Quantum Computing based on Tensor Products
Overview and Introduction

Guillermo Morales Luna

Computer Science Section
CINVESTAV-IPN

E-mail: gmorales@cs.cinvestav.mx

5-th International Workshop on Applied Category Theory
Graph-Operad Logic

Agenda

Agenda

Abstract

We present a short introduction to Quantum Computing (QC) from a procedural point of view. Rather, it is a course of “parallel computing based on tensor products”. We introduce primitive functions and the compositional schemes of QC. We use Tensor Product notation instead of the more conventional Dirac’s ket notation. We introduce basic notions of Tensor Products and Hilbert Spaces and the qubits as points in the unit circle in the two-dimensional complex Hilbert space, then any word consisting of qubits lies in the corresponding unit sphere of the tensor product of these spaces. We illustrate the computing paradigm through the classical Deutsch-Josza algorithm. Then we show the quantum algorithm to compute the Discrete Fourier Transform in linear time and the famous polynomial-time Shor algorithm for integer factorization. We finish our exposition with a basic introduction to Quantum Cryptography and Quantum Communication Complexity.

Agenda

Overview of the whole course

Contents

Agenda

General references

Quantum Computing

- D. Bouwmeester, A. K. Ekert, and A. Zeilinger. *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer, Berlin, 2000.
- G. Brassard. Quantum communication complexity (a survey), 2001.
- G. Brassard, I. Chuang, S. Lloyds, and C. Monroe. Quantum computing. *Proc. Natl. Acad. Sci. USA*, 95:11032–11033, Sept. 1998.
- M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

Physics and Math

- R. Abraham, J. E. Marsden, and T. Ratiu. *Manifolds, Tensor Analysis, and Applications*. Springer-Verlag, Berlin, 1998.
- J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.
- S. Lang. *Algebra, 4-th Edition*. Springer-Verlag, Berlin, 2004.

Special topics

Classics

- D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London Ser. A*, 400:96–117, 1985.
- D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London Ser. A*, 439:553–558, 1992.
- A. S. Holevo. Some estimates of the information transmitted by a quantum communication channel. *Probl. Peredachi Inf.*, 9:3, 1973. Also Probl. Inf. Transm. (USSR) 9, 177 (1973).
- P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994.
- P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.

Algorithmics and Crypto

- T. Hogg. Solving highly constrained search problems with quantum computers. *Journal of Artificial Intelligence Research*, 10:39–66, 1999.
- C. Lavor, L. Manssur, and R. Portugal. Shor's algorithm for factoring large integers. Mar. 2003.
- S. J. Lomonaco. A Quick Glance at Quantum Cryptography. *Cryptologia*, 23:1–41, 1999.
- S. J. Lomonaco. A Talk on Quantum Cryptography or How Alice Outwits Eve. `arXiv: quant-ph/0102016v1`, 2001.

Quantum complexity

- E. Bernstein and U. Vasirani. Quantum complexity theory. In *Proc. of the 25-th Annual ACM Symposium on Theory of Computing*, AIP Conference Proceedings. Association of Computing Machinery, 1993.
- R. Cleve. An introduction to quantum complexity theory, 1999.

Entanglement

- G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Phys. Rev. Lett.*, 83:1874–1877, 1999.
- H. Buhrman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. *SIAM J. Comp.*, 30(6):1829–1841, March 2001.
- S. Massar, D. Bacon, N. Cerf, and R. Cleve. Classical simulation of quantum entanglement without local hidden variables. *Phys. Rev. A*, 63:52305, 2001.

Agenda

Basic notions

Complex field. $\mathbb{C}$

Vector space. $\mathbb{H}$: Non-empty set. $\mathbf{0} \in \mathbb{H}$

Addition. $+ : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$. $(\mathbb{H}, +)$ Abelian group

Scalar multiplication. $\cdot : \mathbb{C} \times \mathbb{H} \to \mathbb{H}$. Distributive w.r.t. addition

Inner product. $\langle\cdot|\cdot\rangle : \mathbb{H} \times \mathbb{H} \to \mathbb{C}$. Sesquilinear form. Positive definite.

Norm. $||\cdot||_2 : \mathbb{H} \to \mathbb{R}^+$, $\mathbf{x} \mapsto ||\cdot||_2 = \sqrt{\langle \mathbf{x}|\mathbf{x}\rangle}$.

Completeness. Every Cauchy sequence is convergent.

Autoduality. For each $T \in \mathbb{H}^*$ exists $\mathbf{y} \in \mathbb{H}$: $T(\mathbf{x}) = \langle \mathbf{y}|\mathbf{x}\rangle$.

Geometrical properties: m-dimensional Hilbert spaces

Canonical basis. $\mathbf{e}_j = (\delta_{ij})_{i<m}$

Unit sphere. $E_m = \{\mathbf{v} \in \mathbb{H} | 1 = \mathbf{v}^H \mathbf{v} =: \langle \mathbf{v} | \mathbf{v} \rangle\}$

Unitary map. $U : \mathbb{H} \to \mathbb{H}$ linear s.t. $M^H M = \mathbf{1}_{mm}$. $U|_{E_m} : E_m \to E_m$

Tensor products

Spaces. $\dim(\mathbb{U}) = n$ & $\dim(\mathbb{V}) = m \;\Rightarrow\; \dim(\mathbb{U} \otimes \mathbb{V}) = nm$.
$\mathbb{U} \times \mathbb{V} \subset \mathbb{U} \otimes \mathbb{V}$. The difference consists of *entangled states*.

Vectors. $\mathbf{x} \in \mathbb{U}$ & $\mathbf{y} \in \mathbb{V} \;\Rightarrow\; \mathbf{x} \otimes \mathbf{y} \in \mathbb{U} \otimes \mathbb{V}$.

Maps. $S : \mathbb{U}_1 \to \mathbb{V}_1$ & $T : \mathbb{U}_2 \to \mathbb{V}_2 \;\Rightarrow\; S \otimes T : \mathbb{U}_1 \otimes \mathbb{U}_2 \to \mathbb{V}_1 \otimes \mathbb{V}_2$.

In current state

$$\mathbf{v} = (v_{i1})_{i<m} = \sum_{i=0}^{m-1} \in E_m,$$

for each $i < m$, with probability $|v_{i1}|^2$ the following is performed:

- The index i is output and
- the computing control is transferred to the state $\mathbf{e}_i$.

Spaces and basis

- $\mathbb{H}_1 = \mathbb{C}^2$; $\mathbb{H}_n = \mathbb{H}_{n-1} \otimes \mathbb{H}_1$
- $\dim(\mathbb{H}_n) = 2^n$
- $\mathbf{e}_0 = [1 \ \ 0]^T$ and $\mathbf{e}_1 = [0 \ \ 1]^T$ basis in $\mathbb{H}_1$.
- $(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0})_{\varepsilon_{n-1},\ldots,\varepsilon_1,\varepsilon_0\in\{0,1\}}$ basis in $\mathbb{H}_n$.

Qubits. $\mathbf{z} \in E_2$ unit sphere in $\mathbb{H}_1$.

Quregister. $\mathbf{z}_1 \otimes \cdots \otimes \mathbf{z}_{n-1} \ \Longleftarrow\ \mathbf{z}_i$, $i \in \mathbb{N}$, qubits

$\mathbf{z}_1 \otimes \cdots \otimes \mathbf{z}_{n-1} \in E_{2^n} \subset \mathbb{H}_n$

Conventional Dirac's "ket" notation

$$\begin{aligned} |\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0\rangle &:= \mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0} \\ &= \mathbf{e}_{\varepsilon_{n-1}}\otimes\cdots\otimes\mathbf{e}_{\varepsilon_1}\otimes\mathbf{e}_{\varepsilon_0} \\ &=: |\varepsilon_{n-1}\rangle\cdots|\varepsilon_1\rangle|\varepsilon_0\rangle \end{aligned} \quad (1)$$

Any state in $\mathbb{H}_n$, $\sigma(\mathbf{z}) = \sum_{\varepsilon\in\{0,1\}^n} z_{\varepsilon}\mathbf{e}_{\varepsilon}$ is determined by 2^n coordinates. If $U : \mathbb{H}_n \to \mathbb{H}_n$ is a quantum operator, the target state $\sigma(U\mathbf{z})$ consists also of 2^n coordinates.

A calculus involving an exponential number of terms is performed in just "one step" of the quantum computation.

Agenda

Function Evaluation

- $V = \{0, 1\}$: binary digits
- Each index in the set $\{0, \ldots, 2^n - 1\}$ corresponds to a string $\varepsilon = (\varepsilon_{n-1}, \ldots, \varepsilon_1, \varepsilon_0) \in V^n$ which in turn corresponds to $\mathbf{e}_{\boldsymbol{\varepsilon}} \in \mathbb{H}_n$.

Let $f : V^n \to V^m$ be a function.

A quantum algorithm $U_f : \mathbb{H}_{n+m} \to \mathbb{H}_{n+m}$ computes f if

$$U_f : \mathbf{e}_{\boldsymbol{\varepsilon}} \otimes \mathbf{0} \mapsto \mathbf{e}_{\boldsymbol{\varepsilon}} \otimes \epsilon \mathbf{e}_{f(\boldsymbol{\varepsilon})}$$

where $|\epsilon| = 1$. A final measurement on last qubits provides the value $f(\boldsymbol{\varepsilon})$, with probability 1.

Agenda

Let $V = \{0, 1\}$ be the set of classical truth values.

Deutsch-Jozsa's problem

Decide, for a given $f : V \to V$, whether it is constant or balanced "in just one computing step".

Given f, let U_f be the $2^2 \times 2^2$-matrix s.t. $U_f(\mathbf{e}_x \otimes \mathbf{e}_z) = (\mathbf{e}_x \otimes \mathbf{e}_{(z+f(x)) \bmod 2})$.
We have $H_2 U_f H_2 : \mathbf{e}_0 \otimes \mathbf{e}_1 \mapsto \varepsilon \mathbf{e}_S \otimes \mathbf{e}_1$
where H_2 is Hadamard's operator, $\varepsilon \in \{-1, 1\}$ is a sign and S is a signal indicating whether f is balanced or not.
S coincides with $f(0) \oplus f(1)$.

Agenda

Quantum Computation of the Discrete Fourier Transform

Given $\mathbf{f} = \sum_{j=0}^{n-1} f(j)\mathbf{e}_j \in \mathbb{C}^n$, its discrete Fourier transform is

$$\mathrm{DFT}(\mathbf{f}) = \hat{\mathbf{f}} = \sum_{j=0}^{n-1} \left[\frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp\left(\frac{2\pi ijk}{n}\right) f(k) \right] \mathbf{e}_j \in \mathbb{C}^n.$$

DFT is linear transform and, w.r.t. the canonical basis, it is represented by the unitary matrix $\mathrm{DFT} = \frac{1}{\sqrt{n}} \left(\exp\left(\frac{2\pi ijk}{n}\right)\right)_{jk}$

If $n = 2^\nu$, $\mathbb{H}_\nu = \mathbb{C}^n$, and by identifying each $j \in [\![0, 2^\nu - 1]\!]$ with $\varepsilon_j = \varepsilon_{j,\nu-1} \cdots \varepsilon_{j,1}\varepsilon_{j,0}$:

$$\begin{aligned} \mathrm{DFT}(\mathbf{e}_{\varepsilon_j}) &= \bigotimes_{k=0}^{\nu-1} \frac{1}{\sqrt{2}}\left(\mathbf{e}_0 + \exp\left(\frac{\pi i j}{2^k}\right)\mathbf{e}_1\right) \\ &= \tfrac{1}{\sqrt{2}}\left(\mathbf{e}_0+\exp\left(\tfrac{\pi i j}{2^0}\right)\mathbf{e}_1\right)\otimes\tfrac{1}{\sqrt{2}}\left(\mathbf{e}_0+\exp\left(\tfrac{\pi i j}{2^1}\right)\mathbf{e}_1\right)\otimes\cdots\otimes\tfrac{1}{\sqrt{2}}\left(\mathbf{e}_0+\exp\left(\tfrac{\pi i j}{2^{\nu-1}}\right)\mathbf{e}_1\right) \quad (2) \end{aligned}$$

The products appearing in this tensor product suggest the operators $Q_k : \mathbb{H}_1 \to \mathbb{H}_1$ and their “controlled” versions:

$$Q_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{\pi i}{2^k}\right) \end{bmatrix} \ , \ Q_{kj}^c = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\pi i \frac{j}{2^k}\right) \end{bmatrix}.$$

Algorithm for the Fourier transform

Input. $n = 2^\nu$, $\mathbf{f} \in \mathbb{C}^n = \mathbb{H}_\nu$.

Output. $\hat{\mathbf{f}} = \mathrm{DFT}(\mathbf{f}) \in \mathbb{H}_\nu$.

Procedure $\mathtt{DFT}(n, \mathbf{f})$

1. Let $\mathbf{x}_0 := H(\mathbf{e}_0)$.
2. For each $j \in [\![0, 2^\nu - 1]\!]$, or equivalently, for each $(\varepsilon_{j,\nu-1} \cdots \varepsilon_{j,1}\varepsilon_{j,0}) \in \{0,1\}^\nu$, do (in parallel):
   1. For each $k \in [\![0, \nu - 1]\!]$ do (in parallel):
      1. Let $\delta := R_k\left(\varepsilon_j\big|_k\right)$ be the reverse of the chain consisting of the $(k+1)$ less significant bits.
      2. Let $\mathbf{y}_{jk} := \mathbf{x}_0$.
      3. For $\ell = 0$ to k do { $\mathbf{y}_{jk} := Q^{c2}(\mathbf{y}_{jk}, \mathbf{e}_{\delta_{j,\ell}})$ }
   2. Let $\mathbf{y}_j := \mathbf{y}_{j0} \otimes \cdots \otimes \mathbf{y}_{j,\nu-1}$.
3. Output as result $\hat{\mathbf{f}} = \sum_{j=0}^{2^\nu-1} f_j \mathbf{y}_j$.

Agenda

Let n be an integer to be factored

1. Select an integer m such that $1 < m < n$.
2. If $\gcd(n, m) = d > 1$, then d is a non-trivial factor of n.
3. Otherwise, m is in the multiplicative group of remainders of n.
    1. If m has an even order r, then $k = m^{\frac{r}{2}}$ will be such that $k^2 = 1 \bmod n$, and $(k-1)(k+1) = 0 \bmod n$.
    2. By calculating $\gcd(n, k-1)$ and $\gcd(n, k+1)$, one gets non-trivial factors of n.

Biggest problem

Calculate the order of a current element m in $\Phi(n)$

Let $\nu = \lceil \log_2 n \rceil$, ν is the size of n.
$O(n) = O(2^\nu)$, thus an exhaustive procedure has exponential complexity with respect to the input size. Shor's algorithm is based over a polynomial-time procedure in ν to calculate the order of an element.

Agenda

Quantum Cryptography: Key Agreement Protocols

Two entities, Alice and Bob, should agree in private a common key.
They may use two transmission channels

Quantum channel Transmits just one-way, say from Alice to Bob.

Classical channel Transmits bidirectionally.

We will present the BB84 Protocol, without and with noise.

$E^0 = \{\mathbf{e}_0^0 = (1,0), \mathbf{e}_1^0 = (0,1)\}$: canonical basis of $\mathbb{H}_1$
$H(E^0) = E^1 = \{\mathbf{e}_0^1, \mathbf{e}_1^1\}$: basis of $\mathbb{H}_1$ obtained by applying Hadamard's operator to E^0.
E^0 corresponds to a spin with vertical–horizontal polarization, $E^0 = \{\uparrow, \rightarrow\}$, while
E^1 corresponds to a spin with oblique or NW–NE polarization,
$E^1 = \{\nwarrow, \nearrow\}$.
The same sequence of qubits can be measured either w.r.t. to E^0 or E^1.

An eavesdropper can be detected quite directly!
This is characteristic of Quantum Cryptography.

Agenda

The complexity of a communication process is determined by the minimum information quantity that should be transmitted, in order that the total information can be recovered by the receiving part, within a given context.

Optimal Transmission

Let us assume that three sets X, Y, Z are given and a function $f : X \times Y \to Z$. At some moment, Alice, who is a communicating part, possesses a point $x \in X$, Bob, who is a second part, possesses a point $y \in Y$ and both parts should calculate $z = f(x, y)$, by interchanging the minimum information quantity.

Identity Checking

Exact and obvious method

If $f : (x, y) \mapsto \chi_=(x, y)$ is the characteristic function of the identity relation:

$$f(x, y) = 1 \text{ if and only if } x = y,$$

then Alice and Bob should interchange n bits to calculate $f(x, y)$.

n is exponential with respect to its size!

An interesting question is whether an exact algorithm can be obtained with logarithmic complexity.
The following theorem excludes the possibility to communicate more than k (classical) bits of information by transmitting k qubits.

Holevo's Theorem

The information quantity recovered from a register of qubits is upperly bounded by the value of von Neumann's entropy, which is bounded by Shannon's entropy. Both entropies coincide whenever the qubits are pairwise orthogonal.

However, in Quantum Computing the use of the notion of entangled states improves the communication complexities of several procedures.

Pseudotelepathy Game

Given four sets X, Y, A and B, a relation $R \subset X \times and \times A \times B$, and the fact that Alice and Bob are separated, far from each other, at a given moment Alice receives a point $x \in X$, Bob a $y \in Y$ and they, trying to interchange the minimum information, should produce, respectively, $a \in A$ and $b \in B$ such that $(x, y, a, b) \in R$.

In particular, for $n = 2^k$ a power of 2, $X = \{0,1\}^n = Y$, $A = \{0,1\}^k = B$

R is Deutsch-Josza relation

$$(x,y,a,b) \in R \ \Leftrightarrow \left[(H_n(x,y) = 0 \ \wedge \ a = b) \ \vee \ \left(H_n(x,y) = \frac{n}{2} \ \wedge \ a \neq b\right) \ \vee \ H_n(x,y) \notin \left\{0, \frac{n}{2}\right\}\right] \tag{3}$$

- If the points x and y of Alice and Bob coincide, then the sequences that they produce should coincide
- If x and y differ exactly in half of the bits, then the produced sequences should differ
- In any other case no restrictions on produced sequences