OSNOVE KVANTNEGA RAČUNALNIŠTVA, 2. DEL

MATIJA PRETNAR

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 68Q12, 81P68

V drugem delu članka si ogledamo Deutschev algoritem, ki je bil prvi kvantni algoritem, ter najznamenitejša kvantna algoritma: Groverjev algoritem za iskanje v neurejeni tabeli in Shorov algoritem za razcep na praštevila.

THE BASICS OF QUANTUM COMPUTING, PART 2

The second part looks at Deutsch's algorithm, which was the first quantum algorithm, and at two most famous quantum algorithms: Grover's search algorithm and Shor's factorization algorithm.

Simulacija klasičnih vezij

Preden se začnemo navduševati nad učinkovitostjo kvantnih računalnikov, najprej preverimo, ali lahko z njimi res izračunamo vse, kar bi želeli. Torej, za vsako funkcijo $f\colon \{0,1\}^m \to \{0,1\}^n$, ki jo znamo izračunati na običajnem računalniku, želimo poiskati ustrezno unitarno preslikavo oziroma kvantno vezje U_f, ki bo dajala enake odgovore.

Kaj pomeni, da bodo odgovori enaki? Če nastavimo kubite na začetno bazno stanje $|x\rangle = |x_0 x_1 \cdots x_{m-1}\rangle$, kjer so x_i posamezni vhodni biti, potem želimo s pomočjo U_f izračunati stanje $|f(x)\rangle = |y_0 y_1 \cdots y_{n-1}\rangle$. Toda kako lahko z unitarnimi preslikavami izračunamo funkcijo, ki nima inverza? Še več: kaj, če funkcija f nima enakega števila vhodnih in izhodnih bitov?

Obema težavama se izognemo tako, da vezje poleg vhoda $|x\rangle$ sprejme še nekaj dodatnih kubitov, na katere bomo shranili izhod $|f(x)\rangle$. Za začetek si oglejmo primer, ko f izračuna en bit, torej ko je $n = 1$. Vezje U_f tedaj iz stanja $|x\rangle|0\rangle$ izračuna stanje $|x\rangle|f(x)\rangle$. Natančneje: iz stanja $|x\rangle|b\rangle$ bomo izračunali stanje $|x\rangle|b \oplus f(x)\rangle$, kjer je *ekskluzivni ali* $\oplus$ podan z:

$$0 \oplus 0 = 0 \quad 0 \oplus 1 = 1 \quad 1 \oplus 0 = 1 \quad 1 \oplus 1 = 0.$$

Iz enakosti $\textsc{cnot}|x\rangle|b\rangle = |x\rangle|b \oplus x\rangle$ izvira tudi oznaka za CNOT v kvantnih vezjih.

Če je izhodnih kubitov več, ravnamo podobno: iz vhoda $|x\rangle|b\rangle$, kjer je b zdaj zaporedje n kubitov, enako izračunamo $|x\rangle|b \oplus f(x)\rangle$, le da tokrat $\oplus$ deluje po posameznih kubitih.