Proof by Contradiction.
Sets of Sets.
(Recap: NP)
Lecture 21
Boolean Circuits
Boolean Circuits

A directed acyclic graph: Boolean valued wires, AND, OR, NOT gates, inputs, output
Boolean Circuits

A directed acyclic graph: Boolean valued wires, AND, OR, NOT gates, inputs, output

Circuit evaluation CKT-VAL: given circuit C and inputs x, find C(x) (i.e., C’s boolean output value, on input x)
Boolean Circuits

- A directed acyclic graph: Boolean valued wires, AND, OR, NOT gates, inputs, output

- Circuit evaluation **CKT-VAL**: given circuit C and inputs x, find C(x) (i.e., C’s boolean output value, on input x)

- Can be done very efficiently: if done in the right order, evaluating each wire takes $O(1)$ time. CKT-VAL is in P
Boolean Circuits

- A directed acyclic graph: Boolean valued wires, AND, OR, NOT gates, inputs, output

- Circuit evaluation **CKT-VAL**: given circuit $C$ and inputs $x$, find $C(x)$ (i.e., $C$'s boolean output value, on input $x$)

- Can be done very efficiently: if done in the right order, evaluating each wire takes $O(1)$ time. CKT-VAL is in P

- **CKT-SAT**: given circuit $C$, is there a “satisfying” input for $C$ (s.t. output=1)? i.e., $\exists x \ C(x)=1$? In NP.
Boolean Circuits

A directed acyclic graph: Boolean valued wires, AND, OR, NOT gates, inputs, output

Circuit evaluation **CKT-VAL**: given circuit C and inputs x, find C(x) (i.e., C's boolean output value, on input x)

Can be done very efficiently: if done in the right order, evaluating each wire takes \(O(1)\) time. CKT-VAL is in P

**CKT-SAT**: given circuit C, is there a "satisfying" input for C (s.t. output=1)? i.e., \(\exists x \ C(x)=1\)? In NP.

**CKT-SAT**: given C, is it that there is no satisfying input. i.e., \(\forall x \ C(x)=0\)? In co-NP.
P & NP
P & NP

P: Class of decision problems \( \mathcal{P} \) that can be solved in polynomial time
P & NP

P: Class of decision problems $\mathcal{A}$ that can be solved in polynomial time

HasSolution$_\mathcal{A}$(instance) can be computed in polynomial time
P & NP

P: Class of decision problems $\mathcal{A}$ that can be solved in polynomial time

- HasSolution$_{\mathcal{A}}$(instance) can be computed in polynomial time

NP: Class of decision problems $\mathcal{A}$ that can be proven/verified to have a solution, in polynomial time
P & NP

P: Class of decision problems $\mathcal{A}$ that can be solved in polynomial time

\[ \text{HasSolution}_\mathcal{A}(\text{instance}) \text{ can be computed in polynomial time} \]

NP: Class of decision problems $\mathcal{A}$ that can be proven/verified to have a solution, in polynomial time

\[ \text{HasSolution}_\mathcal{A}(\text{instance}) \equiv \exists \text{cert } \text{Verify}_\mathcal{A}(\text{instance, cert}), \text{ where } \text{Verify}_\mathcal{A} \text{ can be computed in polynomial time} \]
P & NP

P: Class of decision problems $\mathcal{A}$ that can be solved in polynomial time

HasSolution$_\mathcal{A}$(instance) can be computed in polynomial time

NP: Class of decision problems $\mathcal{A}$ that can be proven/verified to have a solution, in polynomial time

HasSolution$_\mathcal{A}$(instance) = $\exists$cert Verify$_\mathcal{A}$(instance,cert), where Verify$_\mathcal{A}$ can be computed in polynomial time

Equivalently, class of decision problems associated with search problems for which a solution (if it exists) can be found in polynomial time with “guidance”
P & NP

P: Class of decision problems \( \mathcal{A} \) that can be solved in polynomial time

- \( \text{HasSolution}_{\mathcal{A}} \)(instance) can be computed in polynomial time

NP: Class of decision problems \( \mathcal{A} \) that can be proven/verified to have a solution, in polynomial time

- \( \text{HasSolution}_{\mathcal{A}} \)(instance) \( \equiv \exists \text{cert} \ \text{Verify}_{\mathcal{A}} \)(instance, cert), where \( \text{Verify}_{\mathcal{A}} \) can be computed in polynomial time

- Equivalently, class of decision problems associated with search problems for which a solution (if it exists) can be found in polynomial time with "guidance"

- Non-deterministic computation
P & NP
P & NP

NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time
P & NP

NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time

HasSolution(instance) \equiv \exists \text{cert } \text{Verify(instance, cert)}, \text{ where Verify can be computed in polynomial time}
NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time

\[ \text{HasSolution(instance)} \equiv \exists \text{cert } \text{Verify(instance,cert)}, \text{ where Verify can be computed in polynomial time} \]

Every problem in P is in NP
P & NP

NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time

\[ \text{HasSolution(instance)} \equiv \exists \text{cert } \text{Verify(instance,cert)}, \text{ where Verify can be computed in polynomial time} \]

Every problem in P is in NP

**CKT-SAT**: instance: circuit C. \( \text{HasSol}_{\text{CKT-SAT}}(C) = 1 \) iff C satisfiable
P & NP

NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time

\[ \text{HasSolution(instance)} \equiv \exists \text{cert Verify(instance,cert)}, \text{ where Verify can be computed in polynomial time} \]

Every problem in P is in NP

CKT-SAT: instance: circuit C. \[ \text{HasSol}_{\text{CKT-SAT}}(C) = 1 \text{ iff } C \text{ satisfiable} \]

3COL: instance: graph G. \[ \text{HasSol}_{3\text{COL}}(G) = 1 \text{ iff } \chi(G) \leq 3 \]
**P & NP**

- NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time

\[ \text{HasSolution(instance)} \equiv \exists \text{cert Verify(instance,cert)}, \text{ where Verify can be computed in polynomial time} \]

- Every problem in P is in NP

- **CKT-SAT**: instance: circuit C. HasSol\text{\_CKT-SAT}(C) = 1 iff C satisfiable

- **3COL**: instance: graph G. HasSol\text{\_3COL}(G) = 1 iff \( \chi(G) \leq 3 \)

  Certificate: an explicit coloring; verifiable in polynomial time.
NP: Class of decision problems that can be proven/verified to have a solution, in polynomial time

\[ \text{HasSolution(instance)} \equiv \exists \text{cert} \ \text{Verify(instance,cert)}, \text{ where Verify can be computed in polynomial time} \]

Every problem in P is in NP

\text{CKT-SAT: instance: circuit C. HasSol_{CKT-SAT}(C) = 1 iff C satisfiable}

\text{3COL: instance: graph G. HasSol_{3COL}(G) = 1 iff } \chi(G) \leq 3

Certificate: an explicit coloring; verifiable in polynomial time.

Not known to be in co-NP: When G has no 3-coloring, is there always a certificate to prove it? When C is not satisfiable?
NP-completeness
NP-completeness

- Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other
NP-completeness

Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other.

If any one of them is in P, then all of them are in P!
NP-completeness

- Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other.
- If any one of them is in P, then all of them are in P!
- Further, then P=NP! (And then P = NP = co-NP)
NP-completeness

- Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other.
  - If any one of them is in P, then all of them are in P!
  - Further, then P=NP! (And then P = NP = co-NP)
- Proving $P \neq NP$ is the same as proving (say) $\text{CKT-SAT} \notin P$
Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other.

If any one of them is in P, then all of them are in P!

Further, then \( P = \text{NP} \) (And then \( P = \text{NP} = \text{co-NP} \))

Proving \( P \neq \text{NP} \) is the same as proving (say) \( \text{CKT-SAT} \notin \text{P} \)

And proving \( P = \text{NP} \) is the same as proving \( \text{CKT-SAT} \in \text{P} \)
NP-completeness

- Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other.
- If any one of them is in P, then all of them are in P!
- Further, then $P=NP$! (And then $P = NP = co-NP$)
- Proving $P \neq NP$ is the same as proving (say) $CKT\text{-}SAT \notin P$
- And proving $P=NP$ is the same as proving $CKT\text{-}SAT \in P$
- Over 40 years (and counting) of failed attempts at finding polynomial-time algorithms for any of the NP complete problems
NP-completeness

Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other

- If any one of them is in P, then all of them are in P!
- Further, then P=NP! (And then P = NP = co-NP)

Proving P≠NP is the same as proving (say) CKT-SAT∉P

And proving P=NP is the same as proving CKT-SAT∈P

Over 40 years (and counting) of failed attempts at finding polynomial-time algorithms for any of the NP complete problems

Several practically important problems are known to be in NP or co-NP, but not known to be in P. Related to finding the smallest circuitry for a device, finding optimal airline scheduling, breaking a public-key encryption scheme, ...
NP-completeness

- Graph 3-colorability, CKT-SAT and several other problems in NP are tightly related to each other
  - If any one of them is in P, then all of them are in P!
  - Further, then P=NP! (And then P = NP = co-NP)
- Proving P≠NP is the same as proving (say) CKT-SAT∉P
- And proving P=NP is the same as proving CKT-SAT∈P
- Over 40 years (and counting) of failed attempts at finding polynomial-time algorithms for any of the NP complete problems
- Several practically important problems are known to be in NP or co-NP, but not known to be in P. Related to finding the smallest circuitry for a device, finding optimal airline scheduling, breaking a public-key encryption scheme, ...
- The Million Dollar Question: is P=NP?
Proof by Contradiction
Proof by Contradiction
Proof by Contradiction

To prove a proposition p, show that $\neg p \rightarrow F$
Proof by Contradiction

- To prove a proposition $p$, show that $\neg p \rightarrow F$

- Or, $\neg p \rightarrow (q \land \neg q)$ (where $q \land \neg q$ is a “contradiction”; it implies $F$)
Proof by Contradiction

To prove a proposition \( p \), show that \( \neg p \rightarrow F \)

Or, \( \neg p \rightarrow (q \land \neg q) \) (\( q \land \neg q \) is a “contradiction”; it implies \( F \))

e.g., \( C_5 \) is not bipartite
Proof by Contradiction

- To prove a proposition $p$, show that $\neg p \rightarrow F$

- Or, $\neg p \rightarrow (q \land \neg q)$ (where $q \land \neg q$ is a "contradiction"; it implies $F$)

- e.g., $C_5$ is not bipartite

- Suppose, for the sake of contradiction, that $C_5$ is bipartite. Then there is a valid coloring $f: V \rightarrow \{1,2\}$. 
Proof by Contradiction

- To prove a proposition $p$, show that $\neg p \rightarrow F$

- Or, $\neg p \rightarrow (q \land \neg q)$ (q $\land$ $\neg q$ is a “contradiction”; it implies F)

- e.g., $C_5$ is not bipartite

Suppose, for the sake of contradiction, that $C_5$ is bipartite. Then there is a valid coloring $f: V \rightarrow \{1,2\}$.

Let $V=\{0,...,4\}$. W.l.o.g, $f(0)=1$. Since $\{0,1\} \in E$, $f(1) \neq f(0)$, so $f(1)=2$. Since $\{1,2\} \in E$, $f(2) \neq f(1)$, so $f(2)=1$. Similarly, $f(3)=2$, $f(4)=1$. So $f(4)=f(0)$. 
Proof by Contradiction

To prove a proposition $p$, show that $\neg p \rightarrow F$

Or, $\neg p \rightarrow (q \land \neg q)$ ($q \land \neg q$ is a “contradiction”; it implies $F$)

E.g., $C_5$ is not bipartite

Suppose, for the sake of contradiction, that $C_5$ is bipartite. Then there is a valid coloring $f: V \rightarrow \{1, 2\}$.

Let $V = \{0, \ldots, 4\}$. W.l.o.g, $f(0) = 1$. Since $\{0, 1\} \in E$, $f(1) \neq f(0)$, so $f(1) = 2$. Since $\{1, 2\} \in E$, $f(2) \neq f(1)$, so $f(2) = 1$. Similarly, $f(3) = 2$, $f(4) = 1$. So $f(4) = f(0)$.

But $\{0, 4\} \in E$. So $f$ not a valid coloring! Hence contradiction! So our initial assumption wrong.
Contradiction & Contrapositive
Contradiction & Contrapositive

Proof by contradiction: To prove a proposition $p$, show that $\neg p \rightarrow \text{F}$
Contradiction & Contrapositive

Proof by contradiction: To prove a proposition p, show that \(\neg p \rightarrow F\)

Or, \(\neg p \rightarrow (q \land \neg q)\) (\(q \land \neg q\) is a “contradiction”; it implies F)
Contradiction & Contrapositive

Proof by contradiction: To prove a proposition \( p \), show that \( \neg p \rightarrow F \)

Or, \( \neg p \rightarrow (q \wedge \neg q) \) (\( q \wedge \neg q \) is a “contradiction”; it implies \( F \))

Proof by contradiction could be viewed as proving the contrapositive of \( T \rightarrow p \)
Contradiction & Contrapositive

**Proof by contradiction:** To prove a proposition $p$, show that $\neg p \rightarrow F$

Or, $\neg p \rightarrow (q \land \neg q)$ ($q \land \neg q$ is a "contradiction"; it implies $F$)

Proof by contradiction could be viewed as proving the contrapositive of $T \rightarrow p$

For statements $p$ of the form $p_1 \rightarrow p_2$, proving the contrapositive could be seen as part of a proof by contradiction.
Contradiction & Contrapositive

Proof by contradiction: To prove a proposition $p$, show that $\neg p \rightarrow F$

Or, $\neg p \rightarrow (q \land \neg q)$ (q $\land$ $\neg$q is a “contradiction”; it implies F)

Proof by contradiction could be viewed as proving the contrapositive of $T \rightarrow p$

For statements $p$ of the form $p_1 \rightarrow p_2$, proving the contrapositive could be seen as part of a proof by contradiction.

Suppose $\neg p$. i.e., $p_1 \land \neg p_2$. 

Proof by contradiction: To prove a proposition $p$, show that $\neg p \rightarrow F$

Or, $\neg p \rightarrow (q \land \neg q)$ (where $q \land \neg q$ is a “contradiction”; it implies $F$)

Proof by contradiction could be viewed as proving the contrapositive of $T \rightarrow p$

For statements $p$ of the form $p_1 \rightarrow p_2$, proving the contrapositive could be seen as part of a proof by contradiction.

Suppose $\neg p$. i.e., $p_1 \land \neg p_2$.

Show that $\neg p_2 \rightarrow \neg p_1$. Then, since $\neg p_2$, we have $\neg p_1$. 
Contradiction & Contrapositive

- **Proof by contradiction**: To prove a proposition $p$, show that $\neg p \rightarrow F$
  
  - Or, $\neg p \rightarrow (q \land \neg q)$ (where $q \land \neg q$ is a “contradiction”; it implies $F$)

- Proof by contradiction could be viewed as proving the contrapositive of $T \rightarrow p$

- For statements $p$ of the form $p_1 \rightarrow p_2$, proving the contrapositive could be seen as part of a proof by contradiction.

  - Suppose $\neg p$. i.e., $p_1 \land \neg p_2$.
  
  - **Show that** $\neg p_2 \rightarrow \neg p_1$. Then, since $\neg p_2$, we have $\neg p_1$.
  
  - Hence $p_1$ and $\neg p_1$. Contradiction! Hence $p$. 
√2 is Irrational
√2 is Irrational

Suppose for the sake of contradiction, √2 is rational
\( \sqrt{2} \) is Irrational

- Suppose for the sake of contradiction, \( \sqrt{2} \) is rational.
- Then \( \exists a, b \in \mathbb{Z}^+ \) s.t. \( \sqrt{2} = \frac{a}{b} \) and \( \gcd(a, b) = 1 \).
\sqrt{2} is Irrational

Suppose for the sake of contradiction, \sqrt{2} is rational

Then \exists a,b \in \mathbb{Z}^+ \text{ s.t. } \sqrt{2} = a/b \text{ and } \gcd(a,b) = 1.

Obtained from \sqrt{2} = p/q, taking a = p/\gcd(p,q), b = q/\gcd(p,q)
Suppose for the sake of contradiction, $\sqrt{2}$ is rational

Then $\exists a, b \in \mathbb{Z}^+$ s.t. $\sqrt{2} = a/b$ and $\gcd(a, b) = 1$.

Obtained from $\sqrt{2} = p/q$, taking $a = p/\gcd(p, q)$, $b = q/\gcd(p, q)$

Hence $2 = a^2/b^2$. That is, $2b^2 = a^2$, or $a^2$ even.
$\sqrt{2}$ is Irrational

Suppose for the sake of contradiction, $\sqrt{2}$ is rational.

Then $\exists a, b \in \mathbb{Z}^+ \text{ s.t. } \sqrt{2} = a/b$ and $\gcd(a, b) = 1$.

Obtained from $\sqrt{2} = p/q$, taking $a = p/\gcd(p, q)$, $b = q/\gcd(p, q)$

Hence $2 = a^2/b^2$. That is, $2b^2 = a^2$, or $a^2$ even.

Then $a$ is even: because, if $a$ odd then $a^2$ odd.
\[
\sqrt{2} \text{ is Irrational}
\]

Suppose for the sake of contradiction, \( \sqrt{2} \) is rational

Then \( \exists a, b \in \mathbb{Z}^+ \) s.t. \( \sqrt{2} = a/b \) and \( \gcd(a, b) = 1 \).

Obtained from \( \sqrt{2} = p/q \), taking \( a = p/\gcd(p, q) \), \( b = q/\gcd(p, q) \)

Hence \( 2 = a^2/b^2 \). That is, \( 2b^2 = a^2 \), or \( a^2 \) even.

Then \( a \) is even: because, if \( a \) odd then \( a^2 \) odd.

Proof by contradiction.

Or, contrapositive of the statement

\( a \) odd \( \rightarrow \) \( a^2 \) odd
Proof by contradiction. Or, contrapositive of the statement
\( a \text{ odd } \rightarrow a^2 \text{ odd} \)

\[ \sqrt{2} \text{ is Irrational} \]

Suppose for the sake of contradiction, \( \sqrt{2} \) is rational

Then \( \exists a, b \in \mathbb{Z}^+ \text{ s.t. } \sqrt{2} = a/b \text{ and } \gcd(a, b) = 1. \)

Obtained from \( \sqrt{2} = p/q \), taking \( a = p / \gcd(p, q) \), \( b = q / \gcd(p, q) \)

Hence \( 2 = a^2 / b^2 \). That is, \( 2b^2 = a^2 \), or \( a^2 \) even.

Then \( a \) is even: because, if \( a \) odd then \( a^2 \) odd

Let \( a = 2m \). \( 2b^2 = 4m^2 \rightarrow b^2 = 2m^2 \). Now \( b \) is even.
√2 is Irrational

Proof by contradiction. Or, contrapositive of the statement

a odd → a² odd

Suppose for the sake of contradiction, √2 is rational

Then ∃a,b∈Z⁺ s.t. √2=a/b and gcd(a,b)=1.

Obtained from √2=p/q, taking a=p/gcd(p,q), b=q/gcd(p,q)

Hence 2=a²/b². That is, 2b² = a², or a² even.

Then a is even: because, if a odd then a² odd

Let a=2m. 2b²=4m² → b²=2m². Now b is even.

So 2|a and 2|b → gcd(a,b)=1. Contradiction! Hence √2 rational.
Infinitely Many Primes
Infinitely Many Primes

Claim: There are infinitely many primes
Infinitely Many Primes

Claim: There are infinitely many primes

Proof: Suppose for the sake of contradiction there are only finitely many primes: \( p_1 < p_2 < \ldots < p_n \) (all \( p_i > 1 \))
Claim: There are infinitely many primes

Proof: Suppose for the sake of contradiction there are only finitely many primes: $p_1 < p_2 < \ldots < p_n$ (all $p_i > 1$)

Consider $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$
Claim: There are infinitely many primes

Proof: Suppose for the sake of contradiction there are only finitely many primes: \( p_1 < p_2 < \ldots < p_n \) (all \( p_i > 1 \))

Consider \( q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \)

\[ \forall i \in [n], \gcd(q, p_i) = \gcd(p_i, \text{remainder}(q, p_i)) = \gcd(p_i, 1) = 1 \]
Infinitely Many Primes

Claim: There are infinitely many primes

Proof: Suppose for the sake of contradiction there are only finitely many primes: \( p_1 < p_2 < \ldots < p_n \) (all \( p_i > 1 \))

Consider \( q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \)

\[ \forall i \in [n], \, \gcd(q, p_i) = \gcd(p_i, \text{remainder}(q, p_i)) = \gcd(p_i, 1) = 1 \]

But we have seen (prime factorization theorem a.k.a the Fundamental Theorem of Arithmetic) that some prime number must divide \( q \). Contradiction!
Claim: There are infinitely many primes

Proof: Suppose for the sake of contradiction there are only finitely many primes: $p_1 < p_2 < ... < p_n$ (all $p_i > 1$)

Consider $q = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$

$\forall i \in [n], \gcd(q, p_i) = \gcd(p_i, \text{remainder}(q, p_i)) = \gcd(p_i, 1) = 1$

But we have seen (prime factorization theorem a.k.a the Fundamental Theorem of Arithmetic) that some prime number must divide $q$. Contradiction!

Aside: Can be turned into a (not very efficient) algorithm to generate an infinite list of primes, starting with any finite set
Infinitely Many Primes

Claim: There are infinitely many primes

Proof: Suppose for the sake of contradiction there are only finitely many primes: \( p_1 < p_2 < \ldots < p_n \) (all \( p_i > 1 \))

Consider \( q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \)

\( \forall i \in [n], \gcd(q, p_i) = \gcd(p_i, \text{remainder}(q, p_i)) = \gcd(p_i, 1) = 1 \)

But we have seen (prime factorization theorem a.k.a the Fundamental Theorem of Arithmetic) that some prime number must divide \( q \). Contradiction!

Aside: Can be turned into a (not very efficient) algorithm to generate an infinite list of primes, starting with any finite set

\( \text{e.g. } \{2, 5\} \rightarrow \{2, 5, 11\} \rightarrow \{2, 5, 11, 3\} \) (3 is a factor of \( 2 \cdot 5 \cdot 11 + 1 \))
Lossless vs. Compression
Lossless vs. Compression

- Truly random data is incompressible
Lossless vs. Compression

- Truly random data is incompressible.

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement
- A lossless compression is a one-to-one function from the set of all strings to the same set

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement.
- A lossless compression is a one-to-one function from the set of all strings to the same set.
- If a lossless compression shrinks some strings, then it must expand some others.

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement.
- A lossless compression is a one-to-one function from the set of all strings to the same set.
- If a lossless compression shrinks some strings, then it must expand some others.

\[ L \land S \rightarrow E \]

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement
- A lossless compression is a one-to-one function from the set of all strings to the same set
- If a lossless compression shrinks some strings, then it must expand some others

\[ L \land S \rightarrow E \]

L: f is lossless.
S: f shrinks some string.
E: f expands some string.

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement.
- A lossless compression is a one-to-one function from the set of all strings to the same set.
- If a lossless compression shrinks some strings, then it must expand some others.

\[ L \land S \rightarrow E \]

Heart of the proof: \[ S \land \neg E \rightarrow \neg L \]

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.
Lossless vs. Compression

- Truly random data is incompressible
- A (simpler) combinatorial statement
- A lossless compression is a one-to-one function from the set of all strings to the same set
- If a lossless compression shrinks some strings, then it must expand some others

\( L \land S \rightarrow E \)

L: f is lossless.
S: f shrinks some string.
E: f expands some string.

Heart of the proof: \( S \land \neg E \rightarrow \neg L \)

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.

\[ \exists x \in \{0,1\}^* \text{ s.t. } |x| > |f(x)|. \]

Let \( |f(x)| = m \). Since \( \neg E \), all strings in \( \{0,1\}^m \) also map to \( \{0,1\}^{\leq m} \), in addition to \( x \). By pigeonhole principle, \( f \) not one-to-one
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement.
- A lossless compression is a one-to-one function from the set of all strings to the same set.
- If a lossless compression shrinks some strings, then it must expand some others.

\[ L \land S \rightarrow E \]

- Heart of the proof: \( S \land \neg E \rightarrow \neg L \)
- As a proof by contradiction: Assume \( L \land S \land \neg E \). Derive \( \neg L \). Contradiction!

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.

\[ \exists x \in \{0,1\}^* \text{ s.t. } \lvert x \rvert > \lvert f(x) \rvert. \]
Let \( \lvert f(x) \rvert = m \). Since \( \neg E \), all strings in \( \{0,1\}^{\leq m} \) also map to \( \{0,1\}^{\leq m} \), in addition to \( x \). By pigeonhole principle, \( f \) not one-to-one.
Lossless vs. Compression

- Truly random data is incompressible.
- A (simpler) combinatorial statement:
  - A lossless compression is a one-to-one function from the set of all strings to the same set.
  - If a lossless compression shrinks some strings, then it must expand some others.
- L \land S \rightarrow E

Heart of the proof: S \land \neg E \rightarrow \neg L

As a proof by contradiction: Assume L \land S \land \neg E. Derive \neg L. Contradiction!

- Or: (S \land \neg E \rightarrow \neg L) \equiv (\neg S \lor E \lor \neg L) \equiv \neg (L \land S) \lor E \equiv (L \land S) \rightarrow E

Formalized in Information Theory. Admits probabilistic notions. Shows no non-trivial trade-off between losslessness and compression.

∃x \in \{0,1\}^* \text{ s.t. } |x|>|f(x)|.

Let |f(x)|=m. Since \neg E, all strings in \{0,1\}^m also map to \{0,1\}^{\leq m}, in addition to x. By pigeonhole principle, f not one-to-one.
Bi-partite Graph
Bi-partite Graph

Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite
Bi-partite Graph

Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite

Base case: \( n=1 \). \( C_3 \) has chromatic number 3. ✔
Claim: for all integers n ≥ 1, C_{2n+1} is not bi-partite

Base case: n=1. C_3 has chromatic number 3. ✔

Induction step: For all integers k ≥ 2:
Induction hypothesis: C_{2k-1} is not bi-partite (corresponds to n=k-1)
To prove: C_{2k+1} is not bi-partite (corresponds to n=k)
Bi-partite Graph

Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$ :
Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite
Bi-partite Graph

Claim: for all integers $n \geq 1$, $C_{2n+1}$ is **not** bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$ :
Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite
Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$ :
Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite
i.e., valid 2-coloring $c: \{0, \ldots, 2k\} \rightarrow \{1, 2\}$ of $C_{2k+1}$. 
Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite

Base case: \( n=1 \). \( C_3 \) has chromatic number 3. ✔

Induction step: For all integers \( k \geq 2 \):
Induction hypothesis: \( C_{2k-1} \) is not bi-partite (corresponds to \( n=k-1 \))
To prove: \( C_{2k+1} \) is not bi-partite (corresponds to \( n=k \))

Suppose (for the sake of contradiction) \( C_{2k+1} \) bi-partite
i.e., valid 2-coloring \( c:\{0,\ldots,2k\} \rightarrow \{1,2\} \) of \( C_{2k+1} \).
Then, \( c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2) \). i.e., \( c(0)=c(2k-1)\neq c(2k-2) \).
Bi-partite Graph

Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$:

Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)

To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite

i.e., valid 2-coloring $c: \{0, \ldots, 2k\} \rightarrow \{1,2\}$ of $C_{2k+1}$.

Then, $c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2)$. i.e., $c(0)=c(2k-1)
eq c(2k-2)$. 


Bi-partite Graph

Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite

Base case: \( n=1 \). \( C_3 \) has chromatic number 3. ✔

Induction step: For all integers \( k \geq 2 \):

Induction hypothesis: \( C_{2k-1} \) is not bi-partite (corresponds to \( n=k-1 \))
To prove: \( C_{2k+1} \) is not bi-partite (corresponds to \( n=k \))

Suppose (for the sake of contradiction) \( C_{2k+1} \) bi-partite

i.e., valid 2-coloring \( c:\{0,..,2k\} \rightarrow \{1,2\} \) of \( C_{2k+1} \).

Then, \( c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2) \). i.e., \( c(0)=c(2k-1)\neq c(2k-2) \).
Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite.

Base case: \( n=1 \). \( C_3 \) has chromatic number 3.

Induction step: For all integers \( k \geq 2 \):
- Induction hypothesis: \( C_{2k-1} \) is not bi-partite (corresponds to \( n=k-1 \)).
- To prove: \( C_{2k+1} \) is not bi-partite (corresponds to \( n=k \)).

Suppose (for the sake of contradiction) \( C_{2k+1} \) bi-partite.
- i.e., valid 2-coloring \( c: \{0, \ldots, 2k\} \to \{1,2\} \) of \( C_{2k+1} \).
- Then, \( c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2) \). i.e., \( c(0) = c(2k-1) \neq c(2k-2) \).
Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$:
Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite

i.e., valid 2-coloring $c: \{0, \ldots, 2k\} \rightarrow \{1,2\}$ of $C_{2k+1}$.

Then, $c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2)$. i.e., $c(0)=c(2k-1) \neq c(2k-2)$. 

Bi-partite Graph

- $C_{2k+1}$
Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite.

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$:
Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite
i.e., valid 2-coloring $c:\{0,\ldots,2k\} \to \{1,2\}$ of $C_{2k+1}$.
Then, $c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2)$. i.e., $c(0)=c(2k-1)\neq c(2k-2)$.
Only edge in $C_{2k-1}$ not in $C_{2k+1}$ is $\{0,2k-2\}$. 
Bi-partite Graph

Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$:
Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite
i.e., valid 2-coloring $c:\{0,..,2k\} \rightarrow \{1,2\}$ of $C_{2k+1}$.
Then, $c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2)$. i.e., $c(0)=c(2k-1)\neq c(2k-2)$.
Only edge in $C_{2k-1}$ not in $C_{2k+1}$ is $\{0,2k-2\}$.
Claim: for all integers $n \geq 1$, $C_{2n+1}$ is not bi-partite

Base case: $n=1$. $C_3$ has chromatic number 3. ✔

Induction step: For all integers $k \geq 2$:

- Induction hypothesis: $C_{2k-1}$ is not bi-partite (corresponds to $n=k-1$)
- To prove: $C_{2k+1}$ is not bi-partite (corresponds to $n=k$)

Suppose (for the sake of contradiction) $C_{2k+1}$ bi-partite

i.e., valid 2-coloring $c:\{0,\ldots,2k\} \rightarrow \{1,2\}$ of $C_{2k+1}$.

Then, $c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2)$. i.e., $c(0)=c(2k-1)\neq c(2k-2)$.

Only edge in $C_{2k-1}$ not in $C_{2k+1}$ is $\{0,2k-2\}$.

So $c$ respects all edges of $C_{2k-1}$.
Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite.

Base case: \( n=1 \). \( C_3 \) has chromatic number 3. ✔

Induction step: For all integers \( k \geq 2 \):
Induction hypothesis: \( C_{2k-1} \) is not bi-partite (corresponds to \( n=k-1 \))
To prove: \( C_{2k+1} \) is not bi-partite (corresponds to \( n=k \))

Suppose (for the sake of contradiction) \( C_{2k+1} \) bi-partite
i.e., valid 2-coloring \( c:\{0,..,2k\} \rightarrow \{1,2\} \) of \( C_{2k+1} \).
Then, \( c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2) \). i.e., \( c(0)=c(2k-1) \neq c(2k-2) \).
Only edge in \( C_{2k-1} \) not in \( C_{2k+1} \) is \( \{0,2k-2\} \).
So \( c \) respects all edges of \( C_{2k-1} \).
So \( c':\{0,..,2k-2\} \rightarrow \{1,2\} \) with \( c'(u)=c(u) \) is a valid coloring of \( C_{2k-1} \).
Bi-partite Graph

Claim: for all integers \( n \geq 1 \), \( C_{2n+1} \) is not bi-partite

Base case: \( n=1 \). \( C_3 \) has chromatic number 3. ✔

Induction step: For all integers \( k \geq 2 \)
Induction hypothesis: \( C_{2k-1} \) is not bi-partite (corresponds to \( n=k-1 \))
To prove: \( C_{2k+1} \) is not bi-partite (corresponds to \( n=k \))

Suppose (for the sake of contradiction) \( C_{2k+1} \) bi-partite

i.e., valid 2-coloring \( c:\{0,..,2k\} \rightarrow \{1,2\} \) of \( C_{2k+1} \).

Then, \( c(0) \neq c(2k) \neq c(2k-1) \neq c(2k-2) \). i.e., \( c(0)=c(2k-1)\neq c(2k-2) \).

Only edge in \( C_{2k-1} \) not in \( C_{2k+1} \) is \( \{0,2k-2\} \).

So \( c \) respects all edges of \( C_{2k-1} \).

So \( c':\{0,..,2k-2\} \rightarrow \{1,2\} \) with \( c'(u)=c(u) \) is a valid coloring of \( C_{2k-1} \).

Contradiction (with the ind’n hypothesis)! So \( C_{2k+1} \) not bi-partite.
Sets of Sets
Set of Sets
Set of Sets

Sets are a very general notion, and can contain anything as an element (not just elements of the same "type")
Set of Sets

- Sets are a very general notion, and can contain anything as an element (not just elements of the same “type”)

- We will restrict to sets with elements from a “well-defined” universe (typically with all elements of the same “type”: e.g. \( \mathbb{Z}, \mathbb{Z} \times \mathbb{Z} \) etc. but not \( \mathbb{Z} \cup \mathbb{Z} \times \mathbb{Z} \))
Set of Sets

- Sets are a very general notion, and can contain anything as an element (not just elements of the same “type”)
- We will restrict to sets with elements from a “well-defined” universe (typically with all elements of the same “type”: e.g. $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$ etc. but not $\mathbb{Z} \cup \mathbb{Z} \times \mathbb{Z}$)
- Another useful universe to consider: consists of sets with elements from a “ground set”
Set of Sets

Sets are a very general notion, and can contain anything as an element (not just elements of the same “type”)

We will restrict to sets with elements from a “well-defined” universe (typically with all elements of the same “type”: e.g. $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$ etc. but not $\mathbb{Z} \cup \mathbb{Z} \times \mathbb{Z}$)

Another useful universe to consider: consists of sets with elements from a “ground set”

- e.g. Ground set = $\mathbb{Z}$. Some elements in this universe include the set of even numbers, the set of odd numbers, $\{1,2\}$, $\emptyset$, $\mathbb{Z}$, etc.
Set of Sets

Sets are a very general notion, and can contain anything as an element (not just elements of the same “type”).

We will restrict to sets with elements from a “well-defined” universe (typically with all elements of the same “type”: e.g. \(\mathbb{Z}, \mathbb{Z} \times \mathbb{Z}\) etc. but not \(\mathbb{Z} \cup \mathbb{Z} \times \mathbb{Z}\)).

Another useful universe to consider: consists of sets with elements from a “ground set”

- e.g. Ground set = \(\mathbb{Z}\). Some elements in this universe include the set of even numbers, the set of odd numbers, \{1,2\}, \(\emptyset\), \(\mathbb{Z}\), etc.

We can consider a collection of these sets itself as a set (with elements from the new universe).
Set of Sets: Box of boxes
Set of Sets: Box of boxes

Think of a set (of elements from some "ground set") as a box containing the elements.
Set of Sets: Box of boxes

Think of a set (of elements from some “ground set”) as a box containing the elements 3, 4, 2.
Set of Sets: Box of boxes

Think of a set (of elements from some “ground set”) as a box containing the elements.

Then a set of sets is a box with boxes inside it (each box containing some elements).
Set of Sets: Box of boxes

Think of a set (of elements from some “ground set”) as a box containing the elements.

Then a set of sets is a box with boxes inside it (each box containing some elements).
Set of Sets: Box of boxes

Think of a set (of elements from some “ground set”) as a box containing the elements.

Then a set of sets is a box with boxes inside it (each box containing some elements).

Not the same as taking the union.
Set of Sets: Box of boxes

Think of a set (of elements from some “ground set”) as a box containing the elements.

Then a set of sets is a box with boxes inside it (each box containing some elements).

- Not the same as taking the union.
- No two boxes inside can have all same elements, but they may contain shared elements.
Set of Sets: Box of boxes

Think of a set (of elements from some “ground set”) as a box containing the elements

Then a set of sets is a box with boxes inside it (each box containing some elements)

- Not the same as taking the union
- No two boxes inside can have all the same elements, but they may contain shared elements
- Can have the empty-set (one empty box)
Set of Sets: An Example
Set of Sets: An Example

Consider a set of 5-bit strings \{ 00110, 11011, 11111 \}
Set of Sets: An Example

Consider a set of 5-bit strings \{00110, 11011, 11111\}

We can represent each bit string by a subset of \{1,2,3,4,5\} indicating in which positions it has a 1
Set of Sets: An Example

Consider a set of 5-bit strings \{ 00110, 11011, 11111 \}

We can represent each bit string by a subset of \{1,2,3,4,5\} indicating in which positions it has a 1

00110 \rightarrow \{3,4\}
11011 \rightarrow \{1,2,4,5\}
11111 \rightarrow \{1,2,3,4,5\}
Set of Sets: An Example

Consider a set of 5-bit strings \{ 00110, 11011, 11111 \}

We can represent each bit string by a subset of \{1,2,3,4,5\} indicating in which positions it has a 1

\begin{align*}
00110 & \rightarrow \{3,4\} \\
11011 & \rightarrow \{1,2,4,5\} \\
11111 & \rightarrow \{1,2,3,4,5\}
\end{align*}

So the original set could be represented as a set of sets:
\{ \{3,4\}, \{1,2,4,5\}, \{1,2,3,4,5\} \}
Set of Sets: An Example
Set of Sets: An Example

We already saw an example earlier
Set of Sets: An Example

- We already saw an example earlier.
- For a graph $G=(V,E)$, the edge-set $E$ is a set of sets (over the ground set $V$).
Set of Sets: An Example

- We already saw an example earlier.
- For a graph $G=(V,E)$, the edge-set $E$ is a set of sets (over the ground set $V$).
  - e.g., in $C_4$, $E = \{ \{0,1\}, \{1,2\}, \{2,3\}, \{3,0\} \}$
Set of Sets: An Example

- We already saw an example earlier.
- For a graph $G=(V,E)$, the edge-set $E$ is a set of sets (over the ground set $V$).
  - e.g., in $C_4$, $E = \{ \{0,1\}, \{1,2\}, \{2,3\}, \{3,0\} \}$
- In the rest of this lecture (and in the textbook): use $A$, $B$, $C$ etc. to denote sets of sets.
Set of Sets: An Example

We already saw an example earlier.

For a graph $G=(V,E)$, the edge-set $E$ is a set of sets (over the ground set $V$).

- e.g., in $C_4$, $E = \{ \{0,1\}, \{1,2\}, \{2,3\}, \{3,0\} \}$

In the rest of this lecture (and in the textbook), use $A$, $B$, $C$ etc. to denote sets of sets.

- e.g., $E = \{ \{0,1\}, \{1,2\}, \{2,3\}, \{3,0\} \}$
Power Set
Power Set

Given a ground-set $A$, its power-set $P(A)$ is defined as

$P(A) = \{ S \mid S \subseteq A \}$
Power Set

Given a ground-set $A$, its power-set $\mathcal{P}(A)$ is defined as
$$\mathcal{P}(A) = \{ S \mid S \subseteq A \}$$

e.g. $A = \{1,2,3\}$
$\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\} \}$
Power Set

Given a ground-set $A$, its power-set $\mathcal{P}(A)$ is defined as

$$\mathcal{P}(A) = \{ S \mid S \subseteq A \}$$

e.g. $A = \{1,2,3\}$

$$\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\} \}$$

If $A$ is finite, $|\mathcal{P}(A)| = 2^{|A|}$
Power Set

Given a ground-set $A$, its power-set $\mathcal{P}(A)$ is defined as

$$\mathcal{P}(A) = \{ S \mid S \subseteq A \}$$

e.g. $A = \{1,2,3\}$

$$\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\} \}$$

If $A$ is finite, $|\mathcal{P}(A)| = 2^{|A|}$

A subset $S$ of $A$ can be formed by taking each element in $A$ and including it in $S$ or not including it. $2^{|A|}$ ways to do this.
Given a ground-set $A$, its power-set $\mathcal{P}(A)$ is defined as

$$\mathcal{P}(A) = \{ S \mid S \subseteq A \}$$

e.g. $A = \{1,2,3\}$

$$\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\} \}$$

If $A$ is finite, $|\mathcal{P}(A)| = 2^{|A|}$

A subset $S$ of $A$ can be formed by taking each element in $A$ and including it in $S$ or not including it. $2^{|A|}$ ways to do this.

If $A$ is infinite? Later.
**Power Set**

- Given a ground-set $A$, its power-set $P(A)$ is defined as
  
  $P(A) = \{ \; S \mid S \subseteq A \; \}$

- e.g. $A = \{1,2,3\}$
  
  $P(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\} \}$

- If $A$ is finite, $|P(A)| = 2^{|A|}$

  A subset $S$ of $A$ can be formed by taking each element in $A$ and including it in $S$ or not including it. $2^{|A|}$ ways to do this.

- If $A$ is infinite? Later.

- Power-set of a ground-set is the universe for all the sets of sets (with that ground-set)
Power Set

Given a ground-set A, its power-set $\mathcal{P}(A)$ is defined as

$$\mathcal{P}(A) = \{ S \mid S \subseteq A \}$$

e.g. $A = \{1,2,3\}$

$$\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\} \}$$

If A is finite, $|\mathcal{P}(A)| = 2^{|A|}$

A subset S of A can be formed by taking each element in A and including it in S or not including it. $2^{|A|}$ ways to do this.

If A is infinite? Later.

Power-set of a ground-set is the universe for all the sets of sets (with that ground-set)

i.e., if $\mathcal{C}$ is a set of sets with ground-set A, $\mathcal{C} \subseteq \mathcal{P}(A)$