Introducció a la computació quàntica

Javier García

Departament de Física, Universitat de Girona

El 1985 David Deustch va crear el primer algoritme quàntic, on es demostrava clarament la potència de càlcul de la mecànica quàntica. Deu anys més tard, Peter Shor de AT&T Bell Laboratories va marcar un abans i un després en aquest camp, en definir l'algoritme que porta el seu nom i que permet calcular els factors primers d'un nombre donat, a una velocitat exponencialment més gran que en qualsevol ordinador tradicional, de manera que el seu algoritme permet trencar molts dels sistemes de criptografia utilitzats actualment.

El pas del bit "clàssic" al bit "quàntic" (combinació lineal dels estats 0 i 1) obre noves perspectives a la computació basades en les propietats de la mecànica quàntica. Un algorisme quàntic el podem imaginar com un algoritme clàssic, però ara les dades estan construïdes a partir de bits quàntics (vectors) i les instruccions són matrius. Al passar les dades per aquestes matrius es transformen, I així successivament, fins a obtenir l'estat final. L'algoritme ha de ser prou hàbil per tal de produir un estat que al ser observat ens doni la informació necessària per resoldre el problema.

En aquesta xerrada s'introduirà el concepte de quantum bit, l'algoritme de cerca de Grover (en què Google està treballant en l'actualitat amb l'empresa D-Wave) i el de factorització de Shor. Així com una introducció a l'algoritme d'estimació de fase que és la peça clau a l'hora de calcular les autoenergies d'un hamiltonià molecular en un ordinador quàntic.