Egzamin z Teorii informacji. Teoria

23 lutego 2019

Dla informacji podajemy uzasadnienia również tam, gdzie nie były wymagane.

1. Wyciągamy kartę z talii, z pewnym rozkładem prawdopodobieństwa. Niech A oznacza jej kolor (czerwony, czarny), B typ (pik, trefl, karo, kier), a C wartość (nominał lub rodzaj figury).

   Odpowiedzi na oba pytania proszę krótko uzasadnić.

   (a) Czy istnieje taki rozkład prawdopodobieństwa i taka kombinacja trzech różnych $X, Y, Z \in \{A, B, C\}$, dla której

   $$I(X;Y|Z) \quad < \quad I(X;Y) \ ?$$

   Tak. Np. rozkład przypisujący niezerowe prawdopodobieństwo 4 kartom, jak następuje:

	♡	♠
As	$\frac{1}{6}$	$\frac{1}{3}$
Dama	$\frac{1}{3}$	$\frac{1}{6}$

   Wtedy, pamiętając, że A jest funkcją B, mamy

   $$I(A;B) = H(A) = 1,$$

   podczas gdy

   $$I(A;B|C) = H(A|C) = \mathcal{H}(\frac{1}{3}) < 1.$$

   (b) Czy istnieje taki rozkład prawdopodobieństwa i takie dwie kombinacje trzech różnych zmiennych, powiedzmy X, Y, Z i X', Y', Z', że $I(X;Y|Z) < I(X;Y)$, podczas gdy $I(X';Y'|Z') \geq I(X';Y')$?
   Nie, bo $I(X;Y) - I(X;Y|Z) = R(X;Y;Z)$, a ta wielkość nie zależy od kolejności X, Y, Z.

2. Przypomnijmy kanał z zadania domowego, który przymował na wejściu ciąg bitów długości n, z jednostajnym prawdopodobieństwem wybierał pozycję i zmieniał jej wartość. Nazwijmy ten kanał Γ_n. Określamy nowy kanał Δ_n, który przymuje na wejściu ciąg bitów długości n, z jednostajnym prawdopodobieństwem wybiera pozycję, po czym z prawodopobieństwem $\frac{1}{2}$ zmienia jej wartość lub pozostawia bez zmian.

   Który z kanałów ma większą przepustowość?

   Uwaga: odpowiedź może zależeć od n.

   Z definicji kanału $p(B = w|A = w) = \frac{1}{2}$ i $p(B = v|A = w) = \frac{1}{2n}$, gdy v różni się od w jednym bitem. A zatem kolumny w macierzy kanału sumują się do 1, z czego wynika, że B ma rozkład jednostajny, gdy taki rozkład ma A. Dla ustalonego w, mamy

   $$H(B|w) = \frac{1}{2}\log 2 + n \cdot \frac{1}{2n}\log 2n = 1 + \frac{1}{2}\log n,$$

skąd $H(B|A) = 1 + \frac{1}{2}\log n$, niezależnie od rozkładu A. Zatem przepustowość jest osiągana dla B o jednostajnym rozkładzie i równa $n - 1 - \frac{1}{2}\log n$. Jak pamiętamy z rozwiązania zadania domowego, przepustowość kanału Γ_n wynosiła $n - logn$.

Odpowiedź wynika więc z porównania tych dwóch funkcji.

Dla $n \leq 3$, $C(\Delta_n) < C(\Gamma_n)$,

dla $n = 4$, $C(\Delta_n) = C(\Gamma_n)$,

dla $n \geq 5$, $C(\Delta_n) > C(\Gamma_n)$.

3. Ile błędów wykrywają, a ile poprawiają nastęoujące kody?

   (a) Zbiór słów bitowych długości 100, gdzie każdy maksymalny blok złożony z tego samego bitu ma długość podzielną przez 5.
   Minimalna odległość Hamminga dwóch różnych słów jest 5, a zatem kod poprawia 2 błędy, a wykrywa 4.

   (b) Zbiór słów bitowych długości 100, gdzie każdy maksymalny blok jedynek ma długość podzielną przez 5.
   Minimalna odległość Hamminga dwóch różnych słów jest 2 (np. $1^5\,0^{95}, 01^5\,0^{94}$), a zatem kod wykrywa 1 błąd, a poprawia 0.

4. Przypomnijmy, że dla skończonej przestrzeni probabilistycznej S, $L_r(S)$ oznacza minimalną średnią długość słowa w kodzie kodującym elementy S nad alfabetem o mocy r, gdzie $r \geq 2$.

   Czy jest możliwe, że zachodzi równość $L_r(S) = H_r(S)$, a także $L_{r'}(S) = H_{r'}(S)$, dla $r \neq r'$?

   Tak, np. gdy prawdopodobieństwa są potęgami $\frac{1}{4}$, to są także potęgami $\frac{1}{2}$.

   Czy jest możliwe, że równość $L_r(S) = H_r(S)$ zachodzi dla nieskończenie wielu r ?

   Nie, bo dla $r \geq |S|$ mamy zawsze $L_r(S) = 1$, podczas gdy $\lim_{r\to\infty} H_r(S) = 0$.

5. Rozważamy kryptosystem podobny do szyfru Vernama (*One time pad*), a więc zmienne M (wiadomości, ang. *messages*), przyjmują wartości w $\{0,1\}^n$, ale **uwaga!** klucze K przyjmują wartości w $\{0,1\}^{2n}$. Zakładamy, że zmienna K ma rozkład jednostajny i jest niezależna od M. Określamy szyfrogram (*cipher-texts*)

$$C \quad = \quad M \oplus \ell(K) \oplus r(K),$$

   gdzie $|\ell(k)| = |r(k)| = n$ i $k = \ell(k)\, r(k)$.

   Czy ten system jest doskonale bezpieczny? Odpowiedź proszę krótko uzasadnić.

   Tak. Nietrudno widzieć, że $\ell(K) \oplus r(K)$ ma również rozkład jednostajny. Ponadto $I(M; \ell(K) \oplus r(K)) \leq I(M; K) = 0$. Zatem zmienna określona $K' = \ell(K) \oplus r(K)$ spełnia te same warunki co K w definicji *One time pad*, a $C = M \oplus K'$.

Ł.Dębowski, T.Gogacz, D.Niwiński