

Csikvári F. András:

A quantum komputerek majdani alkalmazásának korlátai

(Hozzászólás Kiss Károly: Közeleg a kvantum-kompjúterek korszaka c. írásához)

1. A mai számítógépek számítási kapacitásának elvi határai vannak. Lehetséges a gépek "méretét" valameddig növelni, de a gyorsaságát nem. A nagyon nagy számosságú elemek közti számítások nem lehetségesek (ilyenek például már az "egyszerű" kémiai problémák, de az atomfizikai problémák is tipikusan ilyenek). Ajánlott: <https://www.youtube.com/watch?v=yy6TV9Dntlw>
2. A titkosítások törlése valós veszély, de még nem akut probléma. A matematikusoknak és a rendszergazdáknak már most vannak javaslatai a módosításokra és még idő is bőven áll rendelkezésre.
3. Félrevezető a "chip" szó használata; a quantum computer nem a ma ismert chipekből épül fel, csak a vezérlő rendszerének bizonyos részei és az input-output eszközök bizonyos részei. A quantum computer "lelke" egy atomfizikai egység, ami sajnálatos módon csak 0 K fok közelében dolgozik jól, tehát nagy hűtési kapacitást igényel. (Valójában 15 miliKelvin alatt, ami hidegebb, mint az új hőmérséklete.) Ennek megfelelően egy igen nagy, energiafálgó berendezést kell elképzelnünk. Ajánlott: <https://www.youtube.com/watch?v=AQjKUN8PORM&t=17s>
4. A quantum computer tehát csak bizonyos helyeken, cégeknél lesz üzemeltethető. Ezek a cégek fognak gépidőt eladni a kutatóintézeteknek, de akár az egyszerű felhasználóknak is.
5. A számítási pontosság és annak ellenőrizhetősége már a hagyományos számítógépek elterjedésekor is kérdés volt, és már akkor lemondunk arról, hogy kézi számításokkal ellenőrizzük a gépet. Teljesen együtt tudunk élni ezzel a problémával, megismételt számításokat, módosított megközelítésű számításokat végzünk.
A quantum computereknél teljesen másképp vetődik fel ugyanez a probléma. Eleve többször kell majd ugyanazt a programot lefuttatni és a számítógép nem fogja minden alkalommal ugyanazt az eredményt adni a működés közben keletkező fizikai zajok (zavarások) miatt. Remélhetőleg – statisztikailag – a jó eredményt fogja a legtöbbször adni.
A quantum computer által adott eredményeket tehát szükséges ellenőrizni hagyományos számítógéppel. Meg kell érteni itt egy aszimmetriát: az adott feladatot a hagyományos számítógép ugyan nem tudja megoldani, de ha már megvan az eredmény, akkor annak a megfelelőségét igen. (Az érthetőség kedvéért egy példa: egy nagyon nagy számot nem tudunk szorzatokra bontani hagyományos számítógéppel, nem elvi okok, hanem időhiány miatt. Viszont ha tudjuk a szorzótényezőket, azokat össze tudjuk szorozni és meg tudjuk állapítani, hogy valóban azt a nagy számot kaptuk-e.)

Bp, 2023.06.11.