

# Komunikacja i Kryptografia Kwantowa

## Seria 3

do oddania na 02.11.2010 (100 pkt do podziału)

**Zadanie 1 (30 pkt)** Antek, Basia i Emilia postanowili przysyłać sobie wiadomości za pomocą dwóch okrzyków: „Och” i „Ach”. Basia i Emilia słuchając okrzyków Antka popełniają błąd w interpretacji okrzyku z prawdopodobieństwem odpowiednio 5% i 7%. Antek wydając okrzyki również czasem się myli i wydaje niewłaściwy okrzyk z prawdopodobieństwem 5%. Antek i Basia postanowili wymyślić taki protokół kodowania i dekodowania aby móc przysyłać sobie informację tak by Emilia nie mogła dowiedzieć się niczego na temat wiadomości. Ile bitów sekretnej informacji na jeden okrzyk mogą maksymalnie przysyłać sobie Antek i Basia?

**Zadanie 2 (15 pkt)** Dla  $n$  zmiennych losowych  $X_i$  oraz zmiennej losowej  $Y$  udowodnij następujący fakt (chain rule)

$$I(X_1, \dots, X_n : Y) = \sum_{i=1}^n I(X_i : Y | X_1, \dots, X_{i-1}) \quad (1)$$

**Zadanie 3 (10 pkt)** Dla łańcucha Markowa  $X \rightarrow Y \rightarrow Z$  udowodnij:

$$I(X, Y : Z) = I(Y : Z) \quad (2)$$

Podaj intuicyjne znaczenie powyższej równości.

**Zadanie 4 (10 pkt)** Dla dowolnych trzech zmiennych losowych  $X, Y, Z$  udowodnij, że

$$I(XY : Z | X) = I(Y : Z | X) \quad (3)$$

Podaj intuicyjne znaczenie powyższej równości.

**Zadanie 5 (35 pkt)** Na twierdzenie Csiszar-Korner można patrzeć jak na sytuację w której „zawczasu” nadawca  $A$  wykonuje *korekcję błędów*, kodując wiadomość tak by uprawniony odbiorca  $B$  mógł ją odczytać bez błędów, lecz dodatkowo wprowadzamy pewną losowość w kodowaniu, które powoduje, że nieuprawniony odbiorca  $E$  nie jest w stanie dowiedzieć się nic o przesyłanej wiadomości. Ten drugi element można nazwać *wzmocnieniem prywatności* „zawczasu”.

Wyobraź sobie sytuację, w której  $A$  przesłał ciąg  $n$  bitów bez wykonywania żadnej korekcji błędów ani wzmocnienia prywatności zawczasu. Rozważ, tak jak to było założone w poprzedniej serii, że istnieje dodatkowy publiczny idealny kanał, którym  $A$  może wysłać dodatkową informację. Ponieważ kanał jest publiczny, informacja będzie odczytana zarówno przez  $B$  jak i  $E$ . Mając do dyspozycji taki idealny kanał, spróbuj intuicyjnie opisać co powinni zrobić  $A$  i  $B$  aby na koniec swojego postępowania uzyskać ciąg bitów, który nie ma błędów a o którym  $E$  nic nie wie. Postaraj się gdzie tylko potrafisz podać ilościowe odpowiedzi (np. ile bitów musi przesłać  $A$  do  $B$ , ile bitów zostanie im na koniec, wyrażone przez odpowiednie wielkości charakteryzujące kanał). Ten protokół można nazwać korekcją błędów i wzmocnieniem prywatności „poniewczasie”.