

Egzamin — teoria

Prowadzący: *Stefan Dziembowski, Daniel Malinowski*

MIM UW

1. Podaj nierówność Krafta (zwaną również nierównością McMillana) wraz z dowodem dla kodów prefiksowych (zwanym również kodami bezprefiksowymi).
2. Podaj macierz parzystości i macierz generującą dla kodów Hamminga H_4 .
3. Podaj definicję silnego ekstraktora losowości (ang.: *strong seeded extractor*).

Instrukcja:

1. Część teoretyczna egzaminu trwa 75 minut.
2. W czasie egzaminu nie wolno wychodzić z sali.
3. Nie wolno korzystać z żadnych materiałów pisanych (książki, notatki, itp.)
4. Nie wolno korzystać z żadnych urządzeń elektronicznych (telefony komórkowe, kalkulatory, laptopy, tablety, inteligentne zegarki, Google glass, itp.).

Egzamin — zadania

Prowadzący: *Stefan Dziembowski, Daniel Malinowski*

MIM UW

1. Znajdź kod Huffmana nad alfabetem trzyliterowym $\Sigma = \{0, 1, 2\}$, oraz policz średnią długość kodu dla źródła o rozkładzie prawdopodobieństwa:

$$(0.05, 0.05, 0.08, 0.08, 0.09, 0.1, 0.1, 0.1, 0.1, 0.25).$$

2. Rozważmy kanał Γ_n , w którym alfabet wejściowy Σ_A oraz wyjściowy Σ_B wynoszą $\Sigma_A = \Sigma_B = \{0, 1\}^n$ oraz przesłanie przez kanał symbolu $x = (x_1, x_2, \dots, x_n)$ powoduje zmianę dokładnie jednego bitu, wybranego z jednostajnym prawdopodobieństwem. Formalnie, dla każdego $i = 1, 2, \dots, n$ symbol x przesłany przez kanał Γ_n zamienia się na $(x_1, x_2, \dots, x_{i-1}, x_i \oplus 1, x_{i+1}, \dots, x_n)$ z prawdopodobieństwem $1/n$. Oblicz przepustowość tego kanału.
3. Pokaż, że dla $M = T = Z_p$ i $K = Z_p^2$, gdzie $p > 2$ jest liczbą pierwszą funkcja $f_{a,b}(m) = (m+a)^2 + b \pmod{p}$ jest bezpiecznym jednorazowym kodem uwierzytelniającym (ang. *one-time MAC*) dla zbioru wiadomości M , zbioru kluczy K oraz zbioru etykiet (ang. *tag*) T .
4. Niech A i B będą zmiennymi losowymi, które w ogólności nie muszą być niezależne. Załóżmy, że A przyjmuje wartości ze zbioru skończonego $\mathcal{X}$. Niech U będzie zmienną o rozkładzie jednostajnym na $\mathcal{X}$, niezależną od A, B . Pokaż, że wówczas

$$P(A = B) \leq \Delta((A, B); (U, B)) + 1/|\mathcal{X}|,$$

gdzie Δ oznacza dystans statystyczny rozkładów.

Instrukcja:

1. Część zadaniowa egzaminu trwa 90 minut.
2. W czasie egzaminu nie wolno wychodzić z sali.
3. Wolno korzystać z materiałów pisanych (książki, notatki, itp.).
4. Nie wolno korzystać z żadnych urządzeń elektronicznych (telefony komórkowe, kalkulatory, laptopy, tablety, inteligentne zegarki, Google glass, itp.).