A XVIII-a Conferință internațională – multidisciplinară
„Profesorul Dorin Pavel – fondatorul hidroenergeticii românești”
CLUJ NAPOCA, 2018

PORȚI CUANTICE

George MAHALU

QUANTUM GATES

Classic logic gates are not reversible in the sense that after a logical operation, it is not possible to reconstitute the input states of the recorded output. For this reason, it is considered that the classical computation process is one with increasing entropy (loss of information), which, together with well-known classical physical thermodynamics, will introduce a new field of study, referring to the so-called information thermodynamics.

Keywords: quantum gate, qubit, informational thermodynamics
Cuvinte cheie: poartă cuantică, qubit, termodinamică informațională

1. Introducere

Apariția computerului cuantic a adus cu sine conceptul de *calcul cuantic*, precum și pe cel de *algoritm cuantic*. Un rol esențial în definirea noii tehnologii îl dețin *porțile cuantice*. Acestea constituie echivalentul porților clasice ce structurează computerul cu care lucrăm în mod curent. În continuare se prezintă câteva dintre cele mai reprezentative porți cuantice.

2. Porți cuantice reversibile

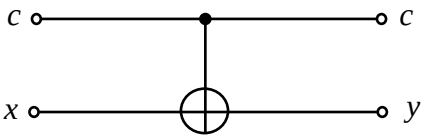
Calculatoarele cuantice utilizează porţi logice reversibile pentru a implementa algoritmi cuantici. Este posibil ca orice poartă logică clasică să fie simulată cu porţi reversibile. De exemplu, aşa cum se va putea

observa ulterior, o poartă reversibilă *NAND* poate fi realizată dintr-o poartă reversibilă *Toffoli*.

Porţile reversibile utilizează *linii de control* care, în circuitele reversibile, pot fi legate pe biţii (qubiţii) auxiliari, aleşi dintre biţii (qubiţii) de lucru. Liniile de control asigură necesarul de biţi (qubiţi) care să permită reconstituirea stării intrării din starea ieşirii.

2.1. Poarta CNOT (Controlled NOT)

Denumirea în limba română ar fi cea de *poartă inversoare controlată*. Spre deosebite de cazul clasic al porţii *NOT*, sunt prevăzute două linii de intrare, notate c şi respectiv x.



c	*x*	*y*
0	*0*	*0*
0	*1*	*1*
1	*0*	*1*
1	*1*	*0*

Fig. 1 Poarta *CNOT*

În figura 1 este prezentată schema de principiu a porţii şi tabelul său de adevăr. Ieşirile porţii sunt notate cu c şi respectiv y.

Se observă că poarta *CNOT* prezintă ca linie de control linia c, aceasta constituind şi linie de ieşire. Linia de lucru este linia x. Ieşirea y se exprimă în acest caz ca rezultat al operaţiei $c \; XOR \; x$.

Se poate remarca principala proprietate a porţii *CNOT*: dacă $c = 0 \;\; \Rightarrow \;\; y = x$ iar dacă $c = 1 \;\; \Rightarrow \;\; y = \bar{x}$.

În conformitate cu această observaţie, se constată că pentru poarta *CNOT* denumirea de *poartă repetoare controlată* poate fi uneori la fel de validă.

Proprietate:

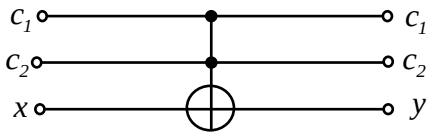
Pentru $x = 0 \;\; \Rightarrow \;\; y = c$ *iar pentru* $x = 1 \;\; \Rightarrow \;\; y = \bar{c}$.

Observaţie:

Conform proprietăţii de mai sus, poarta CNOT este simetrică, linia de intrare şi cea de control fiind echivalente din punctul de vedere al ieşirii y *. Din punctul de vedere al vectorului de ieşire* $\begin{bmatrix} c \\ y \end{bmatrix}$ *însă, echivalenţa nu mai subzistă.*

2.2. Poarta Toffoli

Este numită şi *poarta inversoare dublu comandată* (controlled-controlled *NOT* – C^2NOT). Schema de principiu şi tabelul de adevăr sunt prezentate în figura 2.



c_1	c_2	x	y
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Fig. 2 Poarta *Toffoli*

Se observă că poarta operează conform operatorului *NOT*, furnizând în ieşirea y starea inversată de pe linia de intrare x, doar în situaţia în care pe ambele linii de control starea este 1 logic. Altfel, ieşirea copie starea din intrare.

Proprietăţi:

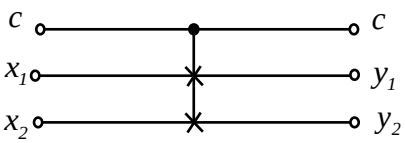
$$T_F(c_1,c_2,x)=(c_1,c_2,x\ XOR\ (c_1\ AND\ c_2))$$
$$T_F(1,1,x)=(1,1,NOT\ x)$$
$$T_F(a,b,1)=(a,b,a\ NAND\ b)$$
$$T_F(a,b,0)=(a,b,a\ AND\ b)$$
$$T_F(a,1,0)=(a,1,a)$$

2.3. Poarta Fredkin

Acest tip de poartă deţine o singură linie de control şi două linii de date. Schema de principiu şi tabelul de adevăr sunt prezentate în figura 3.

Proprietăţi:

$$F_R(c,0,x_2) = (c, c\ AND\ x_2, \bar{c}\ AND\ x_2)$$
$$F_R(1,x_1,x_2) = (1, x_2, x_1)$$
$$F_R(c,1,0) = (c, \bar{c}, c)$$



c	x_1	x_2	y_1	y_2
0	0	0	0	0
0	0	1	0	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	0
1	0	1	1	0
1	1	0	0	1
1	1	1	1	1

Fig. 3 Poarta *Fredkin*

3. Algoritmi cuantici

După cum s-a văzut, capacitatea unui calculator cuantic este datorată paralelismului cuantic asociat cu principiul de superpoziţie. Aceasta înseamnă că un calculator cuantic poate procesa un număr mare de intrări clasice într-o singură rulare.

Problema o constituie extragerea informaţiei utile din starea de ieşire (finală). Această informaţie este, într-un anumit sens, ascunsă. Rezultatul unui proces de măsurare este inerent probabilistic şi probabilităţile diferitelor stări de ieşire posibile sunt determinate de postulatele de bază ale mecanicii cuantice. În prezent, există totuşi algoritmi cuantici eficienţi care permit extragerea informaţiei utile.

Unul dintre algoritmii cuantici a fost propus de Peter Shor [3] în anul 1994 şi el rezolvă eficient problema descompunerii în factori primi: dat fiind un număr N impar întreg şi pozitiv, să se găsească factorii primi în care el poate fi descompus.

Aceasta este o problemă centrală în ştiinţa calculatoarelor şi se afirmă, deşi nu s-a demonstrat, că folosind un calculator clasic este

dificil să se găsească factorii primi pentru un număr *N* dat. Algoritmul lui Shor rezolvă eficient problema factorizării unui număr întreg prin creşterea considerabilă a vitezei de calcul. Trebuie menţionat că există în prezent sisteme de codificare (cryptographic systems), cum ar fi RSA, bazate pe faptul că nu există algoritmi eficienţi pentru rezolvarea problemei descompunerii în factori primi. Deci, algoritmul Shor implementat pe un calculator cuantic va înlocui actualul sistem de codificare RSA.

Au fost realizaţi şi alţi algoritmi cuantici care prezintă avantaje faţă de cei clasici. Astfel, L. Grover a arătat că folosind calculatorul cuantic se poate rezolva uşor problema găsirii unui anumit obiect într-o bază de date care conţine $N = 2^n$ obiecte [4]. Cu un calculator clasic, ceea ce se poate face este să se parcurgă baza de date până ce se găseşte obiectul respectiv. Această cale va necesita deci un maxim de 2^n operaţii. În schimb, folosind calculatorul cuantic problema va putea fi rezolvată în n operaţii.

O a treia clasă de probleme importante privind algoritmii cuantici o constituie cea a simulării sistemelor fizice. De exemplu, se ştie că simularea unui sistem cuantic compus din mai multe particule aflate în interacţiune pe un calculator clasic este foarte dificilă deoarece dimensiunea spaţiului Hilbert al stărilor acestui sistem creşte exponenţial cu numărul de particule. Astfel, pentru un lanţ uni-dimensional compus din *n* particule cu spinul *1/2*, dimensiunea acestui spaţiu este 2^n şi deci o stare posibilă a sistemului respectiv este determinată de 2^n numere complexe. În schimb, cu un calculator cuantic creşterea de memorie necesară este proporţională cu numărul *n* de particule şi este necesară o bază compusă numai din *n* qubiţi. Ca urmare, un calculator cuantic operând pe un registru compus din câteva zeci de qubiţi poate depăşi în performanţă orice calculator clasic actual. Desigur, această afirmaţie este adevărată numai dacă se pot realiza algoritmi cuantici eficienţi pentru extragerea informaţiei utile din calculatorul cuantic. Este foarte interesant de observat că un calculator cuantic poate fi folosit nu numai pentru studiul proprietăţilor sistemelor multi-particulă dar şi pentru determinarea dinamicii sistemelor clasice şi cuantice complexe [5].

4. Concluzii

■ Porțile logice clasice nu sunt reversibile, în sensul că după efectuarea unei operații logice, de regulă nu se mai pot reconstitui

stările intrărilor conforme cu ieșirea înregistrată. Din acest motiv se consideră că procesul de calcul clasic este unul cu creștere de entropie (pierdere de informație), fapt care face ca alături de termodinamica clasică fizică bine cunoscută, să apară un nou domeniu de studiu ținând de o așa numită *termodinamică informațională*.

■ În contrast, porțile cuantice sunt (și trebuie prin necesitate să fie) reversibile. Chiar și prin intermediul acestui aspect subsidiar se poate resimți puterea sporită de operare a sistemelor cuantice comparativ cu cele clasice.

■ Porțile cuantice constituie elementele de bază în configurarea oricărui computer cuantic, fapt ce le face demne de studiat și înțeles în cele mai puțin intuitive aspecte ale lor.

BIBLIOGRAFIE

[1] Benenti, G., Casati, G. and Strini, G., *Principles of Quantum Computation and Information,* Vol. IV Basic Concepts (World Scientific, Singapore 2004).

[2] Nielsen, M.A. and Chuang, I.L., *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[3] Perry, R.T., *The Temple of Quantum Computing*, Merlot Program California State University, 2004.

[4] Williams, C.P., *Explorations in Quantum Computing*, Hardcover Printing, http://www.springer.com/978-1-84628-886-9, 2011.

[5] Takahashi, Y., Tani, S., and Kunihiro, N., *Quantum addition circuits and unbounded fan-out*, Quantum Info. Comput., vol. 10, pp. 872{890, Sept. 2010.

Conf.Dr.Ing. George MAHALU
Universitatea ”Ștefan cel Mare” Suceava
Departamentul de Calculatoare, Electronică și Automatică
Membru AGIR
e-mail: mahalu@eed.usv.ro