Komunikacja i Kryptografia Kwantowa

Seria 11

do oddania na 4.01.2011 (**100 pkt** do podziału)

Zadanie 1 (20 pkt) Udowodnij, że w twierdzeniu Holevo-Schumacher-Westmoreland, maksymalizację po $\{p_x, \rho_x\}$, można zawsze ograniczyć do maksymalizacji po stanach czystych, tzn: $\rho_x = |\psi_x\rangle\langle\psi_x|$

Zadanie 2 (20 pkt) Korzystając z ograniczenia Holevo, udowodnij, że przez jedno-qubitowy idealny kanał kwantowy można maksymalnie przesłać 1 bit informacji.

Zadanie 3 (25 pkt) Oblicz pojemność kanału qubitowego, którego efektem jest izotropowe kurczenie kuli Blocha o współczynnik $r < 1$.

Zadanie 4 (35 pkt) Udowodnij własność strong subadditivity dla entropii Shannona:

$$H(Y) + H(X,Y,Z) \leq H(X,Y) + H(Y,Z) \tag{1}$$

Jaką własność powinny mieć zmienne losowe X, Y, Z aby w powyższej nierówności zachodziła równość. Zastanów się dlaczego nie da się tego dowodu „ukwantowić" (chyba, że się da wtedy będziesz sławny(a)).