Komunikacja i Kryptografia Kwantowa

Seria 2

Odpowiedzi

Zadanie 1 Rozważ jedno-bitowy kanał $X \to Y$, $\mathcal{X} = \mathcal{Y} = \{0, 1\}$, gdzie

$$p(y|x) = \begin{array}{c|c|c} y\backslash x & 0 & 1 \\ \hline 0 & 1-\epsilon & \epsilon \\ \hline 1 & \epsilon & 1-\epsilon \end{array} \tag{1}$$

czyli ϵ można traktować jako prawdopodobieństwo błędu. Znajdź pojemność $\mathcal{C}$ tego kanału.

Odpowiedź: $\mathcal{C} = 1 - h(\epsilon)$, gdzie $h(x) = -x \log x - (1-x)\log(1-x)$

Zadanie 2 Rozważ jedno-bitowy kanał $X \to Y$, $\mathcal{X} = \mathcal{Y} = \{0, 1\}$, gdzie

$$p(y|x) = \begin{array}{c|c|c} y\backslash x & 0 & 1 \\ \hline 0 & 1-\epsilon & 0 \\ \hline 1 & \epsilon & 1 \end{array} \tag{2}$$

Znajdź pojemność $\mathcal{C}$ tego kanału.

Odpowiedź: $\mathcal{C} = \frac{\epsilon}{1-\epsilon} \log \epsilon + \log\left(1 - \epsilon + \epsilon^{-\epsilon/(1-\epsilon)}\right)$

Zadanie 3 Rozważ kanał, $X \to Y$, gdzie $\mathcal{X} = \{0, 1\}$, $\mathcal{Y} = \{0, 1, e\}$,

$$p(y|x) = \begin{array}{c|c|c} y\backslash x & 0 & 1 \\ \hline 0 & 1-\epsilon & 0 \\ \hline 1 & 0 & 1-\epsilon \\ \hline e & \epsilon & \epsilon \end{array} \tag{3}$$

czyli można traktować ten kanał jako kanał z prawdopodobieństwem błędu ϵ, który to błąd w przeciwieństwie to przykładu z Zadania 1, jest sygnalizowany symbolem e. Znajdź pojemność kanału. Porównaj z pojemnością kanału z Zadania 1

Odpowiedź: $\mathcal{C} = 1 - \epsilon$

Zadanie 4 Na twierdzenie Shannona o pojemności kanałów można patrzeć jak na pewną formę korekcji błędów. Wiadomość koduje się w taki sposób aby mimo błędów nie było wątpliwości dla odbiorcy jaka była oryginalna wiadomość — tzn. istnieje procedura dekodująca pozwalająca usunąć błędy. Można na to patrzeć jak na kodowanie w celu „uodpornienia" wiadomości na błędy, albo korekcja błędów „zawczasu".

Rozważmy teraz nieco inny schemat. Wiadomość n bitowa jest przesyłana bezpośrednio przez jednobitowy zaszumiony kanał $X \to Y$ (użyty oczywiście n razy) o pojemności $\mathcal{C} < 1$, bez żadnego kodowania. Naturalnie, że pojawią się błędy. Wyobraźmy sobie teraz, że dysponujemy drugim idealnym kanałem, w którym błędy nie występują. Asymptotycznie, ile dodatkowych bitów informacji co najmniej trzeba przesłać tym drugim idealnym kanałem aby odbiorca korzystjąc z tej dodatkowej informacji był w stanie naprawić praktycznie wszystkie błędy. Postaraj się przedstawić intuicyjny dowód, analogiczny do tego który podany był na wykładzie dla oryginalnego twierdzenia [1].

Można patrzeć na ten protokół jako na korekcje błędów „poniewczasie".

Odpowiedź: Potrzebujemy dodatkowo $nH(X|Y) = n[H(X) - \mathcal{C}]$. Należy rozważyć, z ilu potencjalnie różnych ciągów x^n mógł wziąć się zaobserwowany przez odbiorcę ciąg y^n. Ta niejednoznaczność musi zostać usunięta za pomocą przesłanych dodatkowo bitów.

[1] To zagadnienie może wydać ci się sztuczne. Po co w ogóle przesyłać coś zaszumionym kanałem skoro mamy drugi idealny. Nie mniej jest to ważne zagadnienie, gdyż dokładnie taka sytuacja pojawia się w kwantowej dystrybucji klucza: kanałem zaszumionym jest kanał kwantowy, kanałem idealnym jest kanał klasyczny.