One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.
- clause (klauzule): Formula of a form $(\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k)$ where ℓ_i are literals.

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.
- clause (klauzule): Formula of a form $(\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k)$ where ℓ_i are literals.
- CNF-fomlula: Formula of a form $c_1 \wedge c_2 \wedge \cdots \wedge c_m$ where c_i are clauses. (CNF stands for conjunctive normal form.)

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.
- clause (klauzule): Formula of a form $(\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k)$ where ℓ_i are literals.
- CNF-fomlula: Formula of a form $c_1 \wedge c_2 \wedge \cdots \wedge c_m$ where c_i are clauses. (CNF stands for conjunctive normal form.)
- Example: $(\neg x_1) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_3 \vee \neg x_4)$.

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.
- clause (klauzule): Formula of a form $(\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k)$ where ℓ_i are literals.
- CNF-fomlula: Formula of a form $c_1 \wedge c_2 \wedge \cdots \wedge c_m$ where c_i are clauses. (CNF stands for conjunctive normal form.)
- Example: $(\neg x_1) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_3 \vee \neg x_4)$.

Algorithmic Question (SAT-problem)

- INPUT: A CNF-formula Φ.
- QUESTION: Is Φ satisfiable? That is, is there an assignment of the variables in which is Φ satisfied?

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.
- clause (klauzule): Formula of a form $(\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k)$ where ℓ_i are literals.
- CNF-fomlula: Formula of a form $c_1 \wedge c_2 \wedge \cdots \wedge c_m$ where c_i are clauses. (CNF stands for conjunctive normal form.)
- Example: $(\neg x_1) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_3 \vee \neg x_4)$.

Algorithmic Question (SAT-problem)

- INPUT: A CNF-formula Φ.
- QUESTION: Is Φ satisfiable? That is, is there an assignment of the variables in which is Φ satisfied?

- The formula above is satisfiable, for example, by setting $x_1 =$ FALSE, $x_2 =$ TRUE, $x_3 =$ TRUE, $x_4 =$ FALSE.

One more application of the union bound: Satisfiability

- $x_1, \ldots, x_n$ Boolean variables (TRUE or FALSE)
- literal (literál): Variable or its negation x_i, $\neg x_i$.
- clause (klauzule): Formula of a form $(\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k)$ where ℓ_i are literals.
- CNF-fomlula: Formula of a form $c_1 \wedge c_2 \wedge \cdots \wedge c_m$ where c_i are clauses. (CNF stands for conjunctive normal form.)
- Example: $(\neg x_1) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_3 \vee \neg x_4)$.

Algorithmic Question (SAT-problem)

- INPUT: A CNF-formula Φ.
- QUESTION: Is Φ satisfiable? That is, is there an assignment of the variables in which is Φ satisfied?

- The formula above is satisfiable, for example, by setting $x_1 =$ FALSE, $x_2 =$ TRUE, $x_3 =$ TRUE, $x_4 =$ FALSE.
- NP-hard problem.

Satisfiability, continued

Proposition

Let Φ be a CNF-formula such that each clause has (exactly) k literals (no variable appears in a same clause twice or more times) and the number of the clauses is less than 2^k. Then Φ is satisfiable.

Proof.

- Consider a random assignment of the variables so that each variable is assigned TRUE with prob. $1/2$ and FALSE with prob. $1/2$, independently of other variables.

Satisfiability, continued

Proposition

Let Φ be a CNF-formula such that each clause has (exactly) k literals (no variable appears in a same clause twice or more times) and the number of the clauses is less than 2^k. Then Φ is satisfiable.

Proof.

- Consider a random assignment of the variables so that each variable is assigned TRUE with prob. $1/2$ and FALSE with prob. $1/2$, independently of other variables.
- Probability that any given clause is not satisfied is $1/2^k$.

Satisfiability, continued

Proposition

Let Φ be a CNF-formula such that each clause has (exactly) k literals (no variable appears in a same clause twice or more times) and the number of the clauses is less than 2^k. Then Φ is satisfiable.

Proof.

- Consider a random assignment of the variables so that each variable is assigned TRUE with prob. $1/2$ and FALSE with prob. $1/2$, independently of other variables.
- Probability that any given clause is not satisfied is $1/2^k$.
- $(x_1 \vee \neg x_3 \vee x_4)$: $x_1 = \text{FALSE}$, $x_3 = \text{TRUE}$, $x_4 = \text{FALSE}$.

Satisfiability, continued

Proposition

Let Φ be a CNF-formula such that each clause has (exactly) k literals (no variable appears in a same clause twice or more times) and the number of the clauses is less than 2^k. Then Φ is satisfiable.

Proof.

- Consider a random assignment of the variables so that each variable is assigned TRUE with prob. $1/2$ and FALSE with prob. $1/2$, independently of other variables.
- Probability that any given clause is not satisfied is $1/2^k$.
- $(x_1 \vee \neg x_3 \vee x_4)$: $x_1 = \text{FALSE}$, $x_3 = \text{TRUE}$, $x_4 = \text{FALSE}$.
- Union bound: Probability that some clause is not satisfied is $\leq \frac{m}{2^k}$ where m is the number of clauses.

Satisfiability, continued

Proposition

Let Φ be a CNF-formula such that each clause has (exactly) k literals (no variable appears in a same clause twice or more times) and the number of the clauses is less than 2^k. Then Φ is satisfiable.

Proof.

- Consider a random assignment of the variables so that each variable is assigned TRUE with prob. $1/2$ and FALSE with prob. $1/2$, independently of other variables.
- Probability that any given clause is not satisfied is $1/2^k$.
- $(x_1 \vee \neg x_3 \vee x_4)$: $x_1 =$ FALSE, $x_3 =$ TRUE, $x_4 =$ FALSE.
- Union bound: Probability that some clause is not satisfied is $\leq \frac{m}{2^k}$ where m is the number of clauses.
- This is less then 1 as $m < 2^k$, thus a satisfying assignment exists. □

Erdős-Ko-Rado theorem

- A set system $\mathcal{F}$ is intersecting if $\forall A, B \in \mathcal{F} : A \cap B \neq \emptyset$.

Erdős-Ko-Rado theorem

- A set system $\mathcal{F}$ is intersecting if $\forall A, B \in \mathcal{F} : A \cap B \neq \emptyset$.

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

Erdős-Ko-Rado theorem

- A set system $\mathcal{F}$ is intersecting if $\forall A, B \in \mathcal{F} : A \cap B \neq \emptyset$.

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

- The bound is tight: Consider $X = \{1, \ldots, n\}$ and let $\mathcal{F}$ contains all k-element sets which contain 1. Then $\mathcal{F}$ is intersecting and $|\mathcal{F}| = \binom{n-1}{k-1}$.

Erdős-Ko-Rado theorem

- A set system $\mathcal{F}$ is intersecting if $\forall A, B \in \mathcal{F} : A \cap B \neq \emptyset$.

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

- The bound is tight: Consider $X = \{1, \ldots, n\}$ and let $\mathcal{F}$ contains all k-element sets which contain 1. Then $\mathcal{F}$ is intersecting and $|\mathcal{F}| = \binom{n-1}{k-1}$.
- Question to the audience: How big is the largest intersecting family if $n < 2k$?

Lemma for Erdős-Ko-Rado theorem

Lemma

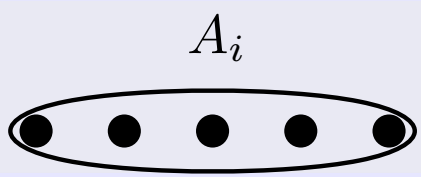
Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Lemma for Erdős-Ko-Rado theorem

Lemma

Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Proof.



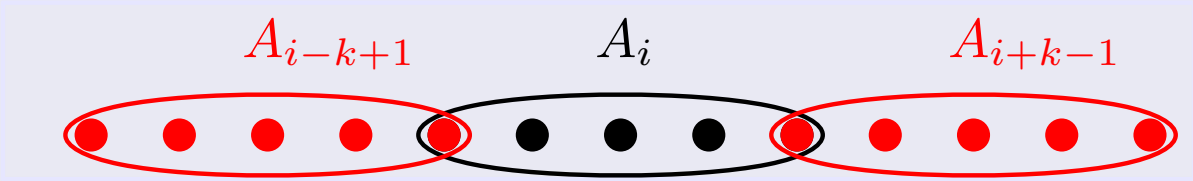
- Assume $A_i \in \mathcal{F}$.

Lemma for Erdős-Ko-Rado theorem

Lemma

Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Proof.



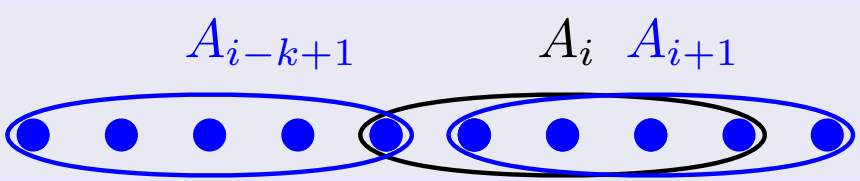
- Assume $A_i \in \mathcal{F}$.
- Then $\mathcal{F}$ may in addition only contain the sets $A_{i-k+1}, \ldots, A_{i-1}, A_{i+1}, \ldots, A_{i+k-1}$. This is $2k-2$ additional sets.

Lemma for Erdős-Ko-Rado theorem

Lemma

Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Proof.



- Assume $A_i \in \mathcal{F}$.
- Then $\mathcal{F}$ may in addition only contain the sets A_{i-k+1}, $\ldots$, A_{i-1}, A_{i+1}, $\ldots$, A_{i+k-1}. This is $2k-2$ additional sets.
- Only one in each pair $\{A_{i-k+1}, A_{i+1}\}$, $\{A_{i-k+2}, A_{i+2}\}$, $\ldots$, $\{A_{i-1}, A_{i+k-1}\}$ is possible.

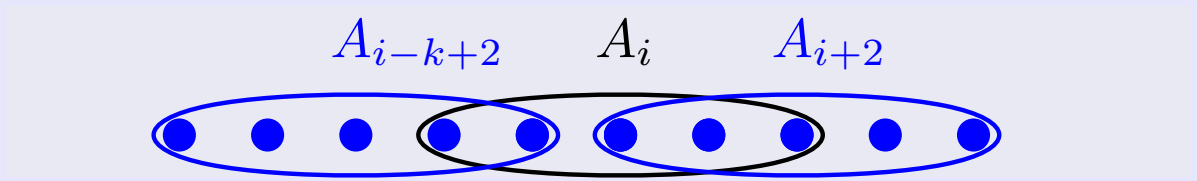
□

Lemma for Erdős-Ko-Rado theorem

Lemma

Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Proof.



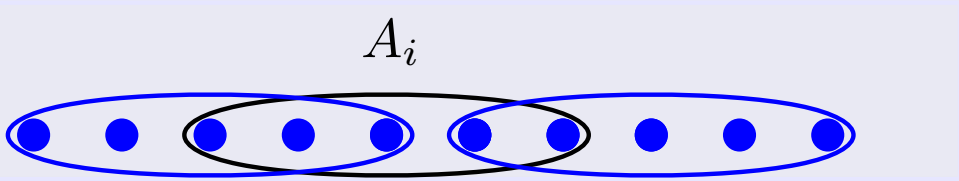
- Assume $A_i \in \mathcal{F}$.
- Then $\mathcal{F}$ may in addition only contain the sets $A_{i-k+1}, \ldots, A_{i-1}, A_{i+1}, \ldots, A_{i+k-1}$. This is $2k-2$ additional sets.
- Only one in each pair $\{A_{i-k+1}, A_{i+1}\}, \{A_{i-k+2}, A_{i+2}\}, \ldots, \{A_{i-1}, A_{i+k-1}\}$ is possible. □

Lemma for Erdős-Ko-Rado theorem

Lemma

Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Proof.



- Assume $A_i \in \mathcal{F}$.
- Then $\mathcal{F}$ may in addition only contain the sets $A_{i-k+1}, \ldots, A_{i-1}, A_{i+1}, \ldots, A_{i+k-1}$. This is $2k-2$ additional sets.
- Only one in each pair $\{A_{i-k+1}, A_{i+1}\}, \{A_{i-k+2}, A_{i+2}\}, \ldots, \{A_{i-1}, A_{i+k-1}\}$ is possible.

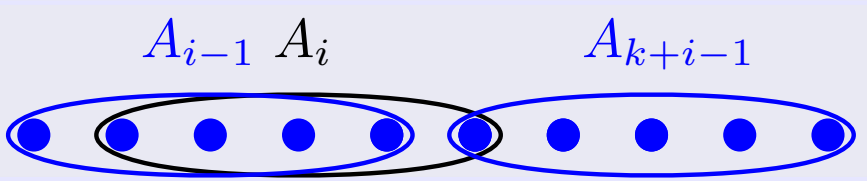
□

Lemma for Erdős-Ko-Rado theorem

Lemma

Let $n \geq 2k$. Let $X := \{0, \ldots, n-1\}$ with addition modulo n and let $A_s = \{s, s+1, \ldots, s+k-1\}$ for $s \in X$. Then for every intersecting family $\mathcal{F} \subseteq \binom{X}{k}$ we get that $\mathcal{F}$ contains at most k sets among the sets A_s.

Proof.



- Assume $A_i \in \mathcal{F}$.
- Then $\mathcal{F}$ may in addition only contain the sets A_{i-k+1}, $\ldots$, A_{i-1}, A_{i+1}, $\ldots$, A_{i+k-1}. This is $2k-2$ additional sets.
- Only one in each pair $\{A_{i-k+1}, A_{i+1}\}$, $\{A_{i-k+2}, A_{i+2}\}$, $\ldots$, $\{A_{i-1}, A_{i+k-1}\}$ is possible.

□

Proof of the Erdős-Ko-Rado theorem

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof of the Erdős-Ko-Rado theorem

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof.

- Without loss of generality: $X = \{0, 1, \ldots, n-1\}$.

Proof of the Erdős-Ko-Rado theorem

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof.

- Without loss of generality: $X = \{0, 1, \ldots, n-1\}$.
- Given a permutation $\sigma \in S_n$, let $\sigma(A_s) := \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$.

Proof of the Erdős-Ko-Rado theorem

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof.

- Without loss of generality: $X = \{0, 1, \ldots, n-1\}$.
- Given a permutation $\sigma \in S_n$, let $\sigma(A_s) := \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$.
- $P[\sigma(A_s) \in \mathcal{F}] \leq \frac{k}{n}$ by the lemma (first we pick σ, then s).

Proof of the Erdős-Ko-Rado theorem

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof.

- Without loss of generality: $X = \{0, 1, \ldots, n-1\}$.
- Given a permutation $\sigma \in S_n$, let $\sigma(A_s) := \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$.
- $P[\sigma(A_s) \in \mathcal{F}] \leq \frac{k}{n}$ by the lemma (first we pick σ, then s).
- $\sigma(A_s)$ is a random k-subset of X (first pick s, then σ). This gives $P[\sigma(A_s) \in \mathcal{F}] = |\mathcal{F}|/\binom{n}{k}$.

Proof of the Erdős-Ko-Rado theorem

Theorem (Erdős-Ko-Rado)

Let X be an n-element set, k be such that $n \geq 2k$ and $\mathcal{F}$ be and intersecting set system consisting of (some) k-element subsets of X. Then $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Proof.

- Without loss of generality: $X = \{0, 1, \ldots, n-1\}$.
- Given a permutation $\sigma \in S_n$, let $\sigma(A_s) := \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$.
- $P[\sigma(A_s) \in \mathcal{F}] \leq \frac{k}{n}$ by the lemma (first we pick σ, then s).
- $\sigma(A_s)$ is a random k-subset of X (first pick s, then σ). This gives $P[\sigma(A_s) \in \mathcal{F}] = |\mathcal{F}|/\binom{n}{k}$.
- Altogether:

$$|\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \frac{k}{n}\frac{n!}{k!(n-k)!} = \binom{n-1}{k-1}. \quad \square$$

Erdös-Ko-Rado, additional explanation

- This slide explains in more detail the following item from the previous slide.
  - $P[\sigma(A_s) \in \mathcal{F}] \leq \frac{k}{n}$ by the lemma (first we pick σ, then s)
- Note that the formula $P[\sigma(A_s) \in \mathcal{F}]$ regards the case where both σ and s are taken uniformly in random.
- First consider a fixed σ and let p_σ be the probability that $\sigma(A_s)$ belongs to $\mathcal{F}$ for $s \in \{0, \ldots, n-1\}$ chosen uniformly at random.
- By lemma, we have $p_\sigma \leq \frac{k}{n}$ because at most k sets among the sets A_s may be intersecting which is equivalent with saying that at most k sets among $\sigma(A_s)$ may be intersecting.
- Now we get $P[\sigma(A_s) \in \mathcal{F}] = \sum_\sigma \frac{1}{n!} p_\sigma$ because we have probability $\frac{1}{n!}$ to pick an individual σ and we have to consider all possible σ. (This is in principle the conditional probability that I mentioned during the lecture but for somebody it maybe easier to see it directly.)

Random variables and the expectation

Definition

Random variable (náhodná veličina) on probability space (Ω, Σ, P) is a P-measurable function $X : \Omega \to R$. (P-measurable: $\forall a \in \mathbb{R}$: $\{\omega \in \Omega : X(\omega) \leq a\} \in \Sigma$).

Random variables and the expectation

Definition

Random variable (náhodná veličina) on probability space (Ω, Σ, P) is a P-measurable function $X : \Omega \to R$. (P-measurable: $\forall a \in \mathbb{R}$: $\{\omega \in \Omega : X(\omega) \leq a\} \in \Sigma$).

- $P[X \leq a]$ is well defined where $P[X \leq a]$ is a standard abbreviation for $P[\{\omega \in \Omega : X(\omega) \leq a\}]$.

Random variables and the expectation

Definition

Random variable (náhodná veličina) on probability space (Ω, Σ, P) is a P-measurable function $X : \Omega \to R$. (P-measurable: $\forall a \in \mathbb{R}$: $\{\omega \in \Omega : X(\omega) \leq a\} \in \Sigma$).

- $P[X \leq a]$ is well defined where $P[X \leq a]$ is a standard abbreviation for $P[\{\omega \in \Omega : X(\omega) \leq a\}]$.

Definition

The expectation (střední hodnota) of a random variable X is defined as

$$E[X] := \int_{\Omega} X(\omega) \mathrm{d}P(\omega).$$

Random variables and the expectation

Definition

Random variable (náhodná veličina) on probability space (Ω, Σ, P) is a P-measurable function $X : \Omega \to R$. (P-measurable: $\forall a \in \mathbb{R}$: $\{\omega \in \Omega : X(\omega) \leq a\} \in \Sigma$).

- $P[X \leq a]$ is well defined where $P[X \leq a]$ is a standard abbreviation for $P[\{\omega \in \Omega : X(\omega) \leq a\}]$.

Definition

The expectation (střední hodnota) of a random variable X is defined as

$$E[X] := \int_{\Omega} X(\omega) \mathrm{d}P(\omega).$$

- Finite probability space: $E[X] = \sum_{\omega \in \Omega} p(\omega) X(\omega)$. Can be also rewritten as $E[X] = \sum_{a \in X(\Omega)} P[X = a] a$.

Linearity of expectation

Lemma (Linearity of expectation)

Let X, Y be random variables and $\alpha, \beta \in \mathbb{R}$. Then $E[\alpha X + \beta Y] = \alpha E[X] + \beta E[Y]$.

Linearity of expectation

Lemma (Linearity of expectation)

Let X, Y be random variables and $\alpha, \beta \in \mathbb{R}$. Then $E[\alpha X + \beta Y] = \alpha E[X] + \beta E[Y]$.

Proof (only for finite prob. spaces).

$$\begin{aligned} E[\alpha X + \beta Y] &= \sum_{\omega \in \Omega} p(\omega)\big(\alpha X(\omega) + \beta Y(\omega)\big) \\ &= \alpha \sum_{\omega \in \Omega} p(\omega) X(\omega) + \beta \sum_{\omega \in \Omega} p(\omega) Y(\omega) \\ &= \alpha E[X] + \beta E[Y]. \end{aligned}$$

□

Independence of random variables

Definition

Two random variables X and Y are independent (nezávislé), if

$$P[X \in A \wedge Y \in B] = P[X \in A]P[Y \in B]$$

for every two Lebesgue-measurable sets $A, B \subseteq \mathbb{R}$.

Independence of random variables

Definition

Two random variables X and Y are independent (nezávislé), if

$$P[X \in A \wedge Y \in B] = P[X \in A]P[Y \in B]$$

for every two Lebesgue-measurable sets $A, B \subseteq \mathbb{R}$.
Equivalently (without proof)

$$P[X \leq a \wedge Y \leq b] = P[X \leq a]P[Y \leq b]$$

for every $a, b \in \mathbb{R}$.

Independence of random variables

Definition

Two random variables X and Y are independent (nezávislé), if

$$P[X \in A \wedge Y \in B] = P[X \in A]P[Y \in B]$$

for every two Lebesgue-measurable sets $A, B \subseteq \mathbb{R}$.
Equivalently (without proof)

$$P[X \leq a \wedge Y \leq b] = P[X \leq a]P[Y \leq b]$$

for every $a, b \in \mathbb{R}$.

Lemma (Expectation of the product of independent variables)

Let X and Y be independent random variables. Then $E[XY] = E[X]E[Y]$.

Proof of the lemma

Lemma (Expectation of the product of independent variables)

Let X and Y be independent random variables. Then $E[XY] = E[X]E[Y]$.

Proof of the lemma

Lemma (Expectation of the product of independent variables)

Let X and Y be independent random variables. Then $E[XY] = E[X]E[Y]$.

Proof.

$$
\begin{aligned}
E[XY] &= \sum_{c \in XY(\Omega)} cP[XY = c] \\
&= \sum_{\substack{a \in X(\Omega) \\ b \in Y(\Omega)}} abP[X = a \wedge Y = b] \\
&= \sum_{\substack{a \in X(\Omega) \\ b \in Y(\Omega)}} abP[X = a]P[X = b] \\
&= \left(\sum_{a \in X(\Omega)} aP[X = a] \right) \left(\sum_{b \in Y(\Omega)} bP[Y = b] \right) = E[X]E[Y] \square
\end{aligned}
$$

Indicators

Definition

Given an event A, the indicator (indikátor) of A is a random variable defined as

$$I_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

Indicators

Definition

Given an event A, the indicator (indikátor) of A is a random variable defined as

$$I_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

- Important observation: $E[I_A] = P[A]$.

Indicators

Definition

Given an event A, the indicator (indikátor) of A is a random variable defined as

$$I_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

- Important observation: $E[I_A] = P[A]$.

Application: Number of fixed points in a random permutation.

Indicators

Definition

Given an event A, the indicator (indikátor) of A is a random variable defined as

$$I_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

- Important observation: $E[I_A] = P[A]$.

Application: Number of fixed points in a random permutation.

- Given a random permutation σ of $[n]$, let A_j be the event expressing that j is fixes point (that is, $\sigma(j) = j$).

Indicators

Definition

Given an event A, the indicator (indikátor) of A is a random variable defined as

$$I_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

- Important observation: $E[I_A] = P[A]$.

Application: Number of fixed points in a random permutation.

- Given a random permutation σ of $[n]$, let A_j be the event expressing that j is fixes point (that is, $\sigma(j) = j$).
- $E[I_{A_j}] = P[A_j] = \frac{1}{n}$.

Indicators

Definition

Given an event A, the indicator (indikátor) of A is a random variable defined as

$$I_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

- Important observation: $E[I_A] = P[A]$.

Application: Number of fixed points in a random permutation.

- Given a random permutation σ of $[n]$, let A_j be the event expressing that j is fixes point (that is, $\sigma(j) = j$).
- $E[I_{A_j}] = P[A_j] = \frac{1}{n}$.
- Then the expectation of the number of fixed points in a random permutation equals

$$\sum_{j=1}^{n} E[I_{A_j}] = n \cdot \frac{1}{n} = 1.$$