Мови програмування для квантових обчислень

Максим Сохацький [1]

[1] Національний технічний університет України
«Київський Політехнічний Інститут» ім. Ігора Сікорського
28 жовтня 2018

Аннотація

Ця робота є спробою огляду існуючих мов програмування для квантових обчислень та їх особливостей.
Ключові слова: Теорія типів, Мови порграмування, Квантові обчислення

Зміст

1 Попередні відомості

1.1 Лінійна алгебра

Нотація Дірака це компактний формалізм лінійної алгебри який будемо застосовувати для визначень квантової механіки.

Таблица 1: Нотація Дірака

Нотація	Визначення
$\|\psi\rangle$	загальний кет-вектор, наприклад $(c_0, ..., c_n)^T$
$\langle\psi\|$	дуальний бра-вектор, наприклад $(c_0^*, ..., c_n^*)$
$\|n\rangle$	n-й базис вектор стандартного базису $N = (\|0\rangle, ..., \|n\rangle)$
$\|\tilde{n}\rangle$	n-й базис вектор альтернативного базису $\tilde{N} = (\|\tilde{0}\rangle, ..., \|\tilde{n}\rangle)$
$\langle\phi\|\psi\rangle$	скалярний добуток
$\|i, j\rangle$	тензорний добуток базисних векторів $\|i\rangle$ та $\|j\rangle$
$\|\phi\rangle \otimes \|\psi\rangle$	тензорний добуток

Визначення 1. (Векторний простір). Множина V називається векторни мпростором над скалярним полем F, тоді і тільки тоді, коли визначені операції $+ : V \times V \to V$ (сума векторів) та $\cdot : F \times V \to V$ (добуток скаляра та вектора) з наступними властивостями: i) $(V, +)$ утворюють комутативну групу; ii) $\lambda|\psi\rangle = |\psi\rangle\lambda$; iii) $\lambda(\mu|\psi\rangle) = (\lambda\mu)|\psi\rangle$; iv) $(\lambda + \mu)|\psi\rangle = \lambda|\psi\rangle + \mu|\psi\rangle$; v) $\lambda(|\psi\rangle + |\varphi\rangle) = \lambda|\psi\rangle + \lambda|\varphi\rangle$. Далі будемо розглядати скалярне поле комплексних чисел $F = C$.

Визначення 2. (Скалярний добуток). Функція $\langle\cdot|\cdot\rangle : V \times V \to C$ називається скалярним добутком, тоді і тільки тоді, коли: i) $\langle\psi|(\lambda\varphi\rangle + \mu|\chi\rangle) = \lambda\langle\psi|\varphi\rangle + \mu\langle\psi|\varphi\rangle$; ii) $\langle\psi|\varphi\rangle = \overline{\langle\varphi|\psi\rangle}^*$; iii) $0 < \langle\psi|\psi\rangle \in \mathbb{R}$. Скалярний добуток визначає норму $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle} = \| \psi \|$.

Визначення 3. (Повний векторний простір). Нехай V векторний простір з нормою $\| \cdot \|$ та $|\psi_n\rangle \in V$ послідовність векторів. i) $|\psi\rangle$ є послідовністю Коші ттт. $\forall\epsilon > 0 \exists N > 0 : \forall n, m > N, \| |\psi_n\rangle - |\psi_{n+1}\rangle \| < \epsilon$. ii) $|\psi\rangle$ сходиться ттт. $\forall\epsilon > 0 \exists N > 0 : \forall n > N, \| |\psi_n\rangle - |\psi\rangle \| < \epsilon$. Простір V повний ттт. кожна послідовність Коші сходиться.

Визначення 4. (Гільбертів простір). Повний векторний простір H зі скалярний добутком $\langle\cdot|\cdot\rangle$ та відповідною нормою $\| \psi \| = \sqrt{\langle\psi|\psi\rangle}$ називається Гільбертовим.

Визначення 5. (Лінійний оператор). Нехай V – векторний простір, а A – функція $A : V \to V$. Тоді A називається лінійним оператором ттт.

$$A(\lambda|\psi\rangle + \mu|\varphi\rangle) = \lambda A|\psi\rangle + \mu A|\varphi\rangle$$

В C^n лінійний оператор є матрицею $m \times n$ з елементами $a_{i,j} = \langle i|A|j\rangle$, де $A = \Sigma_{i,j} a_{i,j} |i\rangle\langle j|$. За визначенням лінійності оператор A можно записати через лінійну суму векторів базису B:

$$A : |n\rangle \to \Sigma_k a_{kn} |k\rangle, \text{ де } |k\rangle \in B.$$

Визначення 6. (Тензорний добуток гільбертових просторів). Нехай H_1 та H_2 — Гільбертові простори з базисами B_1 та B_2. Тоді тензорний добуток

$$H = H_1 \otimes H_2 = \{\Sigma_{|i\rangle \in B_1} \Sigma |j\rangle \in B_2 c_{ij} |i,j\rangle \| c_{ij} \in \mathbb{C}\}.$$

також Гільбертів простір з базисом $B = B_1 \times B_2$ та скалярним добутком:

$$\langle i,j|i',j'\rangle = \langle i|i'\rangle\langle j|j'\rangle = \delta_{ii'}\delta jj', \text{ де } |i\rangle, |i'\rangle \in B_1, |j\rangle, |j'\rangle \in B_2.$$

Визначення 7. (Тензорний добуток лінійних операторів). Нехай A та B лінійні оператори на Гільбертових протосторах H_1 та H_2, тоді тензорний добуток

$$A \otimes B = \Sigma_{i,j} \Sigma i', j'|i,j\rangle\langle i|A|i'\rangle\langle j|B|j'\rangle\langle i',j'|$$

лінійний оператор на на гільбертовому просторі $H_1 \otimes H_2$.

Визначення 8. (Комутатор та антикомутатор). Нехай A та B лінійні оператори на гільбертовому просторі H. Оператор $[A,B] = AB - BA$ називається комутатором, а $A,B = AB + BA$ називається антикомутатором.

2 Інтерпретація квантової механіки

В залежності від того як саме моделюються та конструюються гільбертові простори та гамільтоніани, виникають різні теорії, від нерятивістської квантової електродинаміки до квантової хронодинаміки яка вводить поняття кварків та глюонів.

Теорія квантових обчислень — це ще одна теорія поверх абстрактного квантового формалізму та є інтерпретацією квантової механіки. Однак це не фізична теорія в тому сенсі, що вона не описує природній процес, а є ближчою до схемотехніки, з квабітами та квантовими вентилями, без визначення як саме моделюється квантова система, вона може бути або фізичним об'єктом або симулятором.

Точно так як для апаратного забезпечення будуються мови порграмування та вищі мови програмування, так само для квантових обчислень, квантових станів та квантових логічних елементів (вентилів), існують свої мови програмування. У наступній секції дамо огляд існуючих мов та підходів до їх побудови, а тут дамо основні принципи та компоненти архітекти квантових обчислень, аби пояснити основні мовні елементи.

2.1 Пам'ять квантового комп'ютера

Визначення 9. (Квантовий біт). Квантовий біт або квабіт визначається як квантова система, стан якої може бути повністю виражений як суперпозиція (лінійна комбінація) двох ортонормованих власних базових станів позначених $|0\rangle$ та $|1\rangle$. Загальний стан $|\psi\rangle$ квабіта тоді визначається як $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, |\alpha|^2 + |\beta|^2 = 1$. Значення квабіта описується спостереженням $N = |1\rangle\langle 1|$. $\langle N\rangle$ дає вірогідність знайти систему в стані $|1\rangle$, якщо над квабітом були проведені виміри. Простір станів квабіта є гільбертовим простором $H = \mathbb{C}^2$. Ортонормована система $|0\rangle, |1\rangle$ називається обчислювальним базисом.

Визначення 10. (Сфера Блоха). Загальний стан квабіта може бути виражений в полярних координатах θ та ϕ:

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle.$$

Одиничний вектор стану $|\psi\rangle$ називається вектором Блоха $\tilde{r}_\psi$, та має наступну властивість $\tilde{r}_\phi = -\tilde{r}_\xi \leftrightarrow \langle\phi|\xi\rangle = 0$.

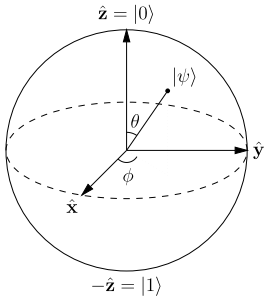

Рис. 1: Сфера Блоха як представлення квабіта $|\psi\rangle$

Визначення 11. (Квантова система).

Визначення 12. (Еволюція системи). Темпоральна еволюція стану системи описується рівнянням Шрьодінгера:

$$i\hbar\frac{\delta}{\delta t}|\psi\rangle = H|\psi\rangle.$$

де $\hbar \equiv 1.05457 \cdot 10^{-43}$ експериментальна константа Планка, а H — фіксований самоспряжений оператор на гільбертовому просторі, знаний як Гамільтоніан квантової системи. В квантовій фізиці нормують відносно $\hbar$ тоді рівняння можна записани у безвимірній формі $i|\psi\rangle = H|\psi\rangle$. Гамільтоніан H повністю визначає квантову систему. Другий спосіб визначення, через унітарний оператор $U = e^{-iH}$. Темпоральна еволюція замкненої квантової системи зі страну $|\psi\rangle$ та часу t_1 в стан $|\psi'\rangle$ та часу t_2 може бути описана унітарним оператором $U = U(t_2 - t_1)$, таким, що $|\psi'\rangle = U|\psi\rangle$.

Визначення 13. (Вимірювання). Проективне вимірювання визначається як самоспряжений оператор M який називається спостереженням зі спектральною композицією $M = \Sigma_m m P_m$, де P_m проекція на власний простір власного значення m. Власні значення m оператора M відповідаються усім можливим результатам вимірювання. Вимірювання $|\psi\rangle$ дасть результат m з вірогідністю $p(m) = \langle\psi|P_m|\psi\rangle$, таким чином через скорочення $|\psi\rangle$ отримаємо новий стан системи $|\psi'\rangle = \frac{1}{\sqrt{p(m)}} P_m|\psi\rangle$. Для стану квабіта, самоспряжений оператор N знаний як стандартне вимірювання.

$$N = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|.$$

Біль загально для простору стану $H = C^n$ стандартне вимірювання визначається як $N = \Sigma_i i|i\rangle\langle i|$.

Визначення 14. (Виважене середнє). Виважене середнє $\langle M\rangle$ усіх можливих результатів вимірювання M називється очікуваним значенням та визначається як

$$\langle M\rangle = \Sigma_n p(m)m = \Sigma_m \langle\psi|mP_m|\psi\rangle = \langle\psi|M|\psi\rangle.$$

3 Огляд існуючих мов

З огляду на новизну предмету розроблено не так багато мов, усі що є можна розділіти на імперативні по духу своєї імплемантації та функціональні, або побудовані на базі певного виду лямбда числення. Ми наведемо приклади програм для обох підходів. У якості порівняльної характеристики візьмемо алгоритм дискретного перетворення Фур'є

3.1 Імперативні мови програмування

Станом на 2018 рік найбільш розробленою мовою, яка компілюється під Linux та Mac є QLC від Бернхарда Омера [1]. До QLC можна відзначти наступні мови: 1) Q-gol від Грега Бейкера (1996) [2]; 2) qGCL від Паоло Зуліані (2000)[4]; 3) Quantum C Language від Стефана Блаха (2002); 4) QPAlg від Марі Лолір та Філіпа Жорранда (2004)[3]; 5) QCP (Communication Quantum Processes) від Саймона Гея та Раджагопала Нагараджана (2004)[2];

Визначення 15. (Заміна).

```
cond qufunct Swap(qureg a,qureg b) {
  int i;
  if #a!=#b { exit "swap arguments must be of equal size"; }
```

[1] Bernhard Ömer. Structured Quantum Programming. PhD. TU Vienna. 2003. `http://tph.tuwien.ac.at/~oemer/doc/structquprog.pdf`

[2] Gregory David Baker. Qgol. A system for simulating quantum computations: Theory, Implementation and Insights. 1996. PhD. Macquarie University.
`http://www.ifost.org.au/~gregb/q-gol/QgolThesis.pdf`

```
  for i=0 to #a-1 {
    CNot(b[i],a[i]);
    CNot(a[i],b[i]);
    CNot(b[i],a[i]);
  }
}
```

Визначення 16. (Зміна порядку квабітів).

```
cond qufunct flip(qureg q) {
  int i;
  for i=0 to #q/2-1 { Swap(q[i],q[#q-i-1]); }
}
```

Визначення 17. (Дискретне перетворення Фур'є, Коперсміт).

```
operator dft(qureg q) {
  const n=#q;
  int i; int j;
  for i=1 to n {
    for j=1 to i-1 { V(pi/2^(i-j),q[n-i] & q[n-j]); }
    H(q[n-i]);
  }
  flip(q);
}
```

3.2 Квантові лямбда числення

Загалом з огляду таксономії лямбла числень, яку виконав Хенк Барендрегт та подав у вигляді лямбда кубу, можна розширити квантовими мовними примітивами будь яке лямбда-числення (яке належить до лямбда кубу) або навіть вводити в вищі лямбда числення з гомотопічними типами та в системи доведення теорем з екстрактом або лише типизацією та обчисленнями на рівні типів.

Однак необхідним компонентом квантового лямбда числення є система лінійних типів, де за час існування змінної в області видимості під час виконання дозволяється звертання до неї тільки один раз. Така система типів уже використовується не тільки в есперимантальних верифікаторах але і в сучасних системних мовах програмування (Rust), де завдяки верифікатору лініних типів вдається обійтися без алгоритмів автоматичного вивільнення памяті під час виконання програми (схема памяті повністю моделюється під час компіляції програми).

Серед робіт присвячених мовам на базі лямбда числень можна відзначити наступні: 1) Вант Тондера; 2) Селінжера та Валірона; 3) Аррігі та Довека[1]; 4) Унруха.

Визначення 18. (Синтаксичне дерево O_H). Синтаксичне дерево O_H визначає лямбда числення з лінійними змінними поєднане з класичним нетипизованим лямбда численням. Тобто O_H є найпростішим операційним квантовим лямбда численням для середовищ виконання.

```
t = x
  | λ x . t
  | let x = t in t
  | t t
  | (t , t)
  | t
  | c
  | ! t
  | λ ! x . t

c = 0 | 1 | H | S | R3 | CNot | X | Y | Z | ...
```

Тут даються примітиви лінійних типів, де доступ до змінної можливий лише раз в обсласті визначення змінної. Для нелінійних або звичайних лямбда функції даються примітиви позначені !. В переліку квантових примітивів с даються: i) ортонормований базис $|0\rangle$ та $|1\rangle$; ii) H — оператор Адамара; iii) S — фазовий вентиль; iv) R_3 — $\pi/8$ вентиль; v) контрольований не вентиль CNot; vi) вентилі Паулі X, Y та Z.

Визначення 19. (Пара Ейнштейна-Подольського-Розена).

$$\mathbf{EPR} = \mathbf{CNot}\ ((\mathbf{H}\ 0), 0) \tag{1}$$

Визначення 20. (Квантова телепортація).

$$\begin{aligned}\mathbf{teleport}\ x = \mathbf{let}\ (e_1, e_2)\ &=\ \mathbf{EPR}\ \mathbf{in} \\ &\mathbf{let}\ (x', y') = \mathbf{alice}\ (x, e_1)\ \mathbf{in}\ \mathbf{bob}\ (x', y', e_2)\end{aligned} \tag{2}$$

$$\begin{aligned}\mathbf{alice}\ (x, e_1) = \mathbf{let}\ (x', y') &= \\ &\mathbf{CNot}\ (x, e_1)\ \mathbf{in}\ ((\mathbf{H}\ x'), y') \\ \mathbf{bob}\ (x', y', e_2) = \mathbf{let}\ (y'', e_2') &= cX\ (y', e_2)\ \mathbf{in} \\ &\mathbf{let}\ (x'', e_2'') = cZ\ (x', e_2')\ \mathbf{in}\ (x'', y'', e_2'')\end{aligned} \tag{3}$$

Визначення 21. (Дискретне перетворення Фур'є).

$$\mathbf{fourier}\ list\ =\ \mathbf{reverse}\ \mathbf{fourier}'\ list \tag{4}$$

$$\mathbf{fourier}'\ list\ =\ \mathbf{case}\ list\ \mathbf{of}\begin{cases}() \to () \\ h : t \to \mathbf{let}\ h'\ :\ t' = \mathbf{phases}\ (\mathbf{H}\ h)\ t\ !2 \\ \mathbf{in}\ h'\ :\ \mathbf{fourier}'\ t'\end{cases} \tag{5}$$

$$\textbf{phases}\ target\ controls\ !n\ =$$
$$\textbf{case}\ control\ \textbf{of}\begin{cases}() \to target \\ control : t \to \textbf{let}\ (control', target') = \\ (cR\ !n)\ (control, target)\ \textbf{in} \\ \textbf{let}\ target'' : t' = \textbf{phases}\ target'\ t\ !(\textbf{succ}\ n)\ \textbf{in} \\ target'' : control' : t'\end{cases} \tag{6}$$

4 Висновки

Як видно для реалізації семантики мови програмування для квантових комп'ютерів достатньо поєднаяти тензорне числення разом з π-численням процесів, або лінійними типами. На сьогоднішній день (2018) серед імперативних мов програмування найбільш завершена, повна та практична на думку автора є QLC від Бернхарда Омера, серед мов для лямбда числень немає жодної достатньо зрілої імплементації. З огляду на це можна сказати що предмет є молодим та серед можливих напрямків розробки ми бачимо поєднання лінійних типів з тензорними ядрами які могли би служити семантичною основою для вбудовування у симулятори квантових комп'ютерів або середовища виконання. Цілком відкритою та недослідженою виявилась область формальних досліджень для систем доведення теорем щодо квантових алгоритмів та семантики тензорного числення. Однак треба сказати, що формалізація семантики π-калкулуса гомотопічними методами — відкрита проблема, а це є необхідним прекурсором до семантики квантових обчислень.

Список литературы

[1] Pablo Arrighi and Gilles Dowek. Operational semantics for formal tensorial calculus. *No*, 2004.

[2] Simon J. Gay and Rajagopal Nagarajan. Communicating quantum processes. In *Proceedings of the 32Nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '05, pages 145–157, New York, NY, USA, 2005. ACM.

[3] Marie Lalire and Philippe Jorrand. A process algebraic approach to concurrent and distributed quantum computation: Operational semantics. *CoRR*, quant-ph/0407005, 2004.

[4] J. W. Sanders and P. Zuliani. Quantum programming. In *Proceedings of the 5th International Conference on Mathematics of Program Construction*, MPC '00, pages 80–99, London, UK, UK, 2000. Springer-Verlag.