Teoria informacji - praca domowa

Tomasz Kępa, tk359746@students.mimuw.edu.pl

26 stycznia 2019

1 Porównanie przepustowości kanałów

1.1 Przepustowość kanału XORującego losowy bit

Ten przypadek jest dość łatwy.

$$C_\Gamma = \max_X I(X;Y) = \max_X (H(Y) - H(Y|X))$$

Dla ustalonego $x \in X$, $H(Y|x) = \log n$ ponieważ każda wiadomość może ulec zmianie na jednej z n pozycji z równym prawdopodobieństwem. Zatem

$$H(Y|X) = \sum_{x \in X} p(x) H(Y|x) = \log n$$

niezależnie od rozkładu X.

Informacja wzajemna $I(X;Y)$ będzie zatem maksymalna wtedy gdy $H(Y)$ będzie maksymalne. $H(Y)$ będzie maksymalne gdy Y będzie miał rozkład jednostajny, a to, dzięki symetrii, następuje wtedy gdy X ma rozkład jednostajny i wtedy $H(Y) = \log 2^n = n$

Ostatecznie

$$C_{\Gamma_{\text{XOR}}} = \max_X I(X;Y) = \max_X (H(Y) - H(Y|X)) = n - \log n$$

1.2 Przepustowość kanału zerującego losowy bit

Kanał zerujący losowy bit jest dużo trudniejszy do analizy. Zacznę od przypadku gdy n jest wystarczająco duże aby zastosować pewne oszacowanie, a następnie sprawdzę ręcznie pozostałe przypadki

Niech $z(x)$ - funkcja, która dla słowa $x \in \{0,1\}^n$ zwraca ilość zer w tym słowie.

Policzę teraz $I(X;Y)$ gdy X ma rozkład jednostajny

$$\begin{aligned} H(X|y) = &- z(y) \cdot \frac{\frac{1}{n}}{\frac{z(y)}{n} + \frac{z(y)}{n}} \cdot \log \frac{\frac{1}{n}}{\frac{z(y)}{n} + \frac{z(y)}{n}} \\ &- \frac{\frac{z(y)}{n}}{\frac{z(y)}{n} + \frac{z(y)}{n}} \cdot \log \frac{\frac{z(y)}{n}}{\frac{z(y)}{n} + \frac{z(y)}{n}} \end{aligned}$$

Pierwszy składnik sumy odpowiada za przypadki, kiedy słowo y powstało przez zamianę jakiejś jedynki na 0. Ponieważ jest $z(y)$ zer to do tego słowa prowadzi w ten sposób $z(y)$ słów, każde z prawdopodobieństwem $\frac{\frac{1}{n}}{\frac{z(n)}{n} + \frac{z(y)}{n}}$ Drugi składnik sumy odpowiada przypadkowi, kiedy kanał wylosował pozycję na której stało już 0. Znowu, jest takich pozycji $x(y)$ i prawdopodobieństwo że nastąpiła taka sytuacja wynosi $\frac{\frac{z(y)}{n}}{\frac{z(y)}{n} + \frac{z(y)}{n}}$ Można teraz uprościć to wyrażenie

$$H(X|y) = -\frac{1}{2} \cdot \log \frac{1}{2 \cdot z(y)} - \frac{1}{2} \cdot \log \frac{1}{2} = 1 + \frac{1}{2} \cdot \log z(y)$$

I dalej, kiedy X ma rozkład jednostajny

$$I(X;Y) = H(X) - H(X|Y) = n - \sum_{y \in Y} p(y) \cdot \left(1 + \frac{1}{2} \cdot \log z(y)\right)$$

Dla przypadku, gdy $n \geq 4$ można zastosować oszacowanie $z(y) \leq n$ co daje

$$I(X;Y) > n - 1 - \frac{1}{2}\log n \geq n - \log n = \mathcal{C}_{\Gamma_{\text{XOR}}}$$

Krótkie wyjaśnienie czemu powyższa nierówność zachodzi dla $n \geq 4$

$$\begin{aligned} n - 1 - \frac{1}{2}\log n &\geq n - \log n \\ \frac{1}{2}\log n &\geq 1 \\ \log n &\geq 2 \end{aligned}$$

A to w oczywisty sposób zachodzi dla $n \geq 4$.

Pokazałem zatem że dla $n \geq 4$ kanał zerujący losowy bit ma większą przepustowość niż kanał XORujący losowy bit.

Dla $n < 4$ oszacowanie nie działa, ale nie znaczy to że kanał zerujący ma we wszystkich tych przypadkach mniejszą przepustowość.

Dla $n = 3$ w przypadku gdy X ma rozkład jednostajny, można ręcznie policzyć dokładną wartość $I(X;Y)$

$$\begin{aligned} H(X|Y) = \sum_{y \in Y} H(X|y) &= \left(\frac{1}{8} + \frac{1}{3}\cdot\frac{3}{8}\right) H\left(\{\frac{1}{2}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}\}\right) \\ &+ \left(\frac{2}{3}\cdot\frac{3}{8} + \frac{2}{3}\cdot\frac{3}{8}\right) H\left(\{\frac{1}{2}, \frac{1}{4}, \frac{1}{4}\}\right) \\ &+ \left(\frac{1}{3}\cdot\frac{3}{8} + \cdot\frac{1}{8}\right) H\left(\{\frac{1}{2}, \frac{1}{2}\}\right) \\ &\geq 1.599 \end{aligned}$$

Kolejne składniki tej sumy odpowiadają za słowa $y \in Y$ o coraz mniejszej ilości zer. Wartość 1.599 jest większa niż $3 - \log 3 \approx 1.415$ zatem dla $n = 3$ kanał ten również ma większą przepustowość

Dla $n = 2$ porównanie jest dużo trudniejsze

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= \left(p_0 + \frac{p_1}{2} + \frac{p_2}{2}\right) \frac{1}{\log\left(p_0 + \frac{p_1}{2} + \frac{p_2}{2}\right)} \\ &+ \left(\frac{p_1}{2} + \frac{p_3}{2}\right) \frac{1}{\log\left(\frac{p_1}{2} + \frac{p_3}{2}\right)} \\ &+ \left(\frac{p_2}{2} + \frac{p_3}{2}\right) \frac{1}{\log\left(\frac{p_2}{2} + \frac{p_3}{2}\right)} \\ &- p_1 - p_2 - p_3 \end{aligned}$$

gdzie

$$p_0 = p(X = 00), p_1 = p(X = 01), p_2 = p(X = 10), p_3 = p(X = 11)$$

Mogę teraz skorzystać ze Złotego Lematu. Przyjmuję następujące wagi

$$\begin{aligned} x_1 &= p_0 + \frac{p_1}{2} + \frac{p_2}{2} \\ x_2 &= \frac{p_1}{2} + \frac{p_3}{2} \\ x_3 &= \frac{p_2}{2} + \frac{p_3}{2} \end{aligned}$$

oraz

$$y_1 = \frac{1}{2}, y_2 = y_3 = \frac{1}{4}$$

Mam teraz

$$\begin{aligned} C_\Gamma &\leq H(Y) - H(Y|X) \\ &\leq \left(p_0 + \frac{p_1}{2} + \frac{p_2}{2}\right)\log 2 + \left(\frac{p_1}{2} + \frac{p_3}{2}\right)\log 4 + \left(\frac{p_2}{2} + \frac{p_3}{2}\right)\log 4 - p_1 - p_2 - p_3 \\ &= p_0 + \frac{p_1}{2} + \frac{p_2}{2} + p_3 \leq p_0 + p_1 + p_2 + p_3 = 1 \end{aligned}$$

Ponieważ jestem w stanie wysłać 1 bit informacji (kodując $0 \to 00, 1 \to 11$), to również $C_\Gamma \geq 1$. Zatem ostatecznie $C_\Gamma = 1$ i w tym przypadku oba kanały mają taką samą przepustowość

Dla $n = 1$ to zwyczajny kanał zapominający i jego przepustowość wynosi $C_\Gamma = 0$, czyli w tym przypadku jest to mniej niż dla kanału XORującego losowy bit.

2 Kody

2.1 Kod dla kanału XORującego

Dla $n = 1$ jest to kanał odwracający i nie tutaj za bardzo o czym mówić - wystarczy odwracać bit na wyjściu.

Przejdę więc do przypadku, kiedy $n = 2$. Wtedy $\mathcal{C} = \{01, 00\}$. Po przejściu przez kanał łatwo je rozróżnić. 01 przechodzi na 00 lub 11, 00 na 01 lub 10.

Można tu poczynić pewną obserwację. W przypadku kodu Hamminga, aby rozróżnić dwie wiadomości, potrzebowaliśmy żeby przechodziły na słowa o minimalnej odległości Hamminga równej 3. Jednak w przypadku tego kanału można skorzystać z faktu, że przekłamanie na którymś bicie nastąpi zawsze. Dzięki temu, można wyróżnić jeden bit, w moim przypadku niech to będzie bit na ostatniej pozycji. Wtedy wystarczy, że bity na pozycjach od 1 do $n-1$ będą słowami o minimalnej odległości 3 między sobą, a ostatni bit będzie podwajał przestrzeń wiadomości. Jeśli po przejściu przez kanał pierwsze $n-1$ pozycji zawiera słowo, które nie jest w kodzie, wtedy wiem że przekłamanie było na jednej z tych pozycji. W takiej sytuacji szukam jedyne słowo kodowe o odległości Hamminga równej 1 a ostatni bit pozostawiam bez zmian. W przeciwnym wypadku przekłamanie wystąpiło na ostatnim bicie i wystarczy że zmienię jego wartość na przeciwną. Jeśli $n-1$ bitów jest liczbą postaci $2^k - 1$, to można na tych bitach po prostu użyć kodu Hamminga.

Niestety, nie mam uniwersalnej metody jak szukać maksymalnego zbioru słów długości n o odległości co najmniej 3. W przypadku, gdy $n-1$ jest liczbą postaci $2^k - 1$, użycie kodu Hamminga o tej długości jest optymalne, w innych przypadkach trzeba szukać takich słów ręcznie.

Przykłady znalezionych przez mnie kodów dla kolejnych n:

n	$\mathcal{C}$	$\lvert\mathcal{C}\rvert$
1	$\{0, 1\}$	2
2	$\{0\{0, 1\}\}$	2
3	$\{00\{0, 1\}\}$	2
4	$\{000\{0, 1\}, 111\{0, 1\}\}$	4
5	$\{0000\{0, 1\}, 1110\{0, 1\}\}$	4
6	$\{00000\{0, 1\}, 11100\{0, 1\}, 11011\{0, 1\}, 00111\{0, 1\}\}$	8
7	$\{000000\{0, 1\}, 111000\{0, 1\}, 110110\{0, 1\}, 101101\{0, 1\}, 011011\{0, 1\}, 100011\{0, 1\}, 010101\{0, 1\}, 001110\{0, 1\}\}$	16

Dla $n = 8$ konstrukcja została już podana w tekście (kod Hamminga na 7 bitach i dodatkowy bit na ósmej pozycji).

2.2 Kod dla kanału zerującego

Również zaczynam od przypadku $n = 2$. Tutaj można zakodować jeden bit przez powtórzenie go, czyli $\mathcal{C} = \{00, 11\}$. Po przejściu przez kanał łatwo te wiadomości odtworzyć – wiadomość 00 musi przejść jako 00, a 11 przejdzie jako 01 lub 10.

Przy $n = 3$ dodatkowy bit nie daje nic więcej.

Przy $n = 4$ można wysyłać dwa bity, kodując je tak samo jak poprzednio, w sumie 4 wiadomości

Przy $n = 5$ pierwsze 4 wiadomości wysyłam tak samo jak w przypadku $n = 4$, natomiast kolejne tworzę używając ostatniego bitu. Bit ten sygnalizuje dodatkowe dwie wiadomości, które charakteryzują

się naprzemiennymi zerami i jedynkami. Jestem w stanie rozróżnić te dodatkowe dwie wiadomości, ponieważ jeśli zgaśnie ostatni bit, to te wiadomości są zupełnie inne niż pierwsze cztery, ponieważ są to dwie pary 01 lub 10, a z tamtych może powstać tylko jedna taka para. Podobnie, jeśli zgaśnie inny bit, to ostatni bit sygnalizuje że była to wiadomość z dodatkowej pary. Podsumowując, dla $n = 5$, kod wygląda następująco $\mathcal{C} = \{00000, 00110, 11000, 11110, 01011, 10101\}$

Dla $n = 6$ kod zaczyna się od wiadomości kodowanych standardowo przez powtórzenie bitów. Daje to $2^3 = 8$ wiadomości. Dodatkowo, można powtórzyć trick z poprzedniego przypadku i dorzucić wiadomości z parami 01 oraz 10 na przemian. Znowu, odróżnienie takie pary jest proste, ponieważ ze standardowego kodowania można otrzymać tylko jedno wystąpienie 01 lub 10 a tu po przejściu przez kanał będą co najmniej dwa. Zatem dla $n = 6$ kod wygląda następująco

$$\mathcal{C} = \{000000, 000011, 001100, 001111, 110000, 110011, 111100, 111111, 010101, 101010\}$$

Dla $n = 7$ można zwyczajnie użyć kod Hamminga, co pozwola na wysyłanie 16 różnych wiadomości.

Dla $n = 8$ można 16 wiadomości zakodować jak poprzednio przez powtórzenie bitów, dodatkowe 4 wiadomości da się uzyskać podobnie jak w przypadku gdy $n = 6$. Te dodatkowe wiadomości to 01010100, 01010111, 10101000, 10101011.

Przypadek $n = 9$ to kodowanie kodem Hamminga 16 wiadomości w pierwszych 7 bitach i kodowanie dodatkowego bitu przez jego podwojenie na końcu. W sumie 5 bitów czyli 32 wiadomości.

Dla $n = 10$ można zacząć od kodowania przez podwojenie bitów – $2^5 = 32$ wiadomości. Dalej można dodać $2 + 2 + 2 * 2 = 8$ wiadomości przez kodowanie połowy bitów w taki sam sposób jak w przypadku gdy n było równe 5. Można zakodować pierwsze 5 bitów, resztę zostawić jako 0, potem ostatnie 5, pozostawiając resztę z zerami, i na koniec można kodować obie połowy niezależnie. W sumie 40 wiadomości.

Dla $n = 11$ znowu używamy kod Hamminga i tym razem kodujemy dodatkowe dwa bity przez ich podwajanie. W sumie 6 bitów czyli 64 wiadomości.

Reguła, którą się tutaj przewija jest z grubsza taka, że dla nieparzystych długości stosujemy jak najdłuższy kod Hamminga (o ile $n \geq 7$) i doklejamy dodatkowe bity kodując je przez ich podwojenie. Dla długości parzystych opłaca się bardziej zaczynać od kodowania $\frac{n}{2}$ bitów przez ich podwajanie a potem wzbogacać kod tak jak w powyższych przykładach. Jeśli kanał jest odpowiednio szeroki może opłacać się też wzięcie dwóch sklejonych kodów Hamminga.