Zestawy egzaminacyjne z przedmiotu Podstawy Informatyki Kwantowej

dr K. Horodecki
Instytut Informatyki, Uniwersytet Gdański

Zestawy egzaminacyjne (tylko to obowiązuje na egzamin). Losowany jest 1 zestaw z poniższych. Każdy zestaw składa się z 3 zagadnień a,b,c. Egazmin jest pisemny. Poprawny opis 1 zagadnienia daje 10 pkt. Egzamin jest zaliczony jeśli uzyska się w sumie min. 15 pkt.

1. (a) Podaj 2 z aksjomatów mechaniki kwantowej: (1) co to jest stan kwantowy oraz (2) aksjomat pommiaru
   (b) Opisz protokół BB84 i główną zasadę jego bezpieczeństwa (pomiar nieznanego stanu z dużym prawdopodobieństwem zaburza układ)
   (c) Podaj definicję podukładów dwuukładowego stanu kwantowego z przykładem obliczenia na jakimś stanie.
2. (a) Opisz protokół destylacji singletów ze stanów mieszanych 2 układowych Bennetta et al. (nie trzeba przywoływać całej tabelki działania dwóch CNOTów, wystarczy 1-2 przykłady)
   (b) Definicja stanu separowalnego (i splątanego). kryterium częściowej transpozycji dla 2x2 i 2x3 splątania stanu. Co to są stany o związanym splątaniu (w tym co to są operacje Lokalne i kls. komunikacja LOKK)
   (c) Opisz protokół gęstego kodowania
3. (a) Podaj 2 aksojmaty m.k. - układu złożonego i ewolucji układu niemierzonego
   (b) Opisz przykładowe 2 ataki na protokół BB84 (przez pomiar w jednej z 2 baz i pstwo tego że Ewa nie jest złapana i wybrany losowo oraz atak man in the middle) i dlaczego nie są one szkodliwe (w tym uwierzytelnianie).
   (c) Udowodnij tw. o nieklonowaniu, opisz na tej podstawie pomysł Wiesnera o kwantowych pieniądzach.
4. (a) Opisz protokół B92
   (b) Podaj dowód tw. że pomiar 2 stanów które nie są ortogonalne albo je narusza, albo nie daje żadnej informacji.
   (c) Opisz algorytm Simona i szkic dowodu jego złożoności kwantowej i klasycznej
5. (a) Podaj definicję wartości średniej obserwabli kwantowej i przykład obliczenia
   (b) Opisz jakie są zawierania pomiędzy zbiorami układów lokalnych, kwantowych i niesygnalizujących oraz które z nich łamią nierówność CHSH. Opisz nierówność CHSH i szkic jej dowodu.
   (c) Opisz protokół one-time-pad oraz wyjaśnij jak można generować klucz kwantowy mając do dyspozycji źródło stanów singletowych. Uzasadnij, że tak otrzymany klucz jest bezpieczny podając definicję dopełniania stanu dwuukładowego do stanu czytego trójukładowego.
6. (a) Opisz działanie i ideę zastosowanie alg. Grovera
   (b) Opisz protokół teleportacji.
   (c) Opisz protokół E91. o jakie 2 założenia opiera się jego bezpieczeństwo ? (w tym kontekście: co to jest device independent quantum cryptography)
7. (a) Definicja entropii Shannona i von Neummanna, oraz przykład występowania entropii von Neumanna i Shannona w kontekście ważnych protokółów (np. state merging) co to jest wzajemna informacja. diagram Venna dla entropii i na jego podstawie znane zależności między wielkościami entropowymi
   (b) Podać bramki kwantowe poznane na wykładzie i ich działanie na bazie standardowej (jednego lub 2 kubitów w zależności od liczby wejść bramki). Czym różnią się od klasycznych ? Opisać algorytm Deutscha.
   (c) Definicja stanów bezpiecznych, rozróżnianie stanów za pomocą operacji LOKK oraz globalnych i zastosowanie do pokazania faktu, że niektóre stany bezpieczne nie nadają się do "key repeaters" - "powtarzania klucza".
8. (a) Opisz kwantową trasformatę Fouriera, oraz opisz jak działa ona i jaką ma złożoność czasową (liczbę kwantowych bramek z których się składa)

(b) Jakie są problemy z kwantową dystrybucją klucza i jak można się ich pozbyć za pomocą splątania (giną fotony, ale jest entanglement swapping i dalej : idea kwantowych powtarzaczy).

(c) Opisz ideę algorytmu Shora rozkładu liczby na czynniki pierwsze i jego zastosowanie (bez definiowania kwantowej tr. Fouriera) w opisie podaj obwód podprocedury która rozwiązuje ten algorytm.