

Uvod do informatiky

Individualny projekt 1.

L^AT_EX

Kvantove pocitace

Ing. Juraj Stefanovic
PEVS Fakulta informatiky

Jan Ondis
PEVS Fakulta informatiky

October 22, 2021

1 Ako funguje kvantovy pocitac

Klasicke pocitace, koduju informacie v binarnych „bitoch”, ktore mozu mat hodnotu 0 s alebo 1 s. V kvantovom pocitaci je zakladnou jednotkou pamate kvantovy bit alebo qubit.

Prvy napad kvantoveho pocitaca bolo pridanie tretieho stavu pomocou magnetu. Kde magnet moze mat az tri stavy - pozitivny, negativny alebo ziaden. Neskor si ale ludia uvedomily, ze meranie udajov moze byt v akejkolvek forme. Dnes sa qubity sa vyrabaju pomocou fyzikalnych systemov, ako je spin elektronu alebo orientacia fotonu. Tieto systemy mozu byt v mnohych roznych usporiadaniach naraz, co je vlastnost znama ako kvantova superpozicia. Qubity mozu byt tiez neoddelitelne spojené pomocou javu nazyvaneho kvantove previazanie, kde 2 atomy vedia o sebe instantne, bez ohladu na ich poziciu vo vesmire. Takto vieme informacie prenasat a nie vysielat.

Napriklad osem bitov staci na to, aby klasicky pocitac reprezentoval akekolvek cislo medzi 0 a 255. Ale osem qubitov staci na to, aby kvantovy pocitac reprezentoval kazde cislo medzi 0 a 255 sucasne. Niekolko stoviek zapletenych qubitov by stacilo na to, aby predstavovali viac cisel, ako je atomov vo vesmire.

2 Kvantovy pocitac vs bezny pocitac

Kvantove pocitace spracovavaju informacie odlisne. Klasicke pocitace používajú tranzistory, ktore su bud 1 alebo 0. Kvantove pocitace používajú qubity, ktore mozu byt sucasne 1 alebo 0. Pocet prepojenych qubitov exponencialne zvyšuje kvantovy vypoctovy vykon. Medzitym prepojenie viacerých tranzistorov zvyšuje vykon iba linearne.

Klasicke pocitace su najvhodnejšie na kazdodenne ulohy, ktore je potrebne vykonat pomocou pocitaca. Medzitym su kvantove pocitace skvele na vykonavanie simulacii a analyz udajov, napríklad na chemicke alebo liekove testy. Tieto pocitace vsak musia byt velmi dobre chladene - omnoho viac ako bezne pocitace. Su tiez oveľa drahsie a narocnejšie na stavbu.

Klasicke vypoctove pokroky zahrnujú pridavanie pamate na zrychlenie pocitacov. Medzitym kvantove pocitace pomáhajú riesit komplikovanejšie problémy. Aj keď kvantove pocitace nemusia bezat v programe Microsoft Word lepsie alebo rychlejšie, mozu komplexnejšie problémy vykonavat rychlejšie.

- Sundar Pichai, CEO Microsoftu: 'Quantum computing and AI can solve the biggest problems.'

3 Prakticke vyuzitie kvantoveho pocitacu

Firma Google mina miliardy dolarov na svoj plan postavit svoj kvantovy pocitac do roku 2029. Spolocnost otvorila v Kalifornii kampus s nazvom Google AI, ktory jej ma pomoc splnit jej ciel. Google do tejto technologie investuje uz roky. Rovnako tak aj ine spolocnosti, ako napríklad Honeywell International (HON) a International Business Machine (IBM). IBM ockava, ze v nasledujucich rokoch dosiahne velke milniky v oblasti kvantovej vypoctovej techniky.

Zatial co niektore spolocnosti postavili osobne (hoci drahe) kvantove pocitace, na komercnej strane stale nie je nic dostupne. A je tu zaujem o kvantovu vypoctovu techniku a jej technologii, pricom JPMorgan Chase a Visa tuto technologii skumaju. Po vyvinuti by Google mohol spustit kvantovu vypoctovu sluzbu prostrednictvom cloudu.

Spolocnosti mozu tiez ziskat pristup ku kvantovej technologii bez toho, aby museli postavit kvantovy pocitac. IBM planuje do roku 2023 mat k dispozicii kvantovy pocitac s 1 000 qubitmi. IBM zatial umoznuje pristup k svojim pocitom, ak su sucastou jeho kvantovej siete. Medzi tie, ktore su sucastou siete, patria vyskumne organizacie, univerzity a laboratoria.

Microsoft tiez ponuka spolocnostiam pristup ku kvantovej technologii prostrednictvom platformy Azure Quantum. To je na rozdiel od Google, ktory nepredava pristup k svojim kvantovym pocitom.

Najpravdepodobnejsie vyuzitie kvantovych pocitacov:

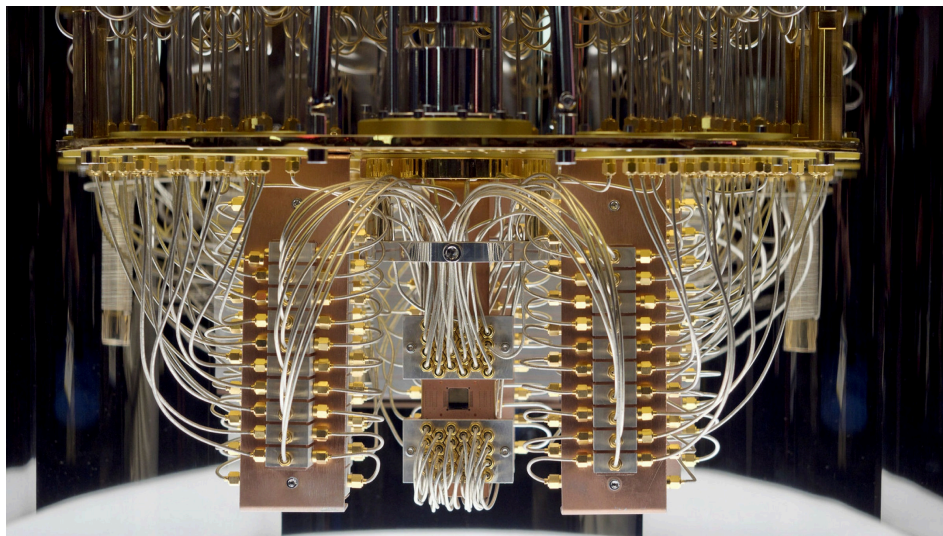
- Kyberneticka bezpecnost
- Vyvoj liekov
- Financie
- Vyvoj baterii
- Optimalizacia dopravy
- Predpoved pocasia a zmena klimy
- Umela inteligencia
- Objavovanie novych chemickych prvkov
- Vakciny
- Optimalizacia dodavatelskeho retazca

4 Kvantova nadradenost (quantum supremacy)

V roku 2012 profesor John Preskill vymyslel termin „kvantova nadradenost“, aby opisal bod, keď sa kvantové počítače stanú dostatočne výkonnými na to, aby vykonali nejakú výpočtovú úlohu, ktorú klasické počítače nedokázali urobiť v rozumnom časovom rámci. Zamerne nevyzadoval, aby výpočtová úloha bola užitočná. Kvantová nadvláda je prechodným milníkom, o ktorý sa treba usilovať dlho predtým, ako bude možné postaviť veľké kvantové počítače na všeobecné účely.

Google tvrdí, že preukázal niečo, čo sa nazýva „kvantova nadradenost“, v článku publikovanom [v Nature](#). To by znamenalo významný milník vo vývoji nového typu počítača, znameho ako kvantový počítač, ktorý by dokázal vykonať veľmi náročné výpočty oveľa rýchlejšie ako čokoľvek iné na bežných „klasických“ počítačoch. Ale tím z IBM zverejnil svoj vlastný dokument, v ktorom tvrdí, že dokáže reprodukovat výsledky Google na existujúcich superpočítačoch.

Zatiaľ čo Google verzus IBM môže byť dobrým príbehom, táto nehoda medzi dvoma najväčšími technologickými spoločnosťami na svete skor odvádza pozornosť od skutočného vedeckého a technologického pokroku, ktorý stojí za prácou oboch tímov. Napriek tomu, ako to môže znieť, ani prekročenie milníka kvantovej nadvlády by neznamenalo, že kvantové počítače sa chystajú prevziať kontrolu. Na druhej strane už len priblíženie sa k tomuto bodu má vzrúšujúce dôsledky pre budúcnosť technológie.



5 Zaver - kedy kvantove pocitace sa stanu beznymi pocitacmi

Pocitace boli kedysi povazovane za spickovu technologi, pristupnu iba vedcom a vyskolenym odbornikom. V druhej polovici 70. rokov vsak doslo v historii vypoctovej techniky k seizmickemu posunu. Nebolo to len tym, ze stroje sa stali oveľa mensimi a vykonnejšimi - aj ked, samozrejme, stali sa. Bol to posun v tom, kto bude pouzivat pocitace a kde, pretoze boli k dispozicii kazdemu na pouzitie vo vlastnom dome.

Dnes je kvantova vypoctova technika v plienkach. Kvantove vypocty zahrnuju niektore z najzaujimavejšich konceptov fyziky 20. storočia. V USA, Google, IBM a NASA experimentuju a stavaju prve kvantove pocitace. Čína tiež intenzívne investuje do kvantových technológií.

Verím, že dojde k analogickému posunu ku kvantovým pocitacom, kde sa nadsenci budú môcť hrať s kvantovými pocitacmi zo svojich domovov. A tento posun nastane oveľa skor, ako si väčšina ľudí uvedomuje.

Nemyslím si však, že by malo zmysel spekulovať o tom, čo bude väčšina ľudí robiť s kvantovými pocitacmi o 50 rokov. Možno by bolo zmysluplnejšie opýtať sa, kedy sa kvantova vypoctova technika stane niečím, čo môže ktokolvek pouzivať z vlastného domova.

Odpoveď je, že je to už možné. V roku 2016 spoločnosť IBM pridala do cloudu malý kvantový pocitac. Každý, kto má pripojenie na internet, môže na tomto pocitaci navrhnuť a spustiť svoje vlastné kvantové obvody. Kvantový obvod je sekvencia základných krokov, ktoré vykonávajú kvantový vypocet.

Kvantový pocitac IBM je nielen voľne použiteľný, ale tento kvantový pocitac má aj jednoduché grafické rozhranie. Je to malý, nie veľmi výkonný stroj - podobne ako prvé domáce pocitace - ale fanusikovia môžu začať hrať. Posun sa začal.

Ľudia vstupujú do veku, kedy je jednoduché učiť sa a experimentovať s kvantovými vypoctami. Rovnako ako pri prvých domácich pocitacoch nemusí byť jasné, že existujú problémy, ktoré je potrebné vyriešiť pomocou kvantových pocitacov, ale keď sa ľudia hrajú, je pravdepodobne, že zistia, že potrebujú viac energie a funkcií. Tým sa otvorí cesta pre nové aplikácie, ktoré sme si doteraz nevedeli predstaviť.