Egzamin z Teorii informacji. Zadania

20 lutego 2018

Rozwiązania zadań proszę pisać na oddzielnych, czytelnie podpisanych kartkach.

Zadanie 1. Niech C będzie kanałem nad alfabetem $\{a,b,c,d\}$ o macierzy

$$\begin{bmatrix} 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \end{bmatrix}$$

Kanał ten wykorzystujemy 4-krotnie, przesyłając ciąg 4 symboli. Tworzymy w ten sposób kanał C^4 nad alfabetem $\{a,b,c,d\}^4$, gdzie

$$P(w_1w_2w_3w_4|v_1v_2v_3v_4) \quad = \quad P(w_1|v_1)\cdot\ldots\cdot P(w_4|v_4)$$

Wyznaczyć przepustowość bezbłędną (*error free capacity*) kanału C^4 określoną jako $\max I(A;B)$,, gdzie maksimum jest brane jedynie po takich parach wejścia-wyjścia (A,B), że $H(A|B)=0$.

Mamy $I(A;B) = H(A) - \underbrace{H(A|B)}_{0} = H(A)$. Potrzebujemy więc zmaksymalizować $H(A)$, ale jedynie po takich A, że $H(A|B)=0$. Warunek ten implikuje, że A musi być funkcją B. Dokładniej, istnieje funkcja $f:\{a,b,c,d\}^4 \to \{a,b,c,d\}^4$, taka że

$$Pr(A = f(w)|B=w) = 1, \text{ o ile } Pr(B=w)>0. \tag{1}$$

Wykażemy, że jest to możliwe tylko dla takich A, gdzie masa prawdopodobieństwa jest skoncentrowana na jednej wartości. Istotnie, przypuśćmy, że $Pr(A=u), Pr(A=v)>0$, dla pewnych różnych słów u,v. Wtedy istnieje słowo w takie, że $Pr(B=w|A=u)>0$ i $Pr(B=w|A=v)>0$ (więc także $Pr(B=w)>0$). W istocie własność tę ma każde słowo $w=w_1w_2w_3w_4$, takie że $w_i \neq u_i, v_i$, dla $i=1,\ldots,4$. Dla takich u,v,w mamy więc także $Pr(A=u|B=w)>0$ i $Pr(A=v|B=w)>0$, co wyklucza warunek (1). A więc maksimum jest osiągnięte dla takich A, dla których $H(A)=\mathbf{0}$ i taka jest bezbłędna przepustowość kanału C^4.

Zadanie 2. Niech $C \subseteq \{0,1\}^n$ będzie kodem o 2^k elementach i o minimalnej odległości Hamminga między słowami kodowymi równej ℓ.

(a) Wykaż, że

$$k+\ell \quad \leq \quad n+2.$$

(b) Przy założeniu, że C jest kodem liniowym, wykaż

$$k+\ell \quad \leq \quad n+1.$$

Ad (a). Niech t będzie największe takie, że $2t+1 \leq \ell$. Wtedy kod C poprawia t błędów, a zatem kule o środkach w słowach kodowych i promieniu t muszą być rozłączne. Jeśli moc takiej kuli oznaczymy przez b_t, oznacza to, że $2^k \cdot b_t \leq 2^n$. Dla rozwiązania zadania wystaczy więc wykazać, że $2^{\ell-2} \leq b_t$. Mamy z definicji

$$b_t = 1 + n + \binom{n}{2} + \ldots + \binom{n}{t}$$

Z drugiej strony znamy ładną zależność

$$2^{2t} = 1 + (2t+1) + \left(\begin{array}{c} 2t+1 \\ 2 \end{array} \right) + \ldots + \left(\begin{array}{c} 2t+1 \\ t \end{array} \right)$$

Ale symbol Newtona jest monotoniczny ze względu na „górną" współrzędną, więc porównując prawe strony powyższych równości, otrzymujemy $2^{2t} \leq b_k$. Dla zakończenia dowodu wystarczy zauważyć, że wobec maksymalności t, mamy $\ell - 2 \leq 2t$.

Ad (b). Jeśli kod jest liniowy rozmiaru 2^k, to jako podprzestrzeń liniowa przestrzeni $\{0,1\}^n$ ma wymiar k. Ponadto minimalna liczba jedynek w niezerowym wektorze kodowym wynosi ℓ. Skorzystamy ze znanego z Ćwiczeń pojęcia *macierzy kontroli parzystości*, czyli macierzy A reprezentującej przekształcenie liniowe $\mathbf{A} : \{0,1\}^n \to \{0,1\}^{n-k}$, dla którego C jest jądrem, tzn.

$$C = \{w : A \cdot w^\top = \vec{0}\}.$$

Z algebry liniowej wiemy, że wymiar $rank(A)$ spełnia

$$n = \underbrace{null(A)}_{k} + rank(A)$$

wystarczy więc udowodnić, że $\ell - 1 \leq rank(A)$. Przypuśćmy, że $rank(A) < \ell - 1$, czyli każde $\ell - 1$ kolumn macierzy A jest liniowo zależne. W ogólności zależność wektorów $u_1, \ldots, u_p$ oznacza możliwość takiego doboru współczynników z ciała, powiedzmy $\alpha_1, \ldots, \alpha_p$, nie wszystkich równych 0, że $\alpha_1 u_1 + \ldots + \alpha_p u_p = \vec{0}$. W naszym wypadku oznacza to po prostu, że możemy wybrać $r \leq \ell - 1$ kolumn macierzy A, które sumują się do $\vec{0}$. Powiedzmy, że są to kolumny o numerach $k_1, \ldots, k_r$. Jeśli teraz określimy wektor u tak, by miał jedynki dokładnie na pozycjach $k_1, \ldots, k_r$ (poza tym zera), to taki wektor należy do jądra przekształcenia $\mathbf{A}$ (a więc do kodu C), a zarazem ma $< \ell$ jedynek, wbrew założeniu. Otrzymana sprzeczność kończy dowód.