Quantum Algebraic Effects

Strah, mentor: doc. dr. Matija Pretnar

15th July 2022

Abstract

Quantum computing is based on many modern programming language theory concepts, such as linear types, (quantum) physics, and many others. In my thesis I will be focusing on these two, but in this article I will only present the latter. Our goal is understanding quantum programs, and a good way of understanding them is understanding program equality.

1 Quantum Mechanics

This part is mostly summarised from [1]. It contains basic definitions (and examples) of mathematical basis of quantum mechanics that we need to define our desired qubit operations.

Notation

Throughout this part I will be using the following symbols:

- $\mathbb{N} = \{0, \dots\}$, $\mathbb{N}_+ = \{1, \dots\}$, $\mathbb{N}_n = \{0, \dots, 2^n - 1\}$,
- $n, m \in \mathbb{N}_+$, which we call the number of qubits,
- $j, k, \dots \in \mathbb{N}_n$,
- a_j j-th component of vector a,
- $j = j_1 \dots j_n$ the binary representation of j.

1.1 Quantum Vectors

Definicija 1. Binary vectors are elements of the space $\mathbf{B}_n \coloneqq \{0,1\}^n$ and I will be writing them as stings of 1s and 0s. For us they represent classical computation.

Example. $\mathbf{B}_2 = \{00, 01, 10, 11\}$.

Remark. 1 and 01 represent different vectors.

Definicija 2 (Hilbert space)**.** Elements of the space $\mathbf{H}_n \coloneqq \mathbb{C}^{2^n}$ are called quantum vectors, while elements of $\mathbf{H} \coloneqq \mathbf{H}_1$ are qubits. The space $\mathbf{H}_n$ is thus called the space of quantum vectors of order n, and its standard basis is denoted with $\{e_j\}$. This is where quantum processes take place.

Definicija 3 (Braket notation)**.** Let $j \in \mathbb{N}_n$ and $\hat{\jmath} \in \mathbf{B}_n$ be the corresponding binary vector. Then $|j\rangle = |\hat{\jmath}\rangle \coloneqq e_j$.

Remark. By definition, it follows that $\mathbf{H}_n = \mathcal{L}_{\mathbb{C}}(\{|j\rangle \mid j \in \mathbf{B}_n\})$.

Example ($n = 1$ and $n = 2$)**.**

$$a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a_0 |0\rangle + a_1 |1\rangle ,$$

$$a = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle .$$

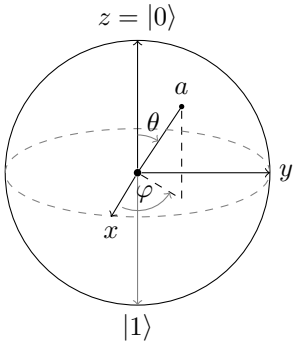
Example (Hadamard vector)**.**

$$\mathbf{h} \coloneqq \rho \left(|0\rangle + |1\rangle \right), \quad \mathbf{h}_n \coloneqq \rho^n \sum_{j \in \mathbf{B}_n} |j\rangle , \quad \rho \coloneqq \frac{1}{\sqrt{2}}.$$

1.2 Bloch Sphere

Statement 1. *In the physical world two qubits that differ by a (complex) factor represent the same state. Mathematically this means states of qubits (also qubits) live in* $\mathbf{P}\mathbb{C}^1 \cong \mathbb{S}^2$*:*

$$a = \cos\frac{\theta}{2}\left|0\right\rangle + e^{i\varphi}\sin\frac{\theta}{2}\left|1\right\rangle, \quad \varphi \in [0, 2\pi), \theta \in [0, \pi].$$



Proof. Let $a = a_0\left|0\right\rangle + a_1\left|1\right\rangle = r_0 e^{i\varphi_0}\left|0\right\rangle + r_1 e^{i\varphi_1}\left|1\right\rangle$.
Denote $r \coloneqq \sqrt{r_0^2 + r_1^2}, \varphi \coloneqq \varphi_1 - \varphi_0, \theta \coloneqq 2\arccos\frac{r_0}{r}$.
Then $a = \hat{a} \coloneqq \frac{a}{re^{i\varphi_0}} = \frac{r_0}{r}\left|0\right\rangle + \frac{r_1}{r}e^{i\varphi}\left|1\right\rangle = \cos\frac{\theta}{2}\left|0\right\rangle + e^{i\varphi}\sin\frac{\theta}{2}\left|1\right\rangle$. □

1.3 Tensor Product

Definicija 4 (Tensor product)**.** The tensor product of spaces $\mathbf{H}_n$ and $\mathbf{H}_m$ is equal to $\mathbf{H}_{n+m}$. We write $\mathbf{H}_n \otimes \mathbf{H}_m$. If $a \in \mathbf{H}_n$ and $b \in \mathbf{H}_m$ then $a \otimes b \in \mathbf{H}_n \otimes \mathbf{H}_m$.

Remark. The operator $\otimes$ is indeed a tensor product.

Example (Tensor product of basis vectors)**.**

$$\left|j\right\rangle \otimes \left|k\right\rangle = \left|j_1 \dots j_n k_1 \dots k_m\right\rangle = \left|j\right\rangle\left|k\right\rangle = \left|jk\right\rangle,$$

Example (General tensor product)**.**

$$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}, \quad a \otimes b = \sum_{\substack{j \in \mathbf{B}_n, \\ k \in \mathbf{B}_m}} a_j b_k \left|jk\right\rangle.$$

Examples (Tensor exponent)**.**

$$\mathbf{h}_n = \mathbf{h}^{\otimes n} = \rho^n \underbrace{(\left|0\right\rangle + \left|1\right\rangle) \otimes \dots \otimes (\left|0\right\rangle + \left|1\right\rangle)}_{n},$$
$$\mathbf{H}_n = \mathbf{H}^{\otimes n} = \underbrace{\mathbf{H} \otimes \dots \otimes \mathbf{H}}_{n}.$$

Definicija 5. If $a \in \mathbf{H}_n$ can be written as $\bigotimes_{j=1}^{n} a_j$ for some $a_j \in \mathbf{H}$ we say it's simple or separable, otherwise it's composite or quantum entangled.

1.4 Quantum Maps

Definicija 6. The space of unitary gates of order n is $\mathbf{U}_n \coloneqq \mathbf{U}(2^n)$, the space of unitary $2^n \times 2^n$ matrices. The tensor product of gates $U \otimes V \coloneqq [u_{jk}V]_{j,k}$ used on $a \otimes b$ is $Ua \otimes Vb$.

Example (Tensor product of unitary gates)**.**

$$\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \otimes B = \begin{bmatrix} a_{00}B & a_{01}B \\ a_{10}B & a_{11}B \end{bmatrix}.$$

Definicija 7. For gates $U_0, \dots, U_s$ we denote their block-diagonal matrix with $D(U_0, \dots, U_s)$.

Theorem 1 (No cloning)**.** *There doesn't exist a unitary gate of odrer* 2*, which maps every vector of the form* $a \otimes \left|0\right\rangle \in \mathbf{H} \otimes \mathbf{H}$ *to* $a \otimes a$*.*

Proof. Let U be such that for all $a \in \mathbf{H}$ we have $U(a \otimes \left|0\right\rangle) = a \otimes a$.
Then for $\mathbf{h} \otimes \left|0\right\rangle = \rho(\left|00\right\rangle + \left|10\right\rangle)$ the following holds:

$$U(\rho(\left|00\right\rangle + \left|10\right\rangle)) = \begin{cases} \rho^2(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle), \\ \rho U\left|00\right\rangle + U\left|10\right\rangle = \rho(\left|00\right\rangle + \left|11\right\rangle), \end{cases}$$

which is a contradiction. □

Example (Pauli matrices)**.** These are the matrices of half-rotation around the axes on the bloch sphere:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

It holds that $X^2 = Y^2 = Z^2 = I_2$. The map X is also called negation, since $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$.

Example (Hadamard matrix)**.**

$$\mathtt{Had} = \rho \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathtt{Had}\,|0\rangle = \mathbf{h}, \quad \mathtt{Had}^{\otimes n}\,|\mathbf{0}^n\rangle = \mathbf{h}_n.$$

Example (Phase shift)**.**

$$S_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}, \text{ posebej označimo } S \coloneqq S_{\pi/2}, T \coloneqq S_{\pi/4},$$
$$S_\alpha\left(a_0\,|0\rangle + a_1\,|1\rangle\right) = a_0\,|0\rangle + a_1 e^{i\alpha}\,|1\rangle\,.$$

1.5 Quantum Measurement

In classical computation we have `if` statements. This can be generalised in two ways; first, with direct measurement (and classical `if` statements), and second by using quantum entanglement. It turns out that after measurement the two ways are equivalent.

Definicija 8 (Quantum Measurement)**.** Denote the measurement of a qubit $a = a_0\,|0\rangle + a_1\,|1\rangle$ with $M(a)$ and it is 0 with probability $|a_0|^2$ and 1 with probability $|a_1|^2$. This will "'destroy"' the qubit a.

Definicija 9 (Quantum Control)**.** For $r, s \in \mathbb{N}$ and $U \in \mathbf{U}_1$ define $C_{r,s}(U)$ and $\overline{C}_{r,s}(U)$ by

$$C_{r,s}(U)\,|j\rangle = \begin{cases} |j\rangle & ; j_r = 0 \\ |j_1 \ldots\rangle\,|Uj_s\rangle\,|\ldots j_n\rangle & ; j_r = 1 \end{cases} \qquad \overline{C}_{r,s}(U)\,|j\rangle = \begin{cases} |j\rangle & ; j_r = 1 \\ |j_1 \ldots\rangle\,|Uj_s\rangle\,|\ldots j_n\rangle & ; j_r = 0 \end{cases}$$

We call such gates controlled ("'on one"' and "'on zero"'). Specially, for $U \in \mathbf{U}_1$ we denote

$$\mathtt{cU} \coloneqq C_{1,2}(U) = D(\mathtt{I}_2, \mathtt{U}), \quad \mathtt{\bar{c}U} \coloneqq \overline{C}_{1,2}(U) = D(\mathtt{U}, \mathtt{I}_2).$$

Example (Entangled qubits)**.** Controlled gates entangle pairs of qubits. For example $\underline{\mathsf{apply}}_{\mathtt{cX}}(a, b)$ behaves like `if` $\underline{\mathsf{measure}}(a) = 0$ `then` (a, b) `else` $(a, \neg b)$. Of course, we know the second expression is not valid (since measurement destroys a), but it is for this exact reason that quantum control is the tool we want to replace `if` statements with!

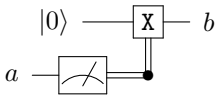
2 Quantum Computation, Algebraic Effects and Diagrams

2.1 Quantum Circuits

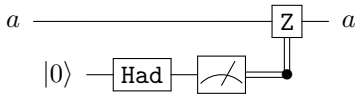
Quantum programs can be represented as circuit diagrams. Boxes represent quantum gates and lines between them wires; single for qubits, double for classical bits. Circles on the wire (and then a vertical wire from them) represent control; empty circles control "'on zero"' and full control "'on one"'. We read such circuits left to right. A more thorough account can be found in [1].

Below are two examples of quantum programs, described both with words and diagrams. We will also see these examples used later.

Example (Projection to the z-axis)**.** First measure a and then depending on the result either flip or leave alone a fresh qubit. On the Bloch sphere this looks approximately like a projection to the z-axis (as the only qubits on it are $|0\rangle$ and $|1\rangle$).



Example (Random phase shift)**.** Measurement of the Hadamard vector simulates a fair coin toss and the Z gate is a phase shift by π radians. The algorithm randomly either shifts the phase or not.



2.2 Algebraic Effects

We often use computational effects while programming: global variable state, IO devices, randomness, exceptions, non-determinism, etc.

Definicija 10 (Computational Effects)**.** If a function or operation has some outward detectable effect other than the returned value we call it a computational effect (effect of the computation).

Definicija 11 (Algebraic Effects)**.** Computational effects that can be represented with some algebraic theory are called algebraic effects.

3 Quantum Programming Language

In our language[2] we have the usual basic constructs, e.g. types, `let` and `if` statements, etc. Other than that we also have quantum elements: the type of qubits `qubit` and for every two types A and B we have the type of entangled pairs $A \otimes B$. Due to the nature of qubits we cannot access their inner state directly, but we do have the following accessor functions:

- $\underline{\mathsf{new}}$: assigns a new qubit with initial value $|0\rangle$,
- $\underline{\mathsf{apply}}_{\mathtt{U}}$: uses gate U on a given vector,
- $\underline{\mathsf{measure}}$: measures a given qubit and returns an element of type `bit`.

3.1 Conversion into Algebraic Expressions

The above constructs are assigned the following algebraic expressions. We also introduce a concise notation for pen and paper manipulation.

Quantum programming language	Algebraic expressions	Mathematical symbols
$\mathtt{let}\ a \leftarrow \underline{\mathsf{new}}()\ \mathtt{in}\ x(a)$	$\mathsf{new}(a.\, x(a))$	$\nu a.\, x(a)$
$\underline{\mathsf{apply}}_{\mathtt{U}}(a);\ x(a)$	$\mathsf{apply}_{\mathtt{U}}(a.\, x(a))$	$\mathtt{U}_a(x(a))$
$\mathtt{if}\ \underline{\mathsf{measure}}(a) = 0\ \mathtt{then}\ t\ \mathtt{else}\ u$	$\mathsf{measure}(a.\, t; u)$	$t\ ?_a\ u$
$\underline{\mathsf{discard}}(a);\ t$	$\mathsf{discard}(a.\, t)$	$\mathsf{disc}_a(t)$

Example (Projection to the z-axis)**.**

1. $\mathtt{if}\ \underline{\mathsf{measure}}(a) = 0\ \mathtt{then}\ \underline{\mathsf{new}}()\ \mathtt{else}\ \underline{\mathsf{apply}}_{\mathtt{X}}(\underline{\mathsf{new}}())$
2. $\mathsf{measure}\Big(a.\, \mathsf{new}(b.\, x(b)); \mathsf{new}\Big(b.\, \mathsf{apply}_{\mathtt{X}}(b.\, x(b))\Big)\Big)$
3. $(\nu b.\, x(b))\ ?_a\ (\nu b.\, \mathtt{X}_b(x(b)))$

Example (Random phase shift)**.**

1. $\mathtt{if}\ \underline{\mathsf{measure}}\Big(\underline{\mathsf{apply}}_{\mathtt{Had}}(\underline{\mathsf{new}}())\Big) = 0\ \mathtt{then}\ a\ \mathtt{else}\ \underline{\mathsf{apply}}_{\mathtt{Z}}(a)$
2. $\mathsf{new}\Big(b.\, \mathsf{apply}_{\mathtt{Had}}\Big(b.\, \mathsf{measure}\Big(b.\, x(a); \mathsf{apply}_{\mathtt{Z}}(a.\, x(a))\Big)\Big)\Big)$
3. $\nu b.\, \mathtt{Had}_b(x(a)\ ?_b\ \mathtt{Z}_a(x(a)))$

3.2 Axioms

We can separate the axioms for program equality into two groups: the first five are conceptual, while the other seven are administrative. The latter tell us apply agrees with the algebraic structure of unitary matrices and that things commute as far as variable binding (and matrix order) allows. A more detailed description (with proofs) can be found in [2].

Quantum negation before measurement is regular negation after measurement:
Axiom A. $\mathtt{X}_a(x \mathbin{?_a} y) = y \mathbin{?_a} x$.

Quantum control is like classical control after measurement:
Axiom B. $D(\mathtt{U},\mathtt{V})_{a,b}(x(b) \mathbin{?_a} y(b)) = \mathtt{U}_b(x(b)) \mathbin{?_a} \mathtt{V}_b(y(b))$.

Quantum gates used on discarded qubits are unnecessary:
Axiom C. $\mathtt{U}_a(\mathsf{disc}_a(t)) = \mathsf{disc}_a(t)$.

Fresh qubits are $|0\rangle$ wrt. measurement:
Axiom D. $\nu a.\, x \mathbin{?_a} y = x$.

Fresh qubits are $|0\rangle$ wrt. control:
Axiom E. $\nu a.\, D(\mathtt{U},\mathtt{V})_{a,b}(x(a,b)) = \mathtt{U}_b(\nu a.\, x(a,b))$.

Symmetric group $\mathbf{U}_n$ structure is respected:
Axiom F. $\mathtt{swap}_{a,b}(x(a,b)) = x(b,a)$,
Axiom G. $\mathtt{I}_a(x(a)) = x(a)$,
Axiom H. $\mathtt{UV}_a(x(a)) = \mathtt{V}_a(\mathtt{U}_a(x(a)))$,
Axiom I. $\mathtt{U} \otimes \mathtt{V}_{a,b}(x(a,b)) = \mathtt{U}_a(\mathtt{V}_b(x(a,b)))$.

Commutativity:
Axiom J. $(u \mathbin{?_b} v) \mathbin{?_a} (x \mathbin{?_b} y) = (u \mathbin{?_a} x) \mathbin{?_b} (v \mathbin{?_a} y)$,
Axiom K. $\nu a.\, \nu b.\, x(a,b) = \nu b.\, \nu a.\, x(a,b)$,
Axiom L. $\nu a.\, x(a) \mathbin{?_b} y(a) = (\nu a.\, x(a)) \mathbin{?_b} (\nu a.\, y(a))$.

Example (Derivation of equality between z-axis projection and random phase shift)**.** The derivation relies on the identities $\mathtt{cX.swap.cX} \overset{\dagger}{=} \mathtt{swap.cX.swap}$ and $\mathtt{swap.cX.swap} \overset{\ddagger}{=} (\mathtt{Had} \otimes \mathtt{I}_2).\mathtt{cZ}.(\mathtt{Had} \otimes \mathtt{I}_2)$.

$$
\begin{aligned}
&(\nu b.\, x(b)) \mathbin{?_a} (\nu b.\, \mathtt{X}_b(x(b))) \\
&\quad = \nu b.\, x(b) \mathbin{?_a} \mathtt{X}_b(x(b)) && (L)\\
&\quad = \nu b.\, \mathtt{cX}_{a,b}(x(b) \mathbin{?_a} x(b)) && (B)\\
&\quad = \nu b.\, \mathtt{cX}_{a,b}(\mathsf{disc}_a(x(b))) && (\text{def.})\\
&\quad = \nu b.\, \mathtt{cX}_{b,a}\big(\mathtt{cX}_{a,b}(\mathsf{disc}_b(x(a)))\big) && (\dagger)\\
&\quad = \nu b.\, \mathtt{cX}_{a,b}(\mathsf{disc}_b(x(a))) && (E)\\
&\quad = \nu b.\, \mathtt{Had}_b\big(\mathtt{cZ}_{b,a}(\mathtt{Had}_b(\mathsf{disc}_b(x(a))))\big) && (\ddagger)\\
&\quad = \nu b.\, \mathtt{Had}_b\big(\mathtt{cZ}_{b,a}(\mathsf{disc}_b(x(a)))\big) && (C)\\
&\quad = \nu b.\, \mathtt{Had}_b(x(a) \mathbin{?_b} \mathtt{Z}_a(x(a))). && (B)
\end{aligned}
$$

References

[1] Sebastian Xambó Juanjo Rué. "Mathematical Essentials of Quantum Computing". In: 2011 (cit. on pp. 1, 3).

[2] Sam Staton. "Algebraic Effects, Linearity, and Quantum Programming Languages". In: *SIGPLAN Not.* 50.1 (Jan. 2015), pp. 395–406. ISSN: 0362-1340. DOI: 10.1145/2775051.2676999. URL: https://doi.org/10.1145/2775051.2676999 (cit. on pp. 4, 5).