

Mechanika Kwantowa dla doktorantów - 18 zestaw
25.3.2009. środa godz. 9:15, sala na antresoli

1. Proszę dokończyć zadanie z poprzedniego zestawu: wyprowadzić relację komutacji operatorów pędu i położenia wyliczając:

$$\langle \chi | m \frac{1}{\epsilon} ((x_{k+1} - x_k)x_k - x_{k+1}(x_{k+1} - x_k)) | \psi \rangle,$$

gdzie

$$\langle \chi | F | \psi \rangle_S = \iint dx_1 dx_2 \chi^*(x_2) \left[\int_{x_1}^{x_2} [\mathcal{D}(x(t)) F[x(t)] e^{\frac{i}{\hbar} S[x(t)}] \right] \psi(x_1).$$

Zadanie wykonać rozważając ewolucję czasową funkcji falowej o jeden krok czasowy, podobnie jak w przypadku dowodu, że f. falowa spełnia równanie Schrödingera.

2. **Kryptografia kwantowa.** Stan początkowy cząstek a i b o spinie $1/2$ jest

$$|\Sigma\rangle = \frac{1}{\sqrt{2}} \{ |\sigma_z = +1\rangle_a |\sigma_z = +1\rangle_b + |\sigma_z = -1\rangle_a |\sigma_z = -1\rangle_b \}. \quad (1)$$

Pokazać, że ten stan można też zapisać jako

$$|\Sigma\rangle = \frac{1}{\sqrt{2}} \{ |\sigma_x = +1\rangle_a |\sigma_x = +1\rangle_b + |\sigma_x = -1\rangle_a |\sigma_x = -1\rangle_b \}. \quad (2)$$

Cząstki przygotowane w stanie (1,2) rozlatują się w dwu przeciwnych kierunkach. Alicja mierzy składową spinu cząstki a wzdłuż osi \vec{n}_{θ_a} . Jakie są możliwe wyniki pomiarów i odpowiadające im prawdopodobieństwa w dwu przypadkach: $\theta_a = 0$ (oś z) lub $\theta_a = \pi/2$ (oś x). Jak wyglądają stany cząstek $a \otimes b$ po dokonaniu przez Alicję w.w. pomiarów w zależności od otrzymanych wyników (tj. oś z wynik $\pm\hbar/2$, oś x wynik $\pm\hbar/2$)?

Po dokonanych przez Alicję pomiarze, Bolek mierzy składową spinu cząstki b wzdłuż osi \vec{n}_{θ_b} . Jakie są możliwe wyniki pomiarów Bolka i odpowiadające im prawdopodobieństwa w zależności od wyników otrzymanych przez Alicję? Kiedy Alicja i Bolek otrzymają z prawdopodobieństwem 1 ten sam wynik?

3. Rozważmy przypadek, kiedy $\theta_a = 0$. Przypuśćmy, że agent S, ukryty między źródłem a Bolkiem mierzy spin cząstki b wzdłuż osi n_{θ_s} . Jakie wyniki otrzyma agent S w zależności od wyników otrzymanych przez Alicję? Następnie po pomiarze dokonanym przez agenta S, Bolek mierzy spin b dla kąta $\theta_b = 0$. Jakie wyniki otrzymuje Bolek w zależności od wyników pomiarów agenta? Jakie są prawdopodobieństwa ich otrzymania?

Jakie jest prawdopodobieństwo $P(\theta_s)$, że Alicja i Bolek otrzymają te same rezultaty, po pomiarze dokonanym przez agenta S? Jaka jest wartość oczekiwana $P(\theta_s)$, jeżeli agent S wybiera kąt θ_s w sposób przypadkowy z przedziału $[0, 2\pi]$ z jednorodnym rozkładem prawdopodobieństwa? Jaka jest wartość oczekiwana $P(\theta_s)$, jeżeli agent S wybiera kąt $\theta_s = 0$ lub $\theta_s = \pi/2$ z prawdopodobieństwami $1/2$?

4. Aby przekazać poufną informację (informacja to sekwencja bitów $++--+\dots$) Alicja i Bolek przyjmują następującą procedurę:

- (a) Alicja i Bolek decydują najpierw, względem których osi dokonywać będą pomiarów (synchronizacja układów współrzędnych).
- (b) Alicja, która ma kontrolę nad źródłem Z , przygotowuje uporządkowaną sekwencję $N \gg n$ dwójek spinów w stanie (1) , gdzie n jest liczbą bitów w przesyłanej wiadomości. Alicja wysyła Bobowi cząstki b a sama zachowuje cząstki a .
- (c) Na każdej cząstce, która do nich dociera, Alicja i Bolek dokonują pomiaru składowej x lub z spinu. Każde z nich wybiera kierunek x lub z w sposób przypadkowy z prawdopodobieństwem $1/2$. Dla danej pary spinów (a, b) nie ma korelacji między wyborem osi przez Alicję i przez Bolka. Oboje zapisują otrzymane wyniki.
- (d) Bolek wybiera ułamek F z N dokonanych pomiarów. We wszystkich tych przypadkach przekazuje Alicji przez telefon oś pomiaru i jego wynik. W praktyce $F \sim 1/2$.
- (e) W wybranych przez Bolka przypadkach, Alicja porównuje swoje wyniki z wynikami Bolka i w ten sposób stwierdza, czy w proces przekazywania wiadomości wmieszał się agent S. Jeśli odkrywa agenta, to zawiadamia policję lub CBS, a proces przekazywania informacji zostaje zakończony. Jeżeli agent nie został wykryty to:
- (f) Alicja otwarcie przyznaje, że agenta nie było, a Bolek przekazuje jej przez telefon osie względem których mierzył spin w pozostałych przypadkach. Jednak nie podaje wyników pomiarów.
- (g)

Jak musi wyglądać punkt (g) aby dokonała się poufna transmisja informacji do Bolka bez dodatkowego wysyłania spinów (tj. tylko na podstawie sekwencji już wysłanych N spinów). Proszę skomentować skuteczność zaproponowanej procedury. Jak Alicja może stwierdzić obecność agenta? Jakie jest prawdopodobieństwo niewykrycia agenta (np. dla $FN = 200$)? Czy agent może się "zamaskować" jeśli zna usytuowanie osi wybranych przez Alicję i Bolka?