

Quiz 3: R



3. We are given π_0. Find $\lim_{n\to\infty} \pi_n$.
   With probability $\alpha := 0.2\pi_0(1) + \pi_0(2) + \pi_0(3)$, the MC ends up in $\{2,3\}$.
   With probability $1-\alpha$, it ends up in state 4.
   If it is in $\{2,3\}$, the probability that it is in state 2 converges to

$$\frac{0.2}{0.2+0.6} = 0.25.$$

   Hence, the limiting distribution is

$$[0, 0.25\alpha, 0.75\alpha, 1-\alpha].$$

Quiz 3: R

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement).

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise.

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.
   $$cov(X, Y) = E[XY] - E[X]E[Y]$$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$,

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X,Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y]$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X,Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X,Y)$.

   $cov(X,Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

   $E[XY] = 2(n-1)/(2n-1) - 1 = -1/(2n-1)$

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X,Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

   $E[XY] = 2(n-1)/(2n-1) - 1 = -1/(2n-1) = cov(X,Y)$.

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

   $E[XY] = 2(n-1)/(2n-1) - 1 = -1/(2n-1) = cov(X, Y)$.

6. What is $L[Y|X]$?

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X,Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

   $E[XY] = 2(n-1)/(2n-1) - 1 = -1/(2n-1) = cov(X,Y)$.

6. What is $L[Y|X]$? $L[Y|X] = -\frac{1}{2n-1}X$.

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X, Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

   $E[XY] = 2(n-1)/(2n-1) - 1 = -1/(2n-1) = cov(X, Y)$.

6. What is $L[Y|X]$? $L[Y|X] = -\frac{1}{2n-1}X$. Indeed, $var(X) = 1$,

Quiz 3: R

4. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   $\rightarrow$ Are X and Y positively, negatively, or un- correlated?

   Clearly, negatively.

5. Calculate $cov(X, Y)$.

   $cov(X,Y) = E[XY] - E[X]E[Y]$

   $E[X] = E[Y]$, by symmetry

   $E[X] = 0$

   $E[XY] = Pr[X = Y] - Pr[X \neq Y] = 2Pr[X = Y] - 1$

   $Pr[X = Y] = (n-1)/(2n-1)$

   E.g., if $X = +1$ = red, then Y is red w.p. $(n-1)/(2n-1)$

   $E[XY] = 2(n-1)/(2n-1) - 1 = -1/(2n-1) = cov(X,Y)$.

6. What is $L[Y|X]$? $L[Y|X] = -\frac{1}{2n-1}X$. Indeed, $var(X) = 1$, obviously!

Quiz 3: R

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Since X takes only two values, any $g(X)$ is linear in X.

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Since X takes only two values, any $g(X)$ is linear in X.
Hence, $E[Y|X] = L[Y|X]$.

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Since X takes only two values, any $g(X)$ is linear in X.
Hence, $E[Y|X] = L[Y|X]$.

Alternatively, Let $\alpha = Pr[X = Y] = (n-1)(2n-1)$.

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Since X takes only two values, any $g(X)$ is linear in X.
Hence, $E[Y|X] = L[Y|X]$.

Alternatively, Let $\alpha = Pr[X = Y] = (n-1)(2n-1)$.Then,

$$E[Y|X = 1] = \alpha - (1-\alpha) = 2\alpha - 1,$$

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Since X takes only two values, any $g(X)$ is linear in X.
Hence, $E[Y|X] = L[Y|X]$.

Alternatively, Let $\alpha = Pr[X = Y] = (n-1)(2n-1)$.Then,

$$E[Y|X=1] = \alpha - (1-\alpha) = 2\alpha - 1,$$
$$E[Y|X=-1] = -\alpha + (1-\alpha) = 1 - 2\alpha.$$

Quiz 3: R

7. A bag has n red and n blue balls. You pick two balls (no replacement). Let $X = 1$ if ball 1 is red and $X = -1$ otherwise. Define Y likewise for ball 2.
   Calculate $E[Y|X]$.

Since X takes only two values, any $g(X)$ is linear in X.
Hence, $E[Y|X] = L[Y|X]$.

Alternatively, Let $\alpha = Pr[X = Y] = (n-1)(2n-1)$.Then,

$$E[Y|X=1] = \alpha - (1-\alpha) = 2\alpha - 1,$$
$$E[Y|X=-1] = -\alpha + (1-\alpha) = 1 - 2\alpha.$$

Thus,

$$E[Y|X] = (2\alpha - 1)X = -\frac{1}{2n-1}X.$$

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0$, $Y = 1$.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0$, $Y = 1$. No: They are independent.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.

Common Mistakes

- $\Omega = \{1, 2, 3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.

- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$.

Common Mistakes

- $\Omega = \{1, 2, 3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.

- $3 \times 3.5 = 12.5$. No.

- $E[X^2] = E[X]^2$. No.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$.

Common Mistakes

- $\Omega = \{1, 2, 3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n, p) \implies var(X) = n^2 p(1 - p)$. No.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$.

Common Mistakes

- $\Omega = \{1, 2, 3\}$. Define X, Y with $cov(X, Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let
  $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n, p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.
- CS70 is difficult.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.
- CS70 is difficult. No.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.
- CS70 is difficult. No.
- I will do poorly on the final.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.
- CS70 is difficult. No.
- I will do poorly on the final. No.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.
- CS70 is difficult. No.
- I will do poorly on the final. No.
- Rao is bad at copying.

Common Mistakes

- $\Omega = \{1,2,3\}$. Define X, Y with $cov(X,Y) = 0$ and X, Y not independent.

  Let $X = 0, Y = 1$. No: They are independent.

  Let $X(1) = -1, X(2) = 0, X(1) = 1, Y(1) = 0, Y(2) = 1, Y(3) = 0$.
- $3 \times 3.5 = 12.5$. No.
- $E[X^2] = E[X]^2$. No.
- $X = B(n,p) \implies var(X) = n^2 p(1-p)$. No.
- $E[X] = E[X|A] + E[X|\bar{A}]$. No.
- $\sum_{n=0}^{\infty} a^n = 1/a$. No.
- CS70 is difficult. No.
- I will do poorly on the final. No.
- Rao is bad at copying. Probably!.

Thanks and Best Wishes!

Thanks and Best Wishes!