Zadgadnienia do egzaminu z algorytmów kwantowych

1. Podstawowe bramki kwantowe — opis, działanie, reprezentacja macierzowa.
2. Które bramki kwantowe tworzą układ zupełny, umożliwiający przybliżoną realizację dowolnej n-qubitoiwej operacji unitarnej?
3. Podać opis działania i reprezentację macierzową bramki "kontrolowane H".
4. Bramki C-NOT i CC-NOT: opis działania i reprezentacja macierzowa.
5. Zaproponować realizację odwracalnej bramki AND.
6. Zaproponować realizację odwracalnej bramki OR.
7. Dla funkcji logicznej $F : \{0,1\}^n \to \{0,1\}$ zaprojektować odwracalną bramkę logiczną.
8. Omówić twierdzenie o zakazie klonowania stanów kwantowych.
9. Reprezentacja stanów pojedynczego qubitu na sferze Blocha.
10. Na czym polega teleportacja stanów kwantowych?
11. Problem Deutscha jedno- i wielo-qubitowy —- na czym polega i jak wygląda jego kwantowe rozwiązanie?
12. Zaprojektować układ kwantowy, który dla danej funkcji logicznej $F : \{0,1\}^n \to \{0,1\}$ generuje superpozycję wszystkich jej wartości.
13. Na czym polega problem Simmona? Jak ma się złożoność obliczeniowa kwantowego rozwiązania do rozwiązania klasycznego?
14. Opisać system kryptograficzny z publicznym kluczem. Na czym opiera się jego bezpieczeństwo?
15. Omówić algorytm szyfrowania RSA. Na czym opiera się jego bezpieczeństwo?
16. Opisać podstawowe kroki w algorytmie Shora. Wskazać, które z nich istotnie wykorzystują mechanizm kwantowy.
17. Opisać kwantową transformatę Fouriera.
18. Rząd elementu w grupie $\mathbb{Z}_n^\times$. Jaką rolę odgrywa wyznaczanie rzędu w zagadnieniu faktoryzacji dużych liczb?
19. Na czym polega estymacja fazy? Jak się ją realizuje kwantowo?
20. Jak wygląda operator unitarny U służący do wyznaczania rzędu (przez estymację fazy U) w algorytmie faktoryzacji Shora?
21. Opisać jak z binarnego przybliżenia liczby wymiernej $\frac{s}{r} \approx 0.b_1b_2b_3\ldots b_t$ odczytać jej mianownik r?
22. Opisać w jakich sytuacjach algorytm Shora może zakończyć się niepowodzeniem.
23. Opisać postać i działanie operatora Grovera G, będącego podstawą algorytmu kwantowego wyszukiwania.
24. Opisać algorytm Grovera kwantowego wyszukiwania.
25. Opisać różnice w działaniu algorytmu kwantowego wyszukiwania Grovera w zależności od tego, jak duża w stosunku do rozmiaru bazy N jest liczba poszukiwanych obiektów M.
26. Na czym polega "kwadratowe przyspieszenie" algorytmów kwantowych w stosunku do ich klasycznych odpowiedników dla problemów klasy NP?