Probabilistic Techniques

Targets of the lecture:

- Show how the probability theory can be used for finding a solution to various problems in combinatorics, theoretical computer science, combinatorial geometry, etc...
- Overview basic notions in the probability theory. (But this lecture is not a replacement for the standard course in probability.)
- Mostly, we will focus to discrete probability. Occasionally, we will touch the continuous case.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Definition

The Ramsey number $R(k)$ is the least integer N with which is the theorem above valid.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Definition

The Ramsey number $R(k)$ is the least integer N with which is the theorem above valid.

- Combinatorics classes: $R(k) < 2^{2k}$.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Definition

The Ramsey number $R(k)$ is the least integer N with which is the theorem above valid.

- Combinatorics classes: $R(k) < 2^{2k}$.
- Probabilistic technique $R(k) > 2^{k/2}$.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Definition

The Ramsey number $R(k)$ is the least integer N with which is the theorem above valid.

- Combinatorics classes: $R(k) < 2^{2k}$.
- Probabilistic technique $R(k) > 2^{k/2}$.
  - Find G on $\lfloor 2^{k/2} \rfloor$ vertices without clique or independent set on k vertices.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Definition

The Ramsey number $R(k)$ is the least integer N with which is the theorem above valid.

- Combinatorics classes: $R(k) < 2^{2k}$.
- Probabilistic technique $R(k) > 2^{k/2}$.
  - Find G on $\lfloor 2^{k/2} \rfloor$ vertices without clique or independent set on k vertices.
  - Put each edge into G randomly with probability $1/2$ independently of other edges.

Examples of probabilistic techniques: Ramsey theory

Theorem (Ramsey theorem for graphs and 2 colors)

For every integer k there is an integer N such that every graph on at least N vertices contains either a clique on k vertices or an independent set on k vertices.

Definition

The Ramsey number $R(k)$ is the least integer N with which is the theorem above valid.

- Combinatorics classes: $R(k) < 2^{2k}$.
- Probabilistic technique $R(k) > 2^{k/2}$.
  - Find G on $\lfloor 2^{k/2} \rfloor$ vertices without clique or independent set on k vertices.
  - Put each edge into G randomly with probability $1/2$ independently of other edges.
  - Compute that there is a positive probability that G contains neither a clique nor an independent set on k vertices.

Examples: Graphs with high girth and chromatic number

- Can a graph without triangles have an arbitrary large chromatic number?

Examples: Graphs with high girth and chromatic number

- Can a graph without triangles have an arbitrary large chromatic number?
- YES!

Theorem (Erdős)

For every two integers k and ℓ there exists a graph G with chromatic number at least k and without cycles of size less than ℓ.

Examples: Graphs with high girth and chromatic number

- Can a graph without triangles have an arbitrary large chromatic number?
- YES!

Theorem (Erdős)

For every two integers k and ℓ there exists a graph G with chromatic number at least k and without cycles of size less than ℓ.

- Construct a graph G randomly with each edge in G with probability suitably chosen p.

Examples: Graphs with high girth and chromatic number

- Can a graph without triangles have an arbitrary large chromatic number?
- YES!

Theorem (Erdős)

For every two integers k and ℓ there exists a graph G with chromatic number at least k and without cycles of size less than ℓ.

- Construct a graph G randomly with each edge in G with probability suitably chosen p.
- With high probability G has chromatic number at least k and no cycles of size less than ℓ.

Examples: Graphs with high girth and chromatic number

- Can a graph without triangles have an arbitrary large chromatic number?
- YES!

Theorem (Erdős)

For every two integers k and ℓ there exists a graph G with chromatic number at least k and without cycles of size less than ℓ.

- Construct a graph G randomly with each edge in G with probability suitably chosen p.
- With high probability G has chromatic number at least k and ~~no cycles of size less than ℓ.~~

Examples: Graphs with high girth and chromatic number

- Can a graph without triangles have an arbitrary large chromatic number?
- YES!

Theorem (Erdős)

For every two integers k and ℓ there exists a graph G with chromatic number at least k and without cycles of size less than ℓ.

- Construct a graph G randomly with each edge in G with probability suitably chosen p.
- With high probability G has chromatic number at least k and ~~no cycles of size less than ℓ.~~
- With high probability short cycles can be removed from G while keeping high chromatic number.

Probability space

Definition

A probability space (pravděpodobnostní prostor) is a triple (Ω, Σ, P), where

- Ω is a set,

Probability space

Definition

A probability space (pravděpodobnostní prostor) is a triple (Ω, Σ, P), where

- Ω is a set,
- $\Sigma \subseteq 2^{\Omega}$ is a σ-algebra on Ω:
  - $\emptyset \in \Sigma$;
  - $A \in \Sigma \Rightarrow \Omega \setminus A \in \Sigma$; and
  - if $A_i \in \Sigma$ for $i \in \mathbb{N}$, then $\bigcup_{i=1}^{\infty} A_i \in \Sigma$

Probability space

Definition

A probability space (pravděpodobnostní prostor) is a triple (Ω, Σ, P), where

- Ω is a set,
- $\Sigma \subseteq 2^\Omega$ is a σ-algebra on Ω:
  - $\emptyset \in \Sigma$;
  - $A \in \Sigma \Rightarrow \Omega \setminus A \in \Sigma$; and
  - if $A_i \in \Sigma$ for $i \in \mathbb{N}$, then $\bigcup_{i=1}^{\infty} A_i \in \Sigma$
- and $P \colon \Sigma \to [0, 1]$ is a probability measure:
  - $P[\emptyset] = 0$;
  - $P[\Omega] = 1$; and
  - $P[\bigcup_{i=1}^{\infty} A_i] = \sum_{i=1}^{\infty} P[A_i]$ for pairwise disjoint sets $A_i \in \Sigma$).

Probability space

Definition

A probability space (pravděpodobnostní prostor) is a triple (Ω, Σ, P), where

- Ω is a set,
- $\Sigma \subseteq 2^\Omega$ is a σ-algebra on Ω:
  - $\emptyset \in \Sigma$;
  - $A \in \Sigma \Rightarrow \Omega \setminus A \in \Sigma$; and
  - if $A_i \in \Sigma$ for $i \in \mathbb{N}$, then $\bigcup_{i=1}^{\infty} A_i \in \Sigma$
- and $P \colon \Sigma \to [0, 1]$ is a probability measure:
  - $P[\emptyset] = 0$;
  - $P[\Omega] = 1$; and
  - $P[\bigcup_{i=1}^{\infty} A_i] = \sum_{i=1}^{\infty} P[A_i]$ for pairwise disjoint sets $A_i \in \Sigma$).

Elements of Σ are called events (jevy). Elements of Ω are elementary events (elementární jevy). Given an event $A \in \Sigma$, $P[A]$ is the probability of A (pravděpodobnost jevu A).

Examples—Finite probability space

Example (Finite probability space)

- Ω finite, $\Sigma = 2^{\Omega}$

Examples—Finite probability space

Example (Finite probability space)

- Ω finite, $\Sigma = 2^{\Omega}$
- The probability $P\colon \Sigma \to [0,1]$ is uniquely determined by a function $p\colon \Omega \to [0,1]$ such that $\sum_{\omega\in\Omega} p(\omega) = 1$. Then $P[A] = \sum_{\omega\in A} p(\omega)$.

Examples—Finite probability space

Example (Finite probability space)

- Ω finite, $\Sigma = 2^{\Omega}$
- The probability $P\colon \Sigma \to [0,1]$ is uniquely determined by a function $p\colon \Omega \to [0,1]$ such that $\sum_{\omega\in\Omega} p(\omega) = 1$. Then $P[A] = \sum_{\omega\in A} p(\omega)$.

Example (Finite probability space with uniform distribution:)

- $p(\omega) = 1/|\Omega|$;
- $P[A] = |A|/|\Omega|$.

Examples—Finite probability space

Example (Finite probability space)

- Ω finite, $\Sigma = 2^{\Omega}$
- The probability $P\colon \Sigma \to [0,1]$ is uniquely determined by a function $p\colon \Omega \to [0,1]$ such that $\sum_{\omega\in\Omega} p(\omega) = 1$. Then $P[A] = \sum_{\omega\in A} p(\omega)$.

Example (Finite probability space with uniform distribution:)

- $p(\omega) = 1/|\Omega|$;
- $P[A] = |A|/|\Omega|$.

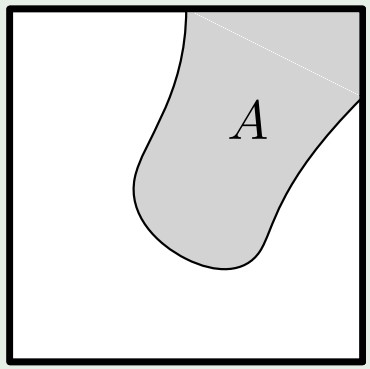
Example (Random graph)

- $G(n,p)$ is finite probability space of random graphs on n vertices with edge probability p;
- Elementary events: Graphs on fixed set of n vertices;
- Prob. of a graph G with m edges $p(G) = p^m(1-p)^{\binom{n}{2}-m}$.

Example of a continuous probability space

Example (Random point in a square)

- $\Omega = [0,1]^2$;
- $\Sigma =$ Lebesgue measurable subsets of $[0,1]^2$;
- $P[A] = \lambda(A)$, the Lebesgue measure of A (area of A).



The union bound

Lemma (Union bound)

Let $A_1, \ldots, A_n$ be events. Then $P[\bigcup_{i=1}^{n} A_i] \leq \sum_{i=1}^{n} P[A_i]$.

The union bound

Lemma (Union bound)

Let $A_1, \ldots, A_n$ be events. Then $P[\bigcup_{i=1}^{n} A_i] \leq \sum_{i=1}^{n} P[A_i]$.

Proof.

- Let $B_i = A_i \setminus (A_1 \cup \cdots \cup A_{i-1})$.

The union bound

Lemma (Union bound)

Let $A_1, \ldots, A_n$ be events. Then $P[\bigcup_{i=1}^n A_i] \leq \sum_{i=1}^n P[A_i]$.

Proof.

- Let $B_i = A_i \setminus (A_1 \cup \cdots \cup A_{i-1})$.
- Then $\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n B_i$ while B_i are pairwise disjoint.

The union bound

Lemma (Union bound)

Let $A_1, \ldots, A_n$ be events. Then $P[\bigcup_{i=1}^n A_i] \leq \sum_{i=1}^n P[A_i]$.

Proof.

- Let $B_i = A_i \setminus (A_1 \cup \cdots \cup A_{i-1})$.
- Then $\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n B_i$ while B_i are pairwise disjoint.
- Consequently

$$P[\bigcup_{i=1}^{n} A_i] = P[\bigcup_{i=1}^{n} B_i] = \sum_{i=1}^{n} P[B_i] \leq \sum_{i=1}^{n} P[A_i].$$

The union bound

Lemma (Union bound)

Let $A_1, \ldots, A_n$ be events. Then $P[\bigcup_{i=1}^n A_i] \leq \sum_{i=1}^n P[A_i]$.

Proof.

- Let $B_i = A_i \setminus (A_1 \cup \cdots \cup A_{i-1})$.
- Then $\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n B_i$ while B_i are pairwise disjoint.
- Consequently

$$P[\bigcup_{i=1}^{n} A_i] = P[\bigcup_{i=1}^{n} B_i] = \sum_{i=1}^{n} P[B_i] \leq \sum_{i=1}^{n} P[A_i].$$

- For the last step $B \subseteq A \Rightarrow P[B] \leq P[A]$ because $P[A] = P[B \cup (A \setminus B)] = P[B] + P[A \setminus B] \geq P[B]$.

Bounds for factorial

- Easy bounds:

$$\left(\frac{n}{2}\right)^{n/2} \leq n! \leq n^n.$$

Bounds for factorial

- Easy bounds:

$$\left(\frac{n}{2}\right)^{n/2} \leq n! \leq n^n.$$

- Improved bounds:

$$\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$$

Bounds for factorial

- Easy bounds:

$$\left(\frac{n}{2}\right)^{n/2} \leq n! \leq n^n.$$

- Improved bounds:

$$\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$$

- Limit behaviour (Stirling formula)

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \text{ i.e. } \lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1.$$

Bounds for binomial coefficients

- Easy bounds:

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq n^k.$$

Bounds for binomial coefficients

- Easy bounds:

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq n^k.$$

- Improved upper bound:

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Bounds for binomial coefficients

- Easy bounds:

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq n^k.$$

- Improved upper bound:

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

- Even better for the middle binomial coefficient:

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}.$$

A very useful inequality

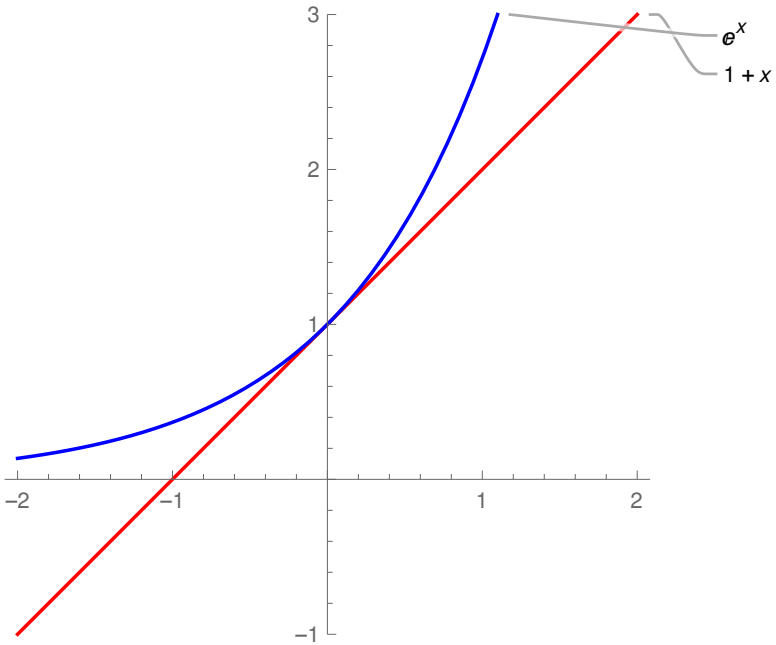
- For every x real we get $1 + x \leq e^x$.

A very useful inequality

- For every x real we get $1 + x \leq e^x$.
- Often used as $(1 - p)^m \leq e^{-mp}$. (On the other hand $1 - p \geq e^{-2p}$ for $p \in [0, 1/2]$.)

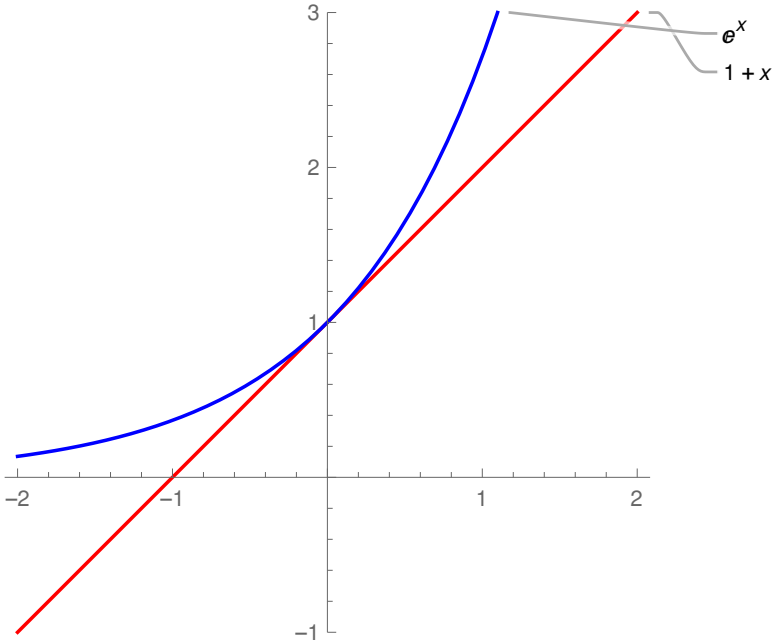
A very useful inequality

- For every x real we get $1 + x \leq e^x$.
- Often used as $(1 - p)^m \leq e^{-mp}$. (On the other hand $1 - p \geq e^{-2p}$ for $p \in [0, 1/2]$.)



A very useful inequality

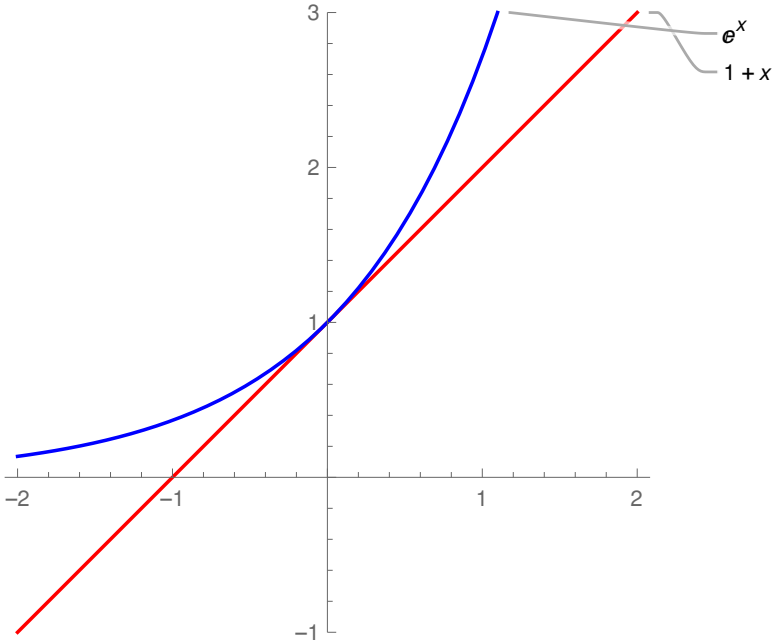
- For every x real we get $1 + x \leq e^x$.
- Often used as $(1 - p)^m \leq e^{-mp}$. (On the other hand $1 - p \geq e^{-2p}$ for $p \in [0, 1/2]$.)



$$1+x \leq e^x \Leftrightarrow e^x-1-x \geq 0$$

A very useful inequality

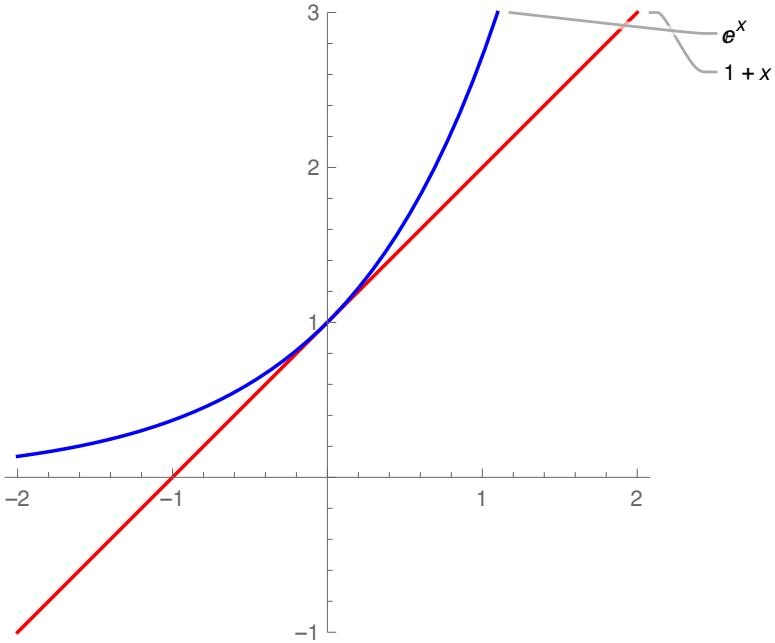
- For every x real we get $1 + x \leq e^x$.
- Often used as $(1 - p)^m \leq e^{-mp}$. (On the other hand $1 - p \geq e^{-2p}$ for $p \in [0, 1/2]$.)



$$1+x \leq e^x \Leftrightarrow e^x-1-x \geq 0$$
$$f(x) = e^x - 1 - x$$

A very useful inequality

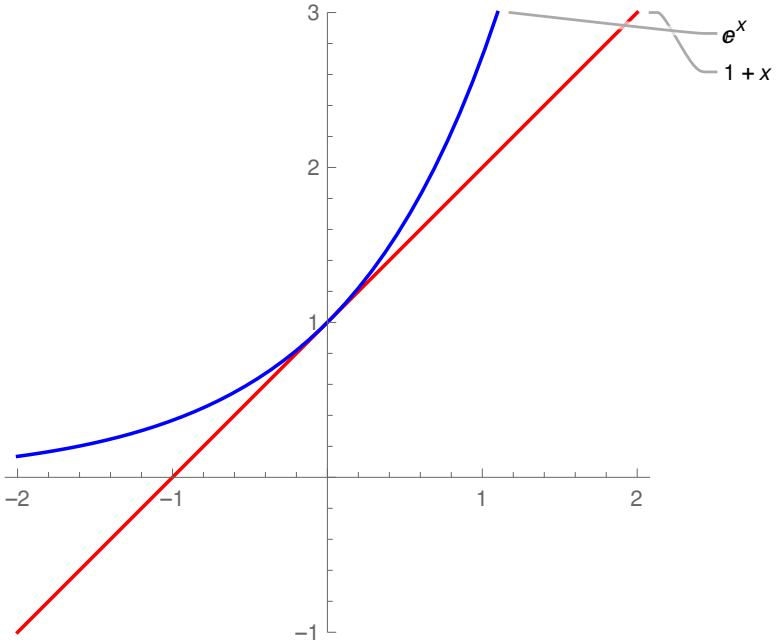
- For every x real we get $1 + x \leq e^x$.
- Often used as $(1 - p)^m \leq e^{-mp}$. (On the other hand $1 - p \geq e^{-2p}$ for $p \in [0, 1/2]$.)



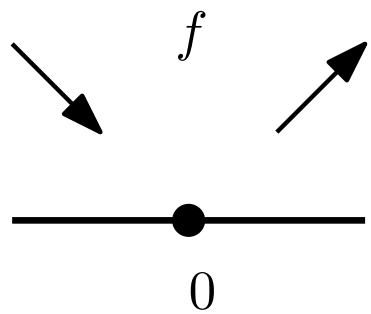
$$1+x \leq e^x \Leftrightarrow e^x-1-x \geq 0$$
$$f(x) = e^x - 1 - x$$
$$f(0) = 0,\ f'(x) = e^x - 1$$

A very useful inequality

- For every x real we get $1 + x \leq e^x$.
- Often used as $(1-p)^m \leq e^{-mp}$. (On the other hand $1 - p \geq e^{-2p}$ for $p \in [0, 1/2]$.)



$$1+x \leq e^x \Leftrightarrow e^x - 1 - x \geq 0$$
$$f(x) = e^x - 1 - x$$
$$f(0) = 0,\ f'(x) = e^x - 1$$



Ramsey numbers revisited

- Recall that $R(k)$ is the least integer such that every graph with $R(k)$ vertices contains either a clique of size k or an independent set of size k.

Ramsey numbers revisited

- Recall that $R(k)$ is the least integer such that every graph with $R(k)$ vertices contains either a clique of size k or an independent set of size k.

Theorem

For every $k \geq 3$ we get $R(k) > 2^{k/2}$.

Ramsey numbers revisited

- Recall that $R(k)$ is the least integer such that every graph with $R(k)$ vertices contains either a clique of size k or an independent set of size k.

Theorem

For every $k \geq 3$ we get $R(k) > 2^{k/2}$.

Proof.

- Take the random graph $G(n, 1/2)$.

Ramsey numbers revisited

- Recall that $R(k)$ is the least integer such that every graph with $R(k)$ vertices contains either a clique of size k or an independent set of size k.

Theorem

For every $k \geq 3$ we get $R(k) > 2^{k/2}$.

Proof.

- Take the random graph $G(n, 1/2)$.
- For a fixed subset of k vertices the probability that it forms a clique or independent set is $2 \cdot 2^{-\binom{k}{2}}$.
- By the union bound: Probability that $G(n, 1/2)$ contains a clique or an independent set on k vertices is at most $\binom{n}{k} \cdot 2 \cdot 2^{-\binom{k}{2}}$.

Ramsey numbers revisited

Proof–continued.

- By the union bound: Probability that $G(n, 1/2)$ contains a clique or an independent set on k vertices is at most $\binom{n}{k} \cdot 2 \cdot 2^{-\binom{k}{2}}$.

Ramsey numbers revisited

Proof–continued.

- By the union bound: Probability that $G(n, 1/2)$ contains a clique or an independent set on k vertices is at most $\binom{n}{k} \cdot 2 \cdot 2^{-\binom{k}{2}}$.
- We want to show that this probability is less than 1 if $n \leq 2^{k/2}$:

Ramsey numbers revisited

Proof–continued.

- By the union bound: Probability that $G(n, 1/2)$ contains a clique or an independent set on k vertices is at most $\binom{n}{k} \cdot 2 \cdot 2^{-\binom{k}{2}}$.
- We want to show that this probability is less than 1 if $n \leq 2^{k/2}$:

$$\binom{n}{k} \cdot 2 \cdot 2^{-\binom{k}{2}} \leq \frac{n^k}{k!} 2^{-(\frac{k(k-1)}{2}-1)} \leq \frac{2^{k \cdot k/2}}{k!} 2^{-(\frac{k(k-1)}{2}-1)} =$$

$$= \frac{2^{k/2+1}}{k!} < 1.$$

Independent events

Definition (Independent events)

Two events A and B are independent (nezávislé) if $P[A \cap B] = P[A]P[B]$.

Independent events

Definition (Independent events)

Two events A and B are independent (nezávislé) if $P[A \cap B] = P[A]P[B]$. Events $A_1, \ldots, A_n$ are independent if $\forall I \subseteq [n]$ we have $P\left[\bigcap_{i \in I} A_i\right] = \prod_{i \in I} P[A_i]$.

Independent events

Definition (Independent events)

Two events A and B are independent (nezávislé) if $P[A \cap B] = P[A]P[B]$. Events $A_1, \ldots, A_n$ are independent if $\forall I \subseteq [n]$ we have $P\left[\bigcap_{i \in I} A_i\right] = \prod_{i \in I} P[A_i]$.

Definition (Conditional probability)

Let A, B be events such that $P[B] > 0$. Then the conditional probability (podmíněná pravděpodobnost) of A, given that B occurs, is defined as $P[A|B] := P[A \cap B]/P[B]$.

Independent events

Definition (Independent events)

Two events A and B are independent (nezávislé) if $P[A \cap B] = P[A]P[B]$. Events $A_1, \ldots, A_n$ are independent if $\forall I \subseteq [n]$ we have $P\left[\bigcap_{i \in I} A_i\right] = \prod_{i \in I} P[A_i]$.

Definition (Conditional probability)

Let A, B be events such that $P[B] > 0$. Then the conditional probability (podmíněná pravděpodobnost) of A, given that B occurs, is defined as $P[A|B] := P[A \cap B]/P[B]$.

- If A and B are independent, then $P[A|B] = P[A]$.