Egzamin z Teorii informacji 20 lutego 2018.

Odpowiedzi proszę wpisywać **na tej kartce**. *Kartkę proszę podpisać. Uzasanienia są wymagane tylko tam, gdzie jest to zaznaczone.*

1. Dla słowa $w \in \{0,1\}^n$, niech $ord(w) = 0^k\, 1^\ell$, gdzie $k = \sharp_0 w$, $\ell = \sharp_1 w$. Np. $ord(0010110) = 0000111$. Rozważamy kanał nad zbiorem symboli $\{0,1\}^n$, który przeprowadza słowo w na słowo $ord(w)$, tzn. $P(B = ord(w)|A = w) = 1$, dla $w \in \{0,1\}^n$. Obliczyć pojemność tego kanału.

   Zauważmy, że w tym kanale B zależy funkcyjnie od A, czyli $H(B|A) = 0$. Zatem potrzebujemy zmaksymalizować $I(A;B) = H(B)$. Zauważmy, że B może przyjąć $n+1$ różnych wartości. Enropia jest największa (równa $\log(n+1)$), gdy B ma rozkład jednostajny. Nietrudno jest to uzyskać, określając rozkład A, tak, by dla każdego $k = 0, 1, \ldots, n$, prawdopodobieństwo $Pr(ord(A) = 0^k 1^{n-k})$ przyjmowało tę samą wartość $\frac{1}{n+1}$.

2. Rzucamy dwa razy niezależnie sprawiedliwą kostką do gry. Zmienne losowe A_1, A_2 o wartościach w zbiorze $\{1, 2, \ldots, 6\}$ reprezentują wyniki rzutów. Określamy $A = A_1 + A_2$ oraz

$$B \quad = \quad \begin{cases} A_1 + A_2 & \text{jeśli} \quad A_1 = A_2 \\ 0 & \text{w pp.} \end{cases}$$

   Porównać następujące liczby

$$H(A),\ H(A|A_1),\ H(B|A_1),\ I(A;B|A_1)$$

   Zauważmy, że

$$\begin{aligned} I(A;B|A_1) &= H(A|A_1) - \underbrace{H(A|B,A_1)}_{>0} \\ &= H(B|A_1) - \underbrace{H(B|A,A_1)}_{=0} \end{aligned}$$

   gdyż B jest funkcją A i A_1, podczas gdy, jak łatwo sprawdzić, A nie zależy funkcyjnie od B i A_1. A zatem

$$I(A;B|A_1) = H(B|A_1) < H(A|A_1) < H(A)$$

   ostatnia nierówność wynika z faktu, że zmienna A nie jest (oczywiście) niezależna od A_1.

3. Przypomnijmy, że w szyfrze Vernama (*One time pad*) zmienne losowe M, K, C przyjmują wartości w zbiorze $\{0,1\}^n$, przy czym $C = f(M,K)$, gdzie

$$f\left((m_1, \ldots, m_n), (k_1, \ldots, k_n)\right) \quad = \quad (m_1 \oplus k_1, \ldots, m_n \oplus k_n),$$

   gdzie $\oplus$ oznacza dodawanie mod2 (inaczej *xor*). Rozważmy system szyfrowania, gdzie K nadal przyjmuje wartości w $\{0,1\}^n$ (z rozkładem jednostajnym), natomiast $M, C \in \{0,1\}^{2n}$, przy czym $C = g(M,K)$, gdzie

$$g\left((m_1, \ldots, m_{2n}), (k_1, \ldots, k_n)\right) \quad = \quad (m_1 \oplus k_1, \ldots, m_n \oplus k_n,\ m_{n+1} \oplus k_1, m_{n+2} \oplus k_2, \ldots, m_{2n} \oplus k_n)\,.$$

   Czy ten szyfr jest doskonale bezpieczny (*perfectly secure*)? Odpowiedź krótko uzasadnij.

Oczywiście nie, bo zgodnie z tzw. pesymistycznym twierdzeniem Shannona (*Theorem 9* w notatkach) w szyfrze doskonale bezpiecznym $H(M) \leq H(K)$ podczas gdy tu długość wiadomości aż dwukrotnie przekracza długość klucza, więc w szczególności, dla jednostajnego rozkładu M zachodzi $H(K) < H(M)$. Przytoczony szyfr odpowiada dwukrotnemu wykorzystaniu klucza w systemie *One time pad*; błąd ten prowadził w historii do poważnych konsekwencji (por. notatki).

4. Niech C_k będzie kodem Hamminga o k bitach kontrolnych. Określmy kody

$$\begin{aligned} C' &= \{ww : w \in C_k\} \\ C'' &= \{vw : v, w \in C_k\} \end{aligned}$$

Ile błędów poprawiają te kody?

Wiemy, że minimalna odległość między słowami w kodzie Hamminga jest 3 (por. Notatki, *Section 2.12*. Łatwo sprawdzić, że minimalna odległość w C'' jest nadal 3, a w C' jest 6. zatem C' poprawia 2 błędy, a C'' jeden błąd.

5. Niech Γ będzie binarnym kanałem symetrycznym (BSC) o macierzy $\begin{pmatrix} P & Q \\ Q & P \end{pmatrix}$, gdzie $P > Q$.

Dla kodu $C \subseteq \{0,1\}^n$ rozważamy dwa parametry: szybkość transmisji (*transmission rate*) $\frac{\log |C|}{n}$ i błąd transmisji $Pr_E(\Delta, C)$, gdzie Δ jest regułą najbliższego sąsiada. Jaki jest związek między asymptotycznym zachowaniem tych parametrów a przepustowością kanału C_Γ?

Odpowiedzi na to pytanie udziela oczywiście twierdzenie Shannona o kanałach. W pracy należało je przytoczyć, my odsyłamy do notatek

`https://www.mimuw.edu.pl/~niwinski/Info/2017-info.pdf`