

Input independence

Yuri Gurevich and Andreas Blass
 University of Michigan, Ann Arbor, Michigan, USA

Abstract

We establish the following *input independence* principle. If a quantum circuit \mathcal{C} computes a unitary transformation U_μ along a computation path μ , then the probability that computation of \mathcal{C} follows path μ is independent of the input.

1 Introduction

In the analysis of quantum computations, estimating the probability that a given circuit computes the desired output is rather important. Typically, the circuit is good enough if that probability is high enough. Static analysis of the circuit may reveal good computation paths, those leading to the desired outcome. But estimating the probability P that the computation follows a good path may not be easy. A priori P depends on the input.

The main result of this paper is the *input independence* principle: If a quantum circuit \mathcal{C} computes a unitary transformation U_μ along a computation path μ , then the probability that computation of \mathcal{C} follows path μ is independent of the input. The principle implies that, if the desired output is given by a unitary transformation U , then the probability P that computation of \mathcal{C} follows a path leading to the desired outcome does not depend on the input. Furthermore, if the unitary transformation is allowed to depend on the path, then P still does not depend on the input.

First, based on the syntax and semantics of quantum circuits in [4], we make the principle mathematically precise. In the process, we recall terminology from [4] and repeat some, though not all, of the definitions.

Setting 1.

- A. Following the standard textbook [7] of Michael Nielsen and Isaac Chuang, we define a (*general*) *measurement* over a Hilbert space \mathcal{K} as an indexed family $M = \langle L_i : i \in I \rangle$ of (bounded linear) operators on \mathcal{K} where $\sum_{i \in I} L_i^\dagger L_i$ is the identity operator $\mathbb{1}$ on \mathcal{K} ; elements of the index set I are (*classical*) *outcomes* of M [7, §2.2.3]. However, contrary to [7], we do not presume that \mathcal{K} is finite dimensional or that I is finite. Instead, as in [3], we presume that \mathcal{K} is separable (and complex), I is countable, and the sum converges in the weak operator topology¹. A *state* in a Hilbert space \mathcal{K} is given by a density operator on \mathcal{K} ; the set of these density operators is denoted $\text{DO}(\mathcal{K})$.

⁰The authors are partially supported by the US Army Research Office under W911NF-20-1-0297.

¹We began this work in the context of quantum computing and required that Hilbert spaces are finite dimensional and measurements have only finitely many outcomes. However, the results work just as well in the broader setting adopted here.

- B. In much of the literature, the meaning of “quantum circuit” is ambiguous. A circuit typically contains unitary operations, often contains measurements, and may contain classical channels. The ambiguity is whether the circuit also tells which gates fire simultaneously and, for those that don’t, the order in which they fire. In the present paper, a quantum circuit may contain unitary operations, measurements, and classical channels. And by default a circuit comes together with a fixed execution schedule (B_1, B_2, \dots, B_N) where B_1 is the set of gates to be fired first, B_2 is the set of gates to be fired next, and so on². It is required of course that the sets B_n are disjoint, that their union contains all the gates, and that, for every n and every gate $G \in B_n$, the set $\bigcup_{k < n} B_k$ of gates scheduled to fire before G contains all (quantum and classical) prerequisites of G .
- C. For uniformity, we treat unitary operators as measurements with a single outcome, so that all gates are measurement gates. Every gate G in a quantum circuit \mathcal{C} is assigned a finite nonempty set of measurements, called G *measurements*. It is assumed without loss of generality that different G measurements have disjoint outcome sets. In addition, G is assigned a *selection* function Σ_G that, in runtime, picks the G measurement to be executed. Let $\text{CS}(G)$ be the set of *classical sources* of G , i.e. the gates with classical channels to G . Given outcomes o_F of the measurements performed by the classical sources F of G , the G measurement $\Sigma_G \langle o_F : F \in \text{CS}(G) \rangle$ is picked. Without loss of generality, we presume that there are no superfluous G measurements: every G measurement is in the range of Σ_G . In particular, if G has no classical sources, then it is assigned (a set comprising) a single G measurement.
- D. A (*computation*) *path*³ μ through a quantum circuit \mathcal{C} is an assignment to each gate G of an outcome $\mu(G)$ of the G -measurement $M_\mu(G) = \Sigma_G \langle \mu(F) : F \in \text{CS}(G) \rangle$. Note that this last equation is a coherence requirement on the measurements performed along the path. Given an input for \mathcal{C} , a path μ represents a potential computation of \mathcal{C} which is said to *follow* path μ on the given input.
- E. Consider quantum circuits \mathcal{C} with principal inputs and outputs (being states) in a Hilbert state \mathcal{H} of dimension ≥ 2 . \mathcal{C} may also use ancillas (initialized in a fixed pure state) and may produce garbage to be discarded at the end of the computation. Let \mathcal{A} be a Hilbert space hosting the ancillas (which we may view as a single higher-dimensional ancilla) at the beginning of computation and the garbage at the end. Accordingly, a full input of \mathcal{C} has the form $\hat{\rho} = \rho \otimes |a\rangle\langle a|$ where $\rho \in \text{DO}(\mathcal{H})$ and $|a\rangle$ is a fixed unit vector in \mathcal{A} . If the computation of \mathcal{C} on input $\hat{\rho}$ follows μ then the output is a density operator $\text{Output}_{\mathcal{C}}(\mu | \hat{\rho})$ on $\mathcal{H} \otimes \mathcal{A}$, and the principal output is the density operator on \mathcal{H} given by the partial trace $\text{Tr}_{\mathcal{A}}(\text{Output}_{\mathcal{C}}(\mu, | \hat{\rho}))$. \triangleleft

Theorem 1.1 (Input independence). *Suppose that a quantum circuit \mathcal{C} computes a unitary operator $U_\mu : \mathcal{H} \rightarrow \mathcal{H}$ along a computation path μ in the sense that density operators $\text{Tr}_{\mathcal{A}}(\text{Output}_{\mathcal{C}}(\mu | \hat{\rho}))$ and $U_\mu \rho U_\mu^\dagger$ represent the same state in \mathcal{H} for all $\rho \in \text{DO}(\mathcal{H})$. Then the probability $P_{\mathcal{C}}(\mu | \hat{\rho})$ that the computation of \mathcal{C} follows path μ on principal input ρ does not depend on ρ .*

The proof of the theorem gives a tiny bit more: It suffices to assume that \mathcal{C} computes U_μ along μ just on pure inputs.

²In [4], we distinguished between circuits with execution schedules and without. A circuit with a fixed execution schedule was called a *circuit algorithm* there.

³Paths were called tracks in [4]

To simplify notation, we assumed in Setting 1.E that principal inputs and outputs of \mathcal{C} are in the same Hilbert space and that the ancillas and garbage are in the same Hilbert space. Accordingly, in Theorem 1.1, \mathcal{C} computes a unitary operator (rather than unitary transformation) along path μ . The generalization where the two assumptions are dropped is obvious.

Corollary 1.2. *Let \mathcal{G} be a set of computation paths through a quantum circuit \mathcal{C} . Suppose that \mathcal{C} computes a unitary operator along every computation path in \mathcal{G} , possibly different operators along different paths. Then the probability that a computation of \mathcal{C} follows a path in \mathcal{G} does not depend on the input.*

The \mathcal{G} in the corollary can represent the set of good paths mentioned in the motivating paragraphs.

Related work

In 2017, Vadym Kliuchnikov conjectured that, if a quantum circuit computes a unitary operator (the same unitary operator along every computation path), then the probability that its computation follows a particular path does not depend on the input. His conjecture provoked this investigation. We confirm the conjecture.

Corollary 1.3. *Suppose that a quantum circuit \mathcal{C} computes a unitary operator U in the sense that \mathcal{C} computes U along every computation path. Then the probability that a computation of \mathcal{C} follows a particular path does not depend on the input.*

Paul Busch formulated the “no information without disturbance” principle for quantum measurements [2, Theorem 2] and sketched the proof of the principle; a slightly more informative version of his sketch appeared earlier in a book by Paul Busch, Pekka J. Lahti, and Peter Mittelstaedt [3, p. 32]. Busch’s principle is a special case of Corollary 1.3 where \mathcal{C} is just a single measurement and U the identity operator. (Busch works with positive operator-valued measurements, POVMs, rather than general measurements but this is not important for our story. “POVMs are best viewed as a special case of the general measurement formalism, providing the simplest means by which one can study general measurement statistics, without the necessity for knowing the post-measurement state” [7, §2.2.6, Box 2.5]. Under our broader assumptions in Setting 1, POVMs still can be viewed as a special case of the general measurement formalism.)

Organization of this paper

The input independence theorem is proved in the rest of this paper. In order to analyze circuit computation, it is useful to untangle and separate distinct computation paths. We do that in §2 where we introduce measurement trees whose branches can be viewed as their computation paths. The reduction theorem, Theorem 2.4, asserts that for every quantum circuit \mathcal{C} there exist a measurement tree \mathcal{T} and a one-to-one correspondence $\mu \mapsto \beta_\mu$ from the computation paths of \mathcal{C} to the branches of \mathcal{T} such that the probability that computation of \mathcal{C} follows μ on a given (full) input is exactly the probability that the computation of \mathcal{T} follows branch β_μ on that input and the two computations produce the same output.

After investigating some basic properties of measurement trees in §3, we prove the input independence theorem for measurement trees, Theorem 4.1, in §4. By the reduction

theorem, the input independence theorem for circuits follows from that for measurement trees.

Appendix A establishes a function constancy criterion which is used in §4 and which is arguably of independent interest. Relegating that task to an appendix makes the exposition in §4 cleaner. Appendix B is devoted to a generalization of Theorem 1.1.

2 Reduction to measurement trees

As usual we take density operators over a Hilbert space \mathcal{K} to be nonzero, positive semidefinite, Hermitian operators on \mathcal{K} . However, instead of requiring them to have trace 1, we only require them to have finite traces, i.e., to be trace-class operators. The set of density operators over \mathcal{K} will be denoted $\text{DO}(\mathcal{K})$. A density operator is *normalized* if its trace is 1.

Convention 2.1. We use density operators, not necessarily normalized, to represent (possibly mixed) states over \mathcal{K} . A density operator ρ represents the same state as its normalized version $\rho/\text{Tr}(\rho)$. If a measurement $M = \langle L_j : j \in J \rangle$ in the state (represented by) ρ produces outcome j , then we will usually use density operator $L_j \rho L_j^\dagger$ (rather than any scalar multiple of it) to represent the post-measurement state. Notice that $\rho \mapsto L_j \rho L_j^\dagger$ is a linear operator and the probability of outcome j is $\text{Tr}(L_j \rho L_j^\dagger)/\text{Tr}(\rho)$. \triangleleft

To analyze computations of a quantum circuit, it is convenient to represent the circuit by a tree where the computations are represented by branches.

Definition 2.2. A *measurement tree*, a *meas tree* in short, over a Hilbert space \mathcal{K} is a directed rooted tree with a finite bound on the lengths of branches, where every non-leaf node x has a measurement M_x over \mathcal{K} associated to it, and the edges emanating from x are labeled in one-to-one fashion with the classical outcomes of M_x . \triangleleft

All our results about meas trees would remain true if the bounded-branch-length assumption were replaced by a weaker assumption that every branch is of finite length. But the bounded-branch-length trees suffice to support the reduction theory, Theorem 2.4, below.

Let \mathcal{T} be a meas tree. A *route* on \mathcal{T} is a sequence of edges $(x_0, x_1), (x_1, x_2), \dots, (x_{n-1}, x_n)$ where x_0 is the root; it may be given by the labels of those edges: (o_1, \dots, o_n) where o_{i+1} is an outcome of the measurement M_{x_i} . The same notation (o_1, \dots, o_n) may be used for the final node x_n of the route; to avoid ambiguity, we may also use notation $\text{End}(o_1, \dots, o_n)$ for x_n . A route is a *branch* if its final node is a leaf.

View \mathcal{T} as the algorithm which works as follows on input $\sigma_0 \in \text{DO}(\mathcal{K})$. If the root is a leaf (and thus the only node), do nothing. Otherwise, perform the root's measurement in state σ_0 producing, with some probability p_1 , an outcome o_1 and post-measurement state σ_1 . If node $\text{End}(o_1)$ is not a leaf, perform its measurement in state σ_1 producing, with some probability p_2 , an outcome o_2 and post-measurement state σ_2 , and so on until a leaf is reached. Let β be the resulting branch (o_1, o_2, \dots, o_N) . The (quantum) output $\text{Output}_{\mathcal{T}}(\beta|\sigma_0)$ of this computation is the post-measurement state σ_N resulting from the last measurement performed. The probability $P_{\mathcal{T}}(\beta|\sigma_0)$ that computation of \mathcal{T} follows branch β on input σ_0 is $p_1 \cdot p_2 \cdots p_N$.

Consider quantum circuits \mathcal{C} with (full) inputs and outputs in some Hilbert space \mathcal{K} . Assume Setting 1 (so that $\mathcal{K} = \mathcal{H} \otimes \mathcal{A}$ but the internal structure of \mathcal{K} will play no role in this section.) Without loss of generality, we may assume that \mathcal{C} comes with a fixed linear order of its gates.

A *bout* of gates of \mathcal{C} is a nonempty set B of gates where no gate is a (quantum or classical) prerequisite for another gate; thus all B gates could be executed in parallel after all their prerequisites have been executed.

A *schedule* of the circuit is a sequence $(B_1, B_2, B_3, \dots, B_N)$ of disjoint gate bouts such that every gate set $\bigcup_{i \leq n} B_i$ is closed under prerequisites and $\bigcup_{n \leq N} B_n$ contains all the gates.

A schedule is *linear* if all its bouts are (composed of) single gates. Paths through a circuit with linear schedule (G_1, G_2, \dots, G_N) can be represented by sequences (o_1, o_2, \dots, o_N) where each o_n is an outcome of the G_n measurement $\Sigma_{G_n} \langle o_i : G_i \in \text{CS}(G_n) \rangle$.

Lemma 2.3. *Let \mathcal{C} be a quantum circuit with a linear schedule (G_1, G_2, \dots, G_N) with (full) inputs and outputs in Hilbert space \mathcal{K} . There exists a meas tree \mathcal{T} over \mathcal{K} such that for every path μ through circuit \mathcal{C} and every σ in $\text{DO}(\mathcal{K})$ we have:*

1. $\beta_\mu = (\mu(G_1), \mu(G_2), \dots, \mu(G_N))$ is a branch of \mathcal{T} , and every branch of \mathcal{T} is obtained that way,
2. $\text{Output}_{\mathcal{C}}(\mu|\sigma) = \text{Output}_{\mathcal{T}}(\beta_\mu|\sigma)$, and
3. $P_{\mathcal{C}}(\mu|\sigma) = P_{\mathcal{T}}(\beta_\mu|\sigma)$.

Proof. We construct the desired meas tree \mathcal{T} . The nodes of \mathcal{T} are initial segments (o_1, \dots, o_n) of paths through \mathcal{C} . If $n < N$ then segments $(o_1, \dots, o_n, o_{n+1})$ are children of the segment (o_1, \dots, o_n) , the label of the edge from segment (o_1, \dots, o_n) to segment $(o_1, \dots, o_n, o_{n+1})$ is o_{n+1} , and the measurement assigned to segment (o_1, \dots, o_n) is $\Sigma_{G_{n+1}} \langle o_i : G_i \in \text{CS}(G_{n+1}) \rangle$. In particular, the empty segment is assigned the unique measurement of the first gate G_1 . As in the definition of computation paths in Setting 1, this description of children incorporates the coherence requirement for the measurements along the route (o_1, \dots, o_{n+1}) . All three claims are easy to verify from the definition of \mathcal{T} . \square

Given measurements $M_1 = \langle A_i : i \in I \rangle$ and $M_2 = \langle B_j : j \in J \rangle$ over Hilbert spaces $\mathcal{K}_1, \mathcal{K}_2$ respectively, consider the tensor product $M_1 \otimes M_2$, i.e. the measurement $\langle A_i \otimes B_j : (i, j) \in I \times J \rangle$ over $\mathcal{K}_1 \otimes \mathcal{K}_2$. If the probabilities of outcomes i, j on inputs σ_1, σ_2 are p_i, q_j respectively, then the probability of outcome (i, j) on input $\sigma_1 \otimes \sigma_2$ is $p_i \cdot q_j$. The tensor products of more than two (but finitely many) measurements are defined similarly.

The following theorem extends Lemma 2.3 to the case of schedules which may not be linear.

Theorem 2.4 (Reduction). *Let \mathcal{C} be a quantum circuit with (full) inputs and outputs in Hilbert space \mathcal{K} . There exist a meas tree \mathcal{T} over \mathcal{K} and a one-to-one correspondence $\mu \mapsto \beta_\mu$ from the set of paths through \mathcal{C} onto the set of branches of \mathcal{T} such that for every path μ through circuit \mathcal{C} and every σ in $\text{DO}(\mathcal{K})$ we have:*

1. $\text{Output}_{\mathcal{C}}(\mu|\sigma) = \text{Output}_{\mathcal{T}}(\beta_\mu|\sigma)$, and

$$2. \quad P_{\mathcal{C}}(\mu|\sigma) = P_{\mathcal{T}}(\beta_\mu|\sigma).$$

Proof. Let (B_1, B_2, \dots, B_N) be the schedule of \mathcal{C} . By Lemma 2.3, it suffices to construct a circuit \mathcal{C}' with linear schedule admitting a one-to-one correspondence $\mu \mapsto \mu'$ from the paths through \mathcal{C} onto those of \mathcal{C}' so that $\text{Output}_{\mathcal{C}}(\mu|\sigma) = \text{Output}_{\mathcal{T}}(\beta_\mu|\sigma)$ and $P_{\mathcal{C}}(\mu|\sigma) = P_{\mathcal{C}'}(\mu'|\sigma)$ for all σ in $\text{DO}(\mathcal{K})$ and all paths μ through \mathcal{C} .

We construct the desired circuit \mathcal{C}' . The gates of \mathcal{C}' are the bouts B_n of the schedule of \mathcal{C} . If the \mathcal{C} gates of B_n are $F_1 < F_2 < \dots$ (in the fixed order of \mathcal{C} gates), then B_n measurements are tensor products $M_{F_1} \otimes M_{F_2} \otimes \dots$ where each M_{F_j} is an F_j measurement in \mathcal{C} . Since, for every gate F in \mathcal{C} , the outcomes of different F measurements are disjoint, the outcomes of different B_n measurements are disjoint.

Next we define a selection functions $\Sigma'_n = \Sigma'_{B_n}$ for each $n = 1, \dots, N$. A \mathcal{C}' gate B_i is a classical source for a \mathcal{C}' gate B_n if some \mathcal{C} gate in B_i is a classical source for a \mathcal{C} gate in B_n . If the \mathcal{C} gates of B_i are $E_1 < E_2 < \dots$ and, in runtime, they produce outcomes o_1, o_2, \dots respectively, then the outcome $O_i = (o_1, o_2, \dots)$ of B_i is sent to B_n . Note that O_i determines the outcomes of all \mathcal{C} gates in B_i . It follows that, for every \mathcal{C} gate F in B_n , the outcomes O_i determine outcomes of all classical sources E of F in \mathcal{C} , and therefore determine an F measurement M_F chosen by the selection function Σ_F of \mathcal{C} . If the \mathcal{C} gates of B_n are $F_1 < F_2 < \dots$, then $\Sigma'_n \langle O_i : B_i \in \text{CS}(B_N) \rangle = M_{F_1} \otimes M_{F_2} \otimes \dots$.

Finally, for every path μ through \mathcal{C} , we define a path μ' through \mathcal{C}' . For each $n = 1, \dots, N$, we need to define an outcome $\mu'(B_n)$. If the \mathcal{C} gates of B_n are $F_1 < F_2 < \dots$, then $\mu'(B_n) = (\mu(F_1), \mu(F_2), \dots)$. It is easy to see that every path through \mathcal{C}' is obtained this way and that $\text{Output}_{\mathcal{C}}(\mu|\sigma) = \text{Output}_{\mathcal{T}}(\beta_\mu|\sigma)$ and $P_{\mathcal{C}}(\mu|\sigma) = P_{\mathcal{C}'}(\mu'|\sigma)$ for all σ in $\text{DO}(\mathcal{K})$ and all paths μ through \mathcal{C} . \square

3 Cumulative operators

Let \mathcal{T} be a meas tree over a Hilbert space \mathcal{K} . A branch β of \mathcal{T} is *attainable on* input σ in $\text{DO}(\mathcal{K})$ if the probability $P(\beta|\sigma)$ that computation of \mathcal{T} on input σ follows branch β is strictly positive.

Definition 3.1. For every branch $\beta = (o_1, o_2, \dots, o_N)$ of \mathcal{T} , the *cumulative operator* C_β is the composition

$$C_\beta = A_N \circ A_{N-1} \circ \dots \circ A_2 \circ A_1$$

where each A_{n+1} is the operator of the measurement at node $\text{End}(o_1, \dots, o_n)$ that produces the outcome o_{n+1} . In the special case of the one-node tree, the length-zero branch has $C_\beta = \mathbb{1}$. \triangleleft

Notice that, for every input σ in $\text{DO}(\mathcal{K})$, $C_\beta \sigma C_\beta^\dagger$ is exactly $\text{Output}_{\mathcal{T}}(\beta|\sigma)$.

Lemma 3.2.

1. $\sum_\beta C_\beta^\dagger C_\beta = \mathbb{1}$,
2. $P(\beta|\sigma) = \frac{\text{Tr}(C_\beta \sigma C_\beta^\dagger)}{\text{Tr}(\sigma)}$,
3. $P(\beta|\sigma) = 0 \iff C_\beta \sigma C_\beta^\dagger = 0$.

Proof. Induction on the number of non-leaf nodes in \mathcal{T} . \square

By the first two claims of the lemma, the indexed family of operators C_β a measurement (that could be called the *aggregate measurement* of \mathcal{T} in terms of [4]).

Setting 2. Let \mathcal{A} , \mathcal{H} , and $|a\rangle$ be as in Setting 1.E. Consider a meas tree \mathcal{T} with principal inputs and outputs in $\text{DO}(\mathcal{H})$. Like circuits, \mathcal{T} may use ancillas and may produce garbage; the full input of \mathcal{T} has the form $\rho \otimes |a\rangle\langle a|$ where ρ ranges over $\text{DO}(\mathcal{H})$ and $|a\rangle$ is a fixed unit vector in \mathcal{A} . Again, we abbreviate $\rho \otimes |a\rangle\langle a|$ to $\dot{\rho}$. Let U be a unitary operator on \mathcal{H} .

Definition 3.3. \mathcal{T} computes U on principal input ρ along branch β if the operator $\text{Tr}_{\mathcal{A}}(C_\beta \dot{\rho} C_\beta^\dagger)$ agrees with $U\rho U^\dagger$ up to a scalar factor and thus represents the same state. \triangleleft

Corollary 3.4. If \mathcal{T} computes U on principal input ρ along branch β then

$$\text{Tr}_{\mathcal{A}}(C_\beta \dot{\rho} C_\beta^\dagger) = P_{\mathcal{T}}(\beta | \dot{\rho}) \cdot U\rho U^\dagger.$$

Proof. According to the definition of ‘‘computes,’’ the two sides of the claimed equation differ by only a positive scalar factor. So it suffices to check that they have the same trace. Since $\text{Tr}(\dot{\rho}) = \text{Tr}(\rho)$ and, by unitarity of U , $\text{Tr}(U\rho U^\dagger) = \text{Tr}(\rho)$, we have $\text{Tr}(\text{Tr}_{\mathcal{A}}(C_\beta \dot{\rho} C_\beta^\dagger)) = \text{Tr}(C_\beta \dot{\rho} C_\beta^\dagger) = P_{\mathcal{T}}(\beta | \dot{\rho}) \text{Tr}(\dot{\rho}) = \text{Tr}(P_{\mathcal{T}}(\beta | \dot{\rho}) U\rho U^\dagger)$. \square

4 Input independence

We use Setting 2.

Theorem 4.1. Suppose that a meas tree \mathcal{T} computes a unitary operator U on all pure inputs along a branch β . Then there is a vector b in \mathcal{A} such that for all (pure or not) principal inputs $\rho \in \text{DO}(\mathcal{H})$, we have:

1. $C_\beta \dot{\rho} C_\beta^\dagger = U\rho U^\dagger \otimes |b\rangle\langle b|$,
2. the probability $P_{\mathcal{T}}(\beta | \dot{\rho})$ that a computation of \mathcal{T} follows branch β on input $\dot{\rho}$ is $\text{Tr}(|b\rangle\langle b|) = \|b\|^2$ and thus is independent of ρ , and
3. if β is attainable on some input, then it is attainable on all inputs.

Proof. Claim 3 obviously follows from claim 2. Claim 2 follows from claim 1:

$$P_{\mathcal{T}}(\beta | \dot{\rho}) = \frac{\text{Tr}(C_\mu \dot{\rho} C_\mu^\dagger)}{\text{Tr}(\dot{\rho})} = \frac{\text{Tr}(U\rho U^\dagger \otimes |b\rangle\langle b|)}{\text{Tr}(\dot{\rho})} = \frac{\text{Tr}(\rho) \times \text{Tr}(|b\rangle\langle b|)}{\text{Tr}(\dot{\rho})} = \text{Tr}(|b\rangle\langle b|).$$

In the rest of the proof we prove Claim 1.

By the linearity of the equation in Claim 1, we may assume without loss of generality that ρ is pure. Then $U\rho U^\dagger$ is also pure. Since \mathcal{T} computes U on ρ , $\text{Tr}_{\mathcal{A}}(C_\beta \dot{\rho} C_\beta^\dagger)$ and $U\rho U^\dagger$ agree up to a scalar factor. By the Pure State Factor Theorem⁴ in [1, §8.3],

$$C_\beta \dot{\rho} C_\beta^\dagger = U\rho U^\dagger \otimes \xi(\rho)$$

⁴In [1] Ballentine works with normalized density operators, but the theorem remains true, because any positive scalar factor can be shifted to $\xi(\rho)$.

for some (possibly mixed) state $\xi(\rho)$ in \mathcal{A} , and therefore $\text{Tr}(C_\beta \dot{\rho} C_\beta^\dagger) = \text{Tr}(\rho) \times \text{Tr}(\xi(\rho))$. Notice that a mixed state σ is pure if and only if $\text{Tr}(\sigma^2) = \text{Tr}(\sigma)^2$. Since ρ is pure, the states $\dot{\rho}$ and $C_\beta \dot{\rho} C_\beta^\dagger$ are pure. We have

$$\begin{aligned} (\text{Tr}(\rho))^2 \times (\text{Tr}(\xi(\rho)))^2 &= (\text{Tr}(C_\beta \dot{\rho} C_\beta^\dagger))^2 \\ &= \text{Tr}((C_\beta \dot{\rho} C_\beta^\dagger)^2) = \text{Tr}(\rho^2) \times \text{Tr}((\xi(\rho))^2). \end{aligned}$$

Canceling $\text{Tr}(\rho)^2 = \text{Tr}(\rho^2)$, we get $(\text{Tr}(\xi(\rho)))^2 = \text{Tr}(\xi(\rho)^2)$, and so $\xi(\rho)$ is pure as well.

Let $\rho = |\psi\rangle\langle\psi|$. Then there is an \mathcal{A} vector $|f(\psi)\rangle$ such that $\xi(\rho) = |f(\psi)\rangle\langle f(\psi)|$. Thus, $C_\beta \dot{\rho} C_\beta^\dagger = U\rho U^\dagger \otimes |f(\psi)\rangle\langle f(\psi)|$. Hence $C_\beta(|\psi\rangle \otimes |a\rangle) = U|\psi\rangle \otimes |f(\psi)\rangle$ up to a phase, which we absorb into $|f(\psi)\rangle$.

Since $U|\psi\rangle \otimes |f(\psi)\rangle = C_\beta(|\psi\rangle \otimes |a\rangle)$ is linear in $|\psi\rangle$, we can apply the function constancy criterion Theorem A.1 in Appendix A with $V_1 = \mathcal{H}$, $V_2 = \mathcal{H}$, $V_3 = \mathcal{A}$, $L = U$, and f is the function $f(\psi)$. We learn that function $f(\psi)$ is constant, with the same value $|b\rangle$ on all nonzero vectors ψ in \mathcal{H} . So we have $C_\beta(|\psi\rangle \otimes |a\rangle) = U|\psi\rangle \otimes |b\rangle$ for every vector $|\psi\rangle$ in \mathcal{H} . In terms of density operators, $C_\beta \dot{\rho} C_\beta^\dagger = U\rho U^\dagger \otimes |b\rangle\langle b|$ for all pure $\rho \in \text{DO}(\mathcal{H})$ and, by linearity, for all $\rho \in \text{DO}(\mathcal{H})$. \square

Corollary 4.2. *If \mathcal{T} computes U on pure inputs along a branch, then it computes U on all inputs along that branch.*

Proof of Theorem 1.1. The reduction theorem, Theorem 2.4, allows us to transfer the results of Theorem 4.1 from meas trees to circuits. Thus Theorem 1.1 follows from the reduction theorem and Theorem 4.1. \square

A A function constancy criterion

Let V_1, V_2, V_3 be vector spaces, $L : V_1 \rightarrow V_2$ a linear transformation of rank ≥ 2 , f an arbitrary function from V_1 to V_3 , and $\mathcal{L} = L \otimes f$ meaning that $\mathcal{L}x = Lx \otimes fx$.

Notice that, if f is constant, then \mathcal{L} is linear, because L is linear and \otimes is bilinear. The same conclusion follows if f is constant only on those vectors x in V_1 for which $Lx \neq 0$. Indeed, changing the value of fx arbitrarily for those x with $Lx = 0$ has no effect on \mathcal{L} . The following theorem provides a useful converse to this observation.

Theorem A.1. *Suppose that \mathcal{L} is linear. Then $fx = fy$ for all x, y with nonzero Lx, Ly .*

Proof. It suffices to prove $fx = fy$ when Lx, Ly are linearly independent. Indeed, there are vectors v_1, v_2 such that Lv_1, Lv_2 are independent because the rank of L is ≥ 2 . If Lx, Ly are linearly dependent but nonzero, then some Lv_i is independent from both Lx and Ly . Then $fx = fv_i = fy$.

So suppose that Lx, Ly are independent, and choose bases

- v_1, v_2, \dots for V_2 , where $v_1 = Lx$ and $v_2 = Ly$, and
- w_1, w_2, \dots for V_3 , where $w_1 = fx$ and $w_2 = aw_1 + bw_2$ for some scalars a, b .

Then $f(x + y) = \sum_j c_j w_j$ for some scalars c_j . Notice that V_2 and V_3 are arbitrary vector spaces and need not have any inner product specified. Even if they (or some of them) are infinite dimensional, we are talking about bases in the simple sense of linear algebra. Therefore $\sum_j c_j w_j$ is a finite sum, i.e., all but finitely many of the coefficients c_j are 0.

By linearity of L and \mathcal{L} , we have

$$(v_1 + v_2) \otimes \sum_j c_j w_j = (Lx + Ly) \otimes f(x + y) = L(x + y) \otimes f(x + y) = \\ \mathcal{L}(x + y) = \mathcal{L}x + \mathcal{L}y = (Lx \otimes fx) + (Ly \otimes fy) = v_1 \otimes w_1 + v_2 \otimes (aw_1 + bw_2).$$

Vectors $v_i \otimes w_j$ form a basis of $V_2 \otimes V_3$. Comparing the coefficients of basis vectors $v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2$ at the left end and the right end, we have

$$c_1 = 1, \quad c_2 = 0, \quad c_1 = a = 1, \quad c_2 = b = 0,$$

and therefore $fy = 1w_1 + 0w_2 = w_1 = fx$. □

B Isometries

A linear operator L on a Hilbert space \mathcal{K} is an *isometry* if it preserves norms: $\|L|\psi\rangle\| = \||\psi\rangle\|$ for every vector $|\psi\rangle$ in \mathcal{K} [6, Def. 2.10].

Equivalently, L preserves inner products [6, Prop. 3.8]. It follows that a (bounded) linear operator L is an isometry if and only if $L^\dagger L = \mathbb{1}$:

$$\langle L\psi | L\varphi \rangle = \langle \psi | \varphi \rangle \text{ for all } |\psi\rangle, |\varphi\rangle \iff \langle L^\dagger L\psi | \varphi \rangle = \langle \mathbb{1}\psi | \varphi \rangle \text{ for all } |\psi\rangle, |\varphi\rangle \iff L^\dagger L = \mathbb{1}.$$

Notice that a single-outcome measurement consists of a single linear operator L with $L^\dagger L = \mathbb{1}$ and therefore amounts to an isometry.

If L is an isometry then $\text{Tr}(L\rho L^\dagger) = \text{Tr}(L^\dagger L\rho) = \text{Tr}(\rho)$ for all ρ in $\text{DO}(\mathcal{K})$. In finite dimensions $L^\dagger L = \mathbb{1}$ implies that $LL^\dagger = \mathbb{1}$, so that $L^\dagger = L^{-1}$ and L is unitary.

Theorem B.1. *The input independence theorem, Theorem 1.1, remains valid if “a unitary operator” is replaced by “an isometry”.*

Proof. By the reduction theorem, Theorem 2.4, it suffices to prove the version of Theorem 4.1 where “a unitary operator” is replaced by “an isometry”. We walk through the proof of Theorem 4.1 and examine all places where the unitarity is or seems to be used.

- The derivation of Claim 2 from Claim 1 uses only the equality $\text{Tr}(U\rho U^\dagger) = \text{Tr}(\rho)$ which is true for isometries U .
- The application of Pure State Factor Theorem remains valid because, if ρ is a pure density operator $|\psi\rangle\langle\psi|$, then $U\rho U^\dagger = U|\psi\rangle\langle\psi|U^\dagger = |U\psi\rangle\langle U\psi|$ is pure as well for any linear operator U .
- The proof that $\xi(\rho)$ is pure requires only a tiny modification:

$$\begin{aligned} \text{Tr}((U\rho U^\dagger)^2) \times (\text{Tr}(\xi(\rho)))^2 &= (\text{Tr}(U\rho U^\dagger))^2 \times (\text{Tr}(\xi(\rho)))^2 = (\text{Tr}(C_\beta \hat{\rho} C_\beta^\dagger))^2 \\ &= \text{Tr}((C_\beta \hat{\rho} C_\beta^\dagger)^2) = \text{Tr}((U\rho U^\dagger)^2) \times \text{Tr}((\xi(\rho))^2). \end{aligned}$$

Cancelling $\text{Tr}((U\rho U^\dagger)^2)$, we get $(\text{Tr}(\xi(\rho)))^2 = \text{Tr}(\xi(\rho)^2)$, and so $\xi(\rho)$ is pure.

Thus, only the isometricity of U is used in the proof of Theorem 4.1. \square

The following proposition shows that the isometricity requirement in Theorem B.1 cannot be substantially weakened at least in the case where the same linear operator is computed along every computation path.

Proposition B.2. *If a quantum circuit computes the same linear operator U on \mathcal{H} along every computation path, then U is an isometry up to a positive scalar factor.*

Proof. By the reduction theorem, Theorem 2.4, it suffices to prove the meas tree version of the proposition: If a meas tree computes the same linear operator U along every branch β , then U is an isometry.

By claim 1 of Theorem B.1, for every branch β there is a vector b_β in \mathcal{A} such that $C_\beta \dot{\rho} C_\beta^\dagger = U\rho U^\dagger \otimes |b_\beta\rangle\langle b_\beta|$. It follows that

$$\text{Tr}_{\mathcal{A}} \sum_{\beta} (C_\beta \dot{\rho} C_\beta^\dagger) = U\rho U^\dagger \otimes \sum_{\beta} \text{Tr}|b_\beta\rangle\langle b_\beta| = t^2 \cdot U\rho U^\dagger,$$

where $t = \sqrt{\sum_{\mu} \langle b_{\mu} | b_{\mu} \rangle}$. We show that tU is isometric.

Let $|\psi\rangle$ be an arbitrary vector in \mathcal{K} and $\rho = |\psi\rangle\langle\psi|$. By Lemma 3.2, $\sum_{\beta} C_\beta^\dagger C_\beta = \mathbb{1}$. We have:

$$\begin{aligned} \langle tU\psi | tU\psi \rangle &= \text{Tr}(t^2 \cdot U\rho U^\dagger) = \text{Tr}\left(\text{Tr}_{\mathcal{A}} \sum_{\beta} (C_\beta \dot{\rho} C_\beta^\dagger)\right) \\ &= \sum_{\beta} \text{Tr}(C_\beta^\dagger C_\beta \dot{\rho}) = \text{Tr}(\dot{\rho}) = \text{Tr}(\rho) = \langle \psi | \psi \rangle. \end{aligned} \quad \square$$

Corollary B.3. *Suppose that the Hilbert space \mathcal{H} is finite dimensional. If a quantum circuit computes the same linear operator U on \mathcal{H} along every computation path, then U is unitary up to a positive scalar factor.*

References

- [1] Ballentine, L. E. “Quantum mechanics: A modern development,” World Scientific 1998
- [2] Busch P., “No information without disturbance: Quantum limitations of measurements,” In W.C. Myrvold and J. Christian (eds.), “Quantum reality, relativistic causality, and closing the epistemic circle,” 229–256, Springer 2009
- [3] Busch P., Lahti P. J., and Mittelstaedt P., “The quantum theory of measurement,” 2nd revised edition, Springer 1996
- [4] Gurevich Y. and Blass A., “Quantum circuits with classical channels and the principle of deferred measurements,” *Theoretical Computer Science* 920 21–32 2022,
DOI <https://doi.org/10.1016/j.tcs.2022.02.002> arXiv:2107.08324
- [5] Kliuchnikov V., Private communication, 2017

- [6] Moretti V., “Spectral theory and quantum mechanics,” Springer 2013
- [7] Nielsen M. A. and Chuang I. L., “Quantum computation and quantum information,” Cambridge University Press, 10th Anniversary Edition, 2010