Alumne: Pol Cid Soria
Tutor: Albert Llamas Cano

Computació quàntica, una nova revolució?

Presentació

Vivim en un món en constant expansió i desenvolupament, i per tant és natural que la tecnologia i les eines de les quals disposem s'adaptin a les nostres necessitats cada vegada més exigents. Però quan les tècniques i models de què disposem avui en dia no siguin suficients, quins seran els nous principis sota els quals es fonamentarà el nostre futur? Sota aquesta pregunta vaig començar a plantejar-me quins eren aquests nous models, i entre ells va aparèixer la computació quàntica.

Quan vaig decidir explorar aquest tema vaig poder comprovar una cosa ràpidament, i és que la majoria de la població no tenia coneixement sobre aquest model, a diferència d'altres, com la intel·ligència artificial. Va ser a partir d'aquest punt, doncs, que van quedar clars els principals objectius del meu treball de recerca. En primer lloc volia investigar i entendre els principis darrere d'aquesta tecnologia per elaborar un treball on trobar explicats els seus punts més fonamentals amb el màxim rigor. En segon lloc, volia comprovar si aquesta tecnologia pot oferir grans avenços i millores en les nostres vides i, en cas afirmatiu, comprovar quins àmbits es veurien més beneficiats.

Metodologia

Per tal de dur a terme el treball l'he dividit en dues parts principals: una part teòrica i una part pràctica. La primera té com a objectiu explicar les bases i els principis darrere de la computació quàntica, així com l'estructura i funcionament dels algorismes i protocols quàntics més importants i famosos.

Per altra banda, la part pràctica té com a objectiu la programació i execució d'algorismes i protocols quàntics en ordinadors quàntics reals. Això últim m'ha estat possible al servei que ofereix IBM, anomenat IBM Quantum Experience. Aquest servei permet que l'usuari programi i dissenyi els seus propis circuits quàntics i que els executi tant en simuladors com en ordinadors quàntics reals repartits en diferents centres d'IBM ubicats en diferents llocs del món.

Cos del treball

Per tal de poder entendre de forma completa les bases de la computació quàntica primer cal explicar el seu element més simple: el qubit.

El qubit és la unitat mínima d'informació que empra la computació quàntica, i tot i ser anàloga al bit en computació clàssica, el qubit té una propietat molt especial: pot emmagatzemar valors en superposició. És a dir, mentre que un bit només és capaç d'emmagatzemar els valors 1 i 0, un qubit és capaç d'emmagatzemar valors que es trobin en superposicions entre els valors 1 i 0. No obstant, a l'hora de mesurar un qubit sempre es mesura un dels dos estats, 0 o 1, amb una probabilitat fixa i coneguda.

El següent element més important de la computació quàntica són les portes quàntiques, que efectuen diferents operacions sobre un grup determinat de qubits. Són anàlogues a les portes lògiques de la computació quàntica i, per tant, presenten algunes similituds amb algunes d'aquestes portes lògiques. La porta quàntica de Pauli-X, per exemple, seria anàloga a la porta lògica NOT, ja que quan el qubit es troba en els estats |0> o |1> aquest passa a tenir l'estat oposat. Entre les portes quàntiques més famoses trobem la porta de Hadamard, la porta CNOT i la porta SWAP. La primera porta, la de Hadamard, aplica un estat de superposició quan s'aplica en un qubit, és a dir, el qubit passa a estar d'un estat clàssic, com |0> o |1>, a un estat que serà mesurat com a |0> un 50 % de les vegades i |1> l'altre 50 % de les vegades. La següent porta, la CNOT, s'aplica sobre dos qubits i realitza l'operació següent: si el primer qubit, anomenat qubit de control, es troba en estat |1> llavors el segon qubit, anomenat qubit objectiu, passarà a tenir el valor oposat al que posseïa. És a dir, si es trobava en l'estat |0> passarà a l'estat |1>, i viceversa. Finalment, la porta SWAP es tracta de la porta quàntica més simple i més versàtil: permet intercanviar l'estat de dos qubits.

Per acabar caldria afegir que aplicar una porta de Hadamard sobre un qubit seguit d'una porta CNOT produeix un efecte molt interessant i curiós anomenat entrellaçament quàntic.

Mentre els dos qubits es troben sota aquest estat comparteixen una propietat: si un dels dos qubits és mesurat en qualsevol estat l'altre qubit serà mesurat en el mateix estat passi el que passi. Aquesta és una propietat molt important i útil que veurem en els circuits quàntics més endavant.
Finalment, l'element més complex de la computació quàntica són els circuits quàntics. Aquests circuits són la unió entre diferents combinacions de portes quàntiques juntament amb codi amb la finalitat de formar diferents algorismes i protocols. Aquests quatre són els que jo he programat i executat en aquest treball: el protocol de Superdense Coding, el protocol de teleportació quàntica, el protocol d'intercanvi de claus quàntiques i l'algorisme de Shor.
El primer protocol, el protocol de Superdense Coding, té com a objectiu enviar dos bits d'informació mitjançant un únic qubit. Prendrem com a exemple una situació en què una persona A (Alice) vol enviar dos bits d'informació a una persona B (Bob). Per poder fer-ho, primer cal que l'Alice posseeixi un parell de qubits i apliqui una porta de Hadamard i una porta CNOT per obtenir un estat d'entrellaçament quàntic, tal i com descrivíem anteriorment. Una vegada realitzada l'operació, només cal que l'Alice apliqui una porta quàntica diferent en funció del parell de bits que vulgui enviar i enviï els qubits a en Bob. Una vegada en Bob rep els qubits només ha de desfer l'entrellaçament aplicant una porta CNOT i una porta de Hadamard i, una vegada mesuri, trobarà els estats que va codificar l'Alice. D'aquesta manera s'aconsegueix codificar dos bits clàssics en un sol qubit.
El següent protocol, el protocol de teleportació quàntica, actua de manera molt similar a l'anterior protocol, però en aquest cas l'objectiu és transmetre l'estat d'un qubit mitjançant dos bits clàssics. Continuant amb l'exemple anterior en què dues persones, Alice i Bob, es volen comunicar, el primer pas és idèntic a l'anterior protocol: s'aplica una porta de Hadamard sobre un dels dos qubits i seguidament s'aplica una porta CNOT sobre els dos qubits. Una vegada s'assoleix l'estat d'entrellaçament i l'Alice disposa del qubit en què s'ha aplicat la porta de Hadamard i en Bob de l'altre qubit, el segon pas es pot iniciar. L'Alice ha d'aplicar una porta CNOT amb el seu qubit com a objectiu i amb el qubit amb l'estat que vol transmetre com a control. Seguidament, l'Alice mesura els estats d'aquests dos qubits i els envia a en Bob. Una vegada en Bob els rep, aquest aplica una porta quàntica sobre el seu qubit en funció dels bits que rebi, i d'aquesta manera el seu qubit tindrà finalment l'estat que l'Alice volia transmetre.
El protocol d'intercanvi de claus quàntiques és un dels protocols més importants, ja que introdueix conceptes que permeten establir canals de seguretat molt més robusts dels que disposem avui en dia. Fins ara hem explicat que els qubits es poden trobar en estats com |0> o |1> i superposicions entre aquest dos estats, però això no és del tot cert, ja que els qubits es poden trobar en superposicions amb altres estats.

Els estats |0> i |1> formen l'anomenada base Z, una de les moltes bases en què es pot mesurar, essent la base X, formada pels estats | + > i | − >, una altra base molt utilitzada. La propietat que permet el funcionament d'aquest protocol estableix que en mesurar un qubit en la mateixa base en què ha estat codificat es troba l'estat que ha estat codificat el 100 % de les vegades, però si es mesura en una base diferent d'aquella en la qual ha estat codificat el qubit, es mesurarà un dels estats de la base mesurada amb un 50 % de probabilitats cadascun.
D'aquesta manera, si l'Alice i en Bob s'envien una cadena de qubits i algú intenta interceptar els qubits, si resulta que mesura un dels qubits en la base equivocada, llavors deixarà la seva marca i alertarà l'Alice i en Bob.
L'últim circuit de tots, l'algorisme de Shor, és possiblement l'algorisme més famós i important de tots, principalment per ser una prova definitiva que la computació quàntica és àmpliament superior a la clàssica en certs àmbits, i perquè el problema que resol és de molta importància en el nostre món.
L'objectiu de l'algorisme de Shor és descompondre un nombre qualsevol en dos factors primers. Aquesta és una tasca que fins ara era considerada impossible de dur a terme per a nombres suficientment grans, però amb l'aparició de la computació quàntica i de l'algorisme de Shor s'ha demostrat que és possible. La importància d'aquest problema resideix en el fet que la criptografia de tot el món, el protocol RSA, partia d'aquesta mateixa suposició. No obstant, la tecnologia de la qual disposem avui en dia no és suficientment avançada per suposar un perill per a la seguretat.

Conclusions

En definitiva, és evident que la computació quàntica ofereix un munt de millores i possibilitats per al nostre futur, però tot i així hi ha certs aspectes que ens impedeixen aprofitar tot el seu potencial. La tecnologia de la qual disposem avui en dia no és suficientment avançada per dur a terme tots els experiments que es plantegen teòricament, només presenta millores per a una selecció concreta de problemes, és molt difícil escalar aquest model per a problemes més grans i tractar amb qubits és molt difícil degut a la seva fragilitat i la seva naturalesa quàntica. Tot i així, és evident que en els pròxims anys la computació quàntica rebrà un impuls que li permetrà innovar i millorar molts aspectes del nostre món.

Bibliografia i bibliografia web

– Sánchez, J. *Instrumentación y control básico de procesos*. Ediciones Díaz de Santos, 2013. – Tinder, Richard F. *Engineering Digital Design: Revised Second Edition*. Elsevier, 2000. – Nielsen, Michael A.; Chuang, Isaac L. «Quantum computation and quantum information». *Phys. Today*, 2001, vol. 54, no 2, p. 60. – *C/CS/Phys191: Qubits, Quantum Mechanics and Computers* [seminari universitari]. Birgitta Wha-

ley. Berkeley, Universitat de California, 2009. – McMahon, D. *Quantum Computing Explained*. John Wiley & Sons, Inc. Hoboken, 2008. – Asfaw, Abraham, *et al*. Learn quantum computation using qiskit. 2020. A Course in Quantum Computing [seminari universitari]. Michael Loceff. Los Altos Hills, Foothill College, 2015. – Rieffel, Eleanor; Polak, Wolfgang. «An introduction to quantum computing for non-physicists». *ACM Computing Surveys* (CSUR), 2000, vol. 32, núm. 3. – Julián Pérez Porto i María Merino (2012). Definició formal de bit. [Consulta: 10 de novembre de 2020]. <http://definicion.de/bit/> – Quantiki, quantum information portal and wiki (26 d'octubre de 2015). Explicació i definició de l'esfera de Bloch. [Consulta: 23 de setembre de 2020]. <https://www.quantiki.org/wiki/bloch-sphere> – Quantiki, quantum information portal and wiki (26 d'octubre de 2015). Explicació del protocol d'intercanvi de Claus quàntiques. [Consulta: 15 de novembre de 2020]. <https://www.quantiki.org/wiki/quantum-key-distribution>