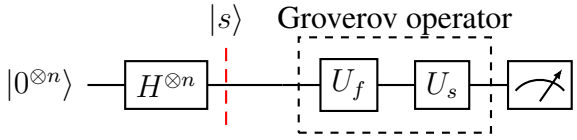
3.4. Groverov algoritam

3.4.1. Opis

Groverov algoritam[2] jedan je od algoritama koji je definirao principe kvantnih algoritama pretraživanja. U načelu, problem koji rješava jest pretraživanje nestrukturirane baze podataka. Klasično računalo taj problem rješava u prosječno $N/2$ koraka, dok kvantno računalo implementirajući Groverov algoritam pronađe rješenje s visokom vjerojatnošću u samo $\sqrt{N}$ koraka.

Definirati Groverov algoritam kao algoritam pretraživanja nestrukturirane baze podataka malo je zavaravajuće jer se u praktičnom smislu nikada ne bi mogao koristiti za točno to. Prikladnija primjena Groverovog algoritma bila bi pronalaženje inverza funkcije što čak i zvuči puno zanimljivijim i korisnijim. Jedna takva funkcija jest kriptografska funkcija sažetka. Groverov algoritam može pronaći kolizije takve funkcije u $\sqrt{N}$ koraka gdje je N veličina domene funkcije, što klasično računalo u načelu može izračunati samo grubom silom.

Kvantni logički krug Groverovog algoritma može se prikazati kao:



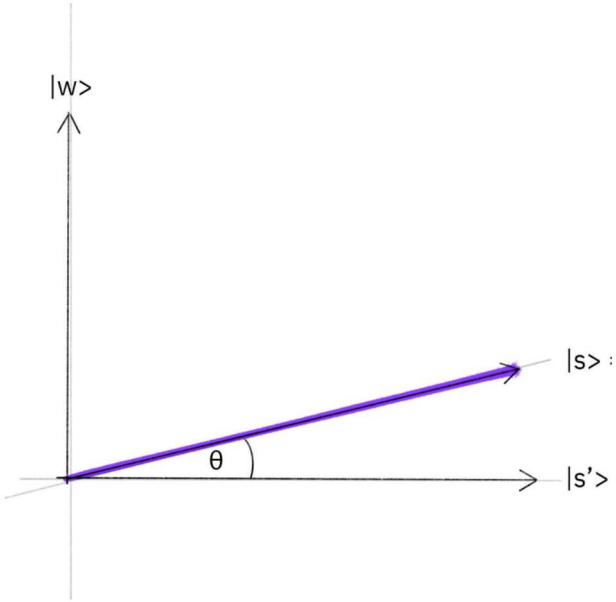
Slika 3.4: Kvantni logički krug Groverovog algoritma

Groverov operator potrebno je primijeniti $\sqrt{N}$ puta gdje je $N = 2^n$, a n broj kvantnih bitova. Sastoji se od kvantnog proroka (engl. *quantum oracle*) U_f i difuzera (engl. *diffuser*) U_s. Kvantni prorok je jedinična matrica koja na mjestu jednog ili više elemenata kojeg tražimo umjesto jedinice ima -1. Difuzer je operator koji provodi operaciju $2\left|s\right\rangle\left\langle s\right| - I_{2^n}$. Uzastopnim primjenjivanjem ovih operatora, stanje sustava se približava ciljnom stanju $|w\rangle$ koje želimo pronaći. Mjerenjem sustava nakon $\sqrt{N}$ primjena Groverovog operatora dobiva se traženi element s dovoljno velikom vjerojatnošću.

3.4.2. Analiza toka algoritma

Algoritam započinje kao i mnogi drugi, postavljanjem svih bitova u stanje superpozicije primjenom Hadamardovih operatora čime dobivamo stanje $|s\rangle$. Neka se traženo stanje zove $|w\rangle$ koji može biti ciljno stanje ili superpozicija ciljnih stanja ako ih ima

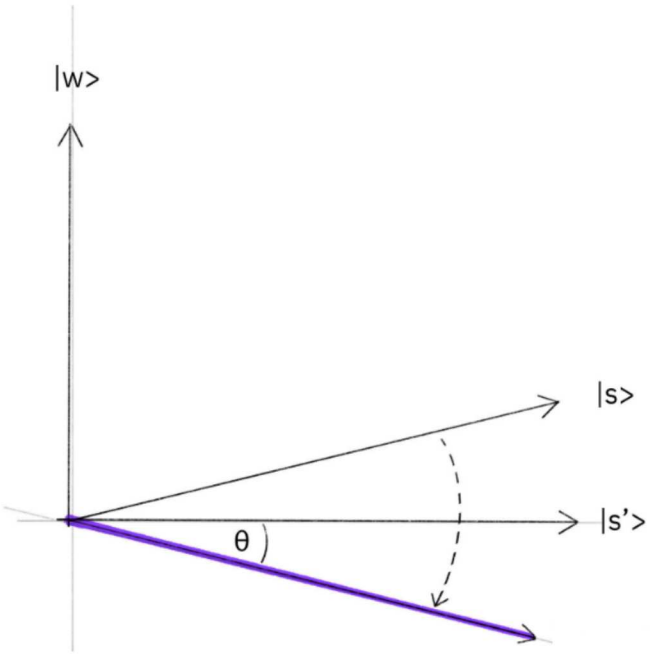
više. Neka se vektor stanja koji je okomit na stanje $|w\rangle$ zove $|s'\rangle$. Takvo stanje može se dobiti oduzimanjem stanja $|w\rangle$ od stanja $|s\rangle$ i normiranjem. Stanja $|w\rangle$, $|s\rangle$ i $|s'\rangle$ mogu se nacrtati u dvodimenzioalnom prostoru:



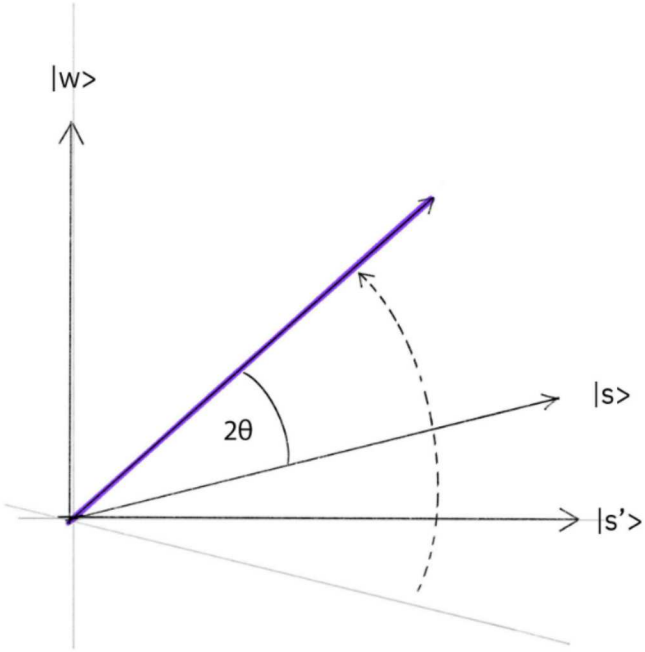
gdje kut θ opisuje koliko je stanje $|s\rangle$ zakrenuto prema $|w\rangle$. Za njega vrijedi:

$$\langle s|w\rangle = \frac{1}{\sqrt{N}} = \sin\theta \approx \theta$$

Idući korak algoritma primjenjuje kvantni prorok U_f na stanje $|s\rangle$. Sve što U_f radi jest refleksiju oko stanja $|s'\rangle$:



Zatim se primjenjuje difuzer U_s koji radi refleksiju oko stanja $|s\rangle$:



Dakle, nakon jedne primjene Groverovog operatora, stanje $|s\rangle$ se zaokrenulo za dodatnih 2θ prema ciljnom stanju $|w\rangle$. Nakon k primjena Groverovog operatora, stanje $|s\rangle$ biti će za $(2k+1)\theta$ zaokrenuto prema stanju $|w\rangle$. Cilj je da to bude što bliže stanju $|w\rangle$, dakle da vrijedi:

$$(2k+1)\theta \approx \frac{\pi}{2}$$

Rješavajući jednadžbu za k, dobiva se:

$$k \approx \frac{\pi}{4\theta} \approx \frac{\pi}{4}\sqrt{N} \approx \sqrt{N}$$

što znači da je potrebno primijeniti Groverov operator približno $\sqrt{N}$ puta kako bi vjerojatnost mjerenja stanja $|w\rangle$ bila najveća.

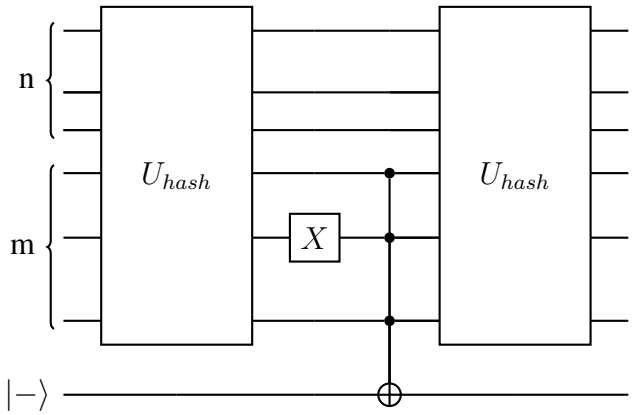
3.4.3. Kvantni prorok

Neka je U_f kvantni prorok Groverovog algoritma koji traži stanje $|10\rangle$. Njegova vrijednost iznosi:

$$U_f = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Čini se kao da je za samu izgradnju logičkog kruga odnosno proroka potrebno poznavati rješenje koje tražimo što poništava cijeli smisao Groverovog algoritma. To je donekle i istina; poznavanjem matrične reprezentacije proroka, moguće je odrediti ciljna stanja, ili obratno, za konstrukciju proroka na ovakav način, potrebno je poznavati ciljna stanja. Iz toga slijedi da je Groverov algoritam koristan jedino kada se prorok tretira kao crna kutija ili ako se prorok konstruira na način gdje njegova vrijednost nije očita, ali da i dalje daje ispravan rezultat. Takva konstrukcija proroka postiže se koristeći kvantni paralelizam i phase kickback.

Neka je f kriptografska funkcija sažetka za koju vrijedi $f : \{0,1\}^n \to \{0,1\}^m$ te neka je njoj potrebno pronaći inverz.



Slika 3.5: Kvantni prorok za pronalaženje inverza od $|101\rangle$

Za implementaciju kvantnog proroka potrebno je $n + m + 1$ kvantnih bitova od kojih su $m + 1$ pomoćni. Prvih n bitova se očekuje da su u stanju superpozicije, idućih m bitova se postavlja u stanje $|0\rangle$, dok se zadnji bit postavlja u stanje $|-\rangle$. Zatim je potrebno u kvantnom logičkom krugu implementirati samu funkciju f na način da će joj ulaz biti prvih n bitova, a izlaz idućih m bitova. Koristeći Toffolijeva vrata sa m upravljačkih bitova, može se odabrati izlaz funkcije kojemu je potrebno pronaći inverz (na slici je to $f(x) = 101$). Ciljni bit Toffolijevih vrata je poslijednji bit koji je u stanju $|-\rangle$. Svrha Toffolijevih vrata je svakoj komponenti stanja koja rezultira željenim izlazom promijeniti predznak. To radi koristeći phase kickback. Naime, vrijedi:

$$CNOT\,|0-\rangle = |0-\rangle$$

$$CNOT\,|1-\rangle = -\,|1-\rangle$$

Pošto se prorok koristi iterativno u algoritmu, potrebno je vratiti svih m izlaznih kvantnih bitova u stanje nule. Zbog reverzibilnosti svih operatora, potrebno je samo ponovno primijeniti funkciju f.