Towards a Formal Testing Theory for Quantum Processes

Mohammad Reza Mousavi[1][0000−0002−4869−6794], Kirstin Peters[2][0000−0002−4281−0074], and Anna Schmitt[3][0000−0001−6675−2879]

[1] King's College London, United Kingdom mohammad.mousavi@kcl.ac.uk
[2] University of Augsburg, Germany kirstin.peters@uni-a.de
[3] TU Darmstadt, Germany anna.schmitt@tu-darmstadt.de

Abstract. Hennessy and De Nicola established the foundations of formal testing for (discrete) processes. In this paper, we review the challenges before establishing a formal testing theory for quantum processes. We survey the recent approaches that provide credible attacks to these challenges and propose some directions towards a testing theory for quantum processes.

1 Introduction

Testing is the most widely used quality assurance technique for computer systems and together with debugging accounts for more than half of the development cost of systems [36]. Grounding testing on a formal foundation and coming up with foundational results about the properties of tests is hence an impactful subject that deserves much research. Rocco De Nicola and Matthew Hennessy [38] were among the first, along with other pioneers such as Marie-Claude Gaudel [24], to address this subject. In their seminal work [38], De Nicola and Hennessy developed a formal method of testing for communicating systems. This led to a proliferation of formal process-theoretic notions of test [41, 9, 49, 43, 50] that eventually found their way to industrial practice [40, 7, 18] and made significant impact.

Quantum information technology (including quantum computing and quantum communication) is gaining a growing prospect of applications: quantum communication is already commercialised [27, 42], e.g., with applications in cybersecurity and key distribution; and various applications of quantum computing are being explored, e.g., in drug discovery and simulating complex materials [6, 48]. Modeling and testing quantum systems is challenging, due to their complex nature, e.g., concerning entangled particles and the superposition of states that often escape intuitive explanations [35]. These phenomena have direct practical implications about the state and evolution of quantum systems and what can be known or tested about them (more on this later in this paper). Moreover, there are alternative representations of quantum systems, e.g., state vectors and density matrices, that can be used as a basis for formal modelling and testing [39]. All of these make designing process-theoretic representation of quantum systems

and building a theory of testing for them a non-trivial task. The purpose of this paper is to provide an overview of available results and a roadmap towards a formal theory of testing for quantum systems.

In this paper, we start with reviewing the development of formal notions of testing equivalence and pre-order in classical (discrete and probabilistic) process calculi (Section 2). Subsequently, we give a brief introduction to the peculiarities of quantum systems and the recent attempts to capture them in process calculi (Section 3). This sets the scene for specifying the requirements on a suitable testing pre-order for quantum systems and the challenges in fulfilling them (Section 4). We draw a roadmap based on these observations towards a formal testing theory for quantum processes (Section 5). We conclude the paper by reviewing the findings and summarising our future research plans (Section 6).

2 Formal Testing Theory: Available Results

Testing on discrete and probabilistic systems is well studied. As we observe in Section 3.2, process calculi for quantum based systems combine features of classical discrete and probabilistic systems with quantum features. Accordingly, the testing theories for discrete and probabilistic systems are the foundations for a testing theory for quantum based systems. In the following we briefly review these existing approaches and hint on literature for further information.

2.1 Testing Theories for Discrete Systems

There were two initial proposals for testing pre-orders on communicating processes, put forward by Kennaway [13] and Darondeau [13], followed by the seminal work of De Nicola and Hennessy [38], on one hand, and Brookes, Hoare, and Roscoe [10], on the other. Rocco De Nicola [37] unified these earlier approaches by providing an extensional definition of a testing pre-order. The De Nicola and Hennessy notion of testing pre-order was later extended by Iain Phillips [41] to allow for a negative observation of refusals (the system not engaging on an input) while testing. Brinksma extended this theory to conformance testing [9] to allow for partial specifications. Tretmans [49] introduced input-output conformance, which, as the name suggests, distinguishes between inputs and outputs and bases the test verdicts on observing incorrect outputs (or lack of any outputs at all, called quiescence). Figure 1 provides an overview of these notions and their relative positioning with respect to trace equivalence and bisimulation. (Note that most of these notions can be defined both as a pre-order and an equivalence.) In this paper we mainly talk about bisimulation that is introduced in Section 3.2.

2.2 Testing Theories for Probabilistic Systems

In probabilistic systems, transitions are augmented with probabilities. Larsen and Skou [33] introduced a first framework for probabilistic testing. Based on a

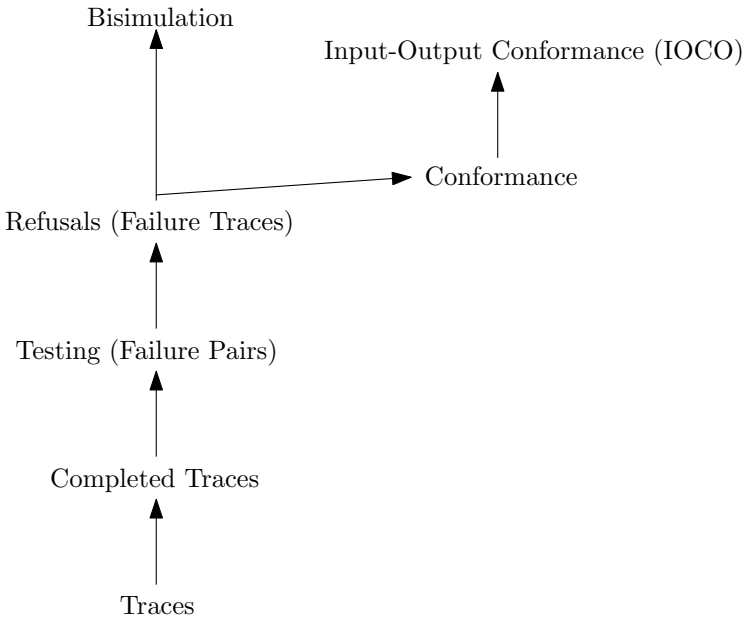

Fig. 1. An overview of formal notions of testing for discrete processes and their positioning with respect to trace equivalence (inclusion) and bisimulation (simulation). An arrow indicates that the source notion is strictly coarser, i.e., relates more systems, than the target notion. The notions are briefly introduced in Section 2.1.

probabilistic transition system as the underlying model for processes, they define a logical framework and operational tests to test properties with arbitrarily high probability. To this end, they follow the ideas of Abramsky [1] and allow multiple copies of the process at any stage of the test. By running the same test on several copies, the probability of success can be approximated. In [8, 51] the characterisation of Larsen and Skou [33] is generalised to the more general setting of labelled Markov processes with continuous state spaces. Again the tester is allowed to make multiple copies of a process in order to experiment independently on one copy at a time. This feature is considered crucial for capturing branching-time equivalences (see [8]). A comparison of different testing equivalences for non-deterministic and probabilistic processes can be found, e.g., in the papers by Bernardo et al. [4, 5].

3 Quantum Systems and Process Theories

We provide a brief introduction to quantum systems and then review process calculi for quantum-based systems and variants of bisimulation developed on these calculi.

3.1 Quantum Systems: Brief Introduction

Quantum systems have access to a register of *quantum bits (qubits)* on that they can perform quantum transformations and measurements to retrieve some information about their current states. The transformations that describe the changes in closed systems are *unitary transformations*. See, e.g., the text book by Nielsen and Chuang [39] for a formal definition of unitary transformations as well as of the following introduced concepts. Note that unitary transformations are reversible. To describe open systems, i.e., interactions with an unknown environment, so-called *super-operators* are used. This is used, for instance, to model noise on *quantum channels*, i.e., channels to transfer qubits. For every unitary transformation there is a super-operator with the same behaviour, but there are super-operators that cannot be precisely expressed as unitary transformations.

In case of a distributed quantum system, any process of the network has access to its own quantum registers (there are, however, some possible couplings among qubits in distributed processes, as described below).

The main difference between a classical bit and a qubit is an effect called *superposition*. While the state of a classical bit is one of two possible Boolean values, typically denoted by 0 and 1, the state of a qubit may be a combination of the two states 0 and 1 with specific amplitudes. The states of qubits are usually written in ket-notation, e.g., $|0\rangle$ is the state that is fully in state 0 (in state 0 with amplitude 1, and in state 1 with amplitude 0). Likewise, a single qubit that is fully in state 1 is denoted by $|1\rangle$. Qubits in superposition are then denoted by $\alpha|0\rangle + \beta|1\rangle$, where the non-zero amplitudes α and β are complex numbers such that $\alpha^2 + \beta^2 = 1$.

Another difference is that the classical bits are always specified on the same basis, namely, 0 and 1. However, the state of the qubit register is usually described by a vector space, i.e., a (finite-dimensional) Hilbert space, and a qubit can be measured with respect to different bases. The basis $\{|0\rangle, |1\rangle\}$ is called the standard basis. The Hadamard basis $\{|+\rangle, |-\rangle\}$ is also frequently used.

Although the current state of a qubit may be specified as a probability distribution of 0 and 1 after measurement, a qubit is **not** a probabilistic variable. A qubit in superposition is indeed in a combination of states at the same time. More importantly, the state of two qubits can be *entangled*: the state of an n-qubit system is not specifiable in terms of n independent random variables. That is why operations on an n-qubit system have the potential of modifying them in tandem, a phenomenon that is sometimes referred to as quantum parallelism [39]. It is, however, very challenging to exploit this type of parallelism to obtain substantial savings in computational complexity. One of the best known success stories in this regard is Shor's algorithm [45, 46] for prime factorisation in polynomial time.

Entanglement connects the states of two qubits in superposition. Measuring a qubit may affect the state of other qubits if there is entanglement. There are different ways to entangle qubits. For instance, there are the so-called Bell's states or EPR pairs for two fully entangled qubits. In the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ the two qubits are in superposition but their states are not in-

dependent. After measuring either one of the two qubits (on a standard basis) resulting in either 0 or 1 for the measured qubit, the state of the other qubit is also immediately reduced to $|0\rangle$ or $|1\rangle$, respectively. Because of that, a subsequent measurement of the other qubit will result in exactly the same value as the first measurement. The effect is instantaneously and independent of space. Hence, it does not matter how much time may pass between the two measurements (or whether any time passes at all) nor does it matter how far the two qubits are separated in space. Note that it is possible to locally entangle qubits and then to communicate these qubits without destroying the entanglement.

Entanglement can be used to ensure the absence of eavesdroppers in a distributed system with arbitrary large probability. This is used in quantum key distribution protocols such as the BB84 protocol [3, 47]. Entanglement can also cause practical problems: it is difficult to keep a quantum register stable, i.e., to ensure that all state changes are intended and caused by explicit operations on the qubits. Therefore, qubits have to be isolated from their environment, because entanglement with particles in the environment can cause unintended and unpredictable state changes.

A drawback of qubits and the main reason that limits the applicability of superposition to algorithms is that it is impossible to retrieve the exact state of a qubit. Qubits **cannot** be read or copied, but only measured and a measurement destroys the state in superposition and drags it to one of the bases of the measurement, with probabilities proportional to the square root of the amplitudes α and β, specified above. Only if α is one (and thus β is zero) or vice versa, the respective value is returned. Else, the result of measurement is described by a probability distribution, but a single measurement will return either one of the values.

To retrieve full information about the state of a qubit in superposition, one needs to perform many measurements and reconstruct the probability distribution from these measurements. For an n-qubit system the situation is much worse and one needs to perform an exponential number of measurements (in the number of qubits) to reconstruct the entangled state of the system, a problem referred to as full tomography [39]. There are practical ways to avoid this exponential blow-up by trading the number of measurements for less information or less precise information [30].

A direct consequence of the impossibility to read a qubit is the *no-cloning principle*. It states that it is impossible to make an exact copy of an unknown qubit state, because that would require to read the qubit.

3.2 Quantum Process Theories

The first programming languages for quantum systems were developed in the 90'th. For further information, we refer to the surveys on the early research of such languages, e.g., in [44, 25]. To analyse quantum programs, different quantum process calculi and behavioural equivalences have been proposed. Among the earliest calculi were [31, 26]. As bisimulation is the most important behavioural

equivalence for classical systems, research currently focus'es on variants of bisimulation for the quantum case. Moreover, to allow for a compositional analysis of programs, congruences are desired. The formulation of quantum bisimulation that is a congruence with respect to parallel composition turned out to be one of the main challenges in the study of quantum process calculi.

Consider a set of terms—that are either processes or configurations as explained below—and a labelled semantics $\dot{\rightarrow}$ such that $X \xrightarrow{\alpha} X'$ is a transition from term X with label α to the term X'. X' is denoted as continuation. A symmetric relation $\mathcal{R}$ is a strong (labelled) bisimulation if whenever $(X,Y) \in \mathcal{R}$ then $X \xrightarrow{\alpha} X'$ implies $Y \xrightarrow{\alpha} Y'$ for some Y' such that $(X',Y') \in \mathcal{R}$. For weak (labelled) bisimulation, we distinguish a special label τ that is usually used to denote an unobservable (or internal or silent) transition. Moreover, we use * to denote the reflexive and transitive closure. A symmetric relation $\mathcal{R}$ is a weak bisimulation if whenever $(X,Y) \in \mathcal{R}$ then $X \xrightarrow{\alpha} X'$ implies that either $\alpha = \tau$ and $(X',Y) \in \mathcal{R}$ or $Y \xrightarrow{\tau}{}^* \xrightarrow{\alpha} \xrightarrow{\tau}{}^* Y'$ for some Y' such that $(X',Y') \in \mathcal{R}$. A symmetric relation $\mathcal{R}$ is a branching bisimulation if whenever $(X,Y) \in \mathcal{R}$ then $X \xrightarrow{\alpha} X'$ implies that either $\alpha = \tau$ and $Y \xrightarrow{\tau}{}^* Y'$ such that $(X,Y'), (X',Y') \in \mathcal{R}$ or $Y \xrightarrow{\tau}{}^* Y_1 \xrightarrow{\alpha} Y_2 \xrightarrow{\tau}{}^* Y'$ such that $(X,Y_1), (X',Y_2), (X',Y') \in \mathcal{R}$. Alternatively, the semantics can be given as an unlabelled, so-called reduction semantics $\longmapsto$, where a reduction is a transition $X \longmapsto X'$ from X to X'. The definition of strong reduction bisimulation is obtained from the above by omitting the labels. A symmetric relation $\mathcal{R}$ is a weak reduction bisimulation if whenever $(X,Y) \in \mathcal{R}$ then $X \longmapsto X'$ implies $Y \longmapsto^* Y'$ for some Y' such that $(X',Y') \in \mathcal{R}$. To compensate for the missing labels, (strong or weak) reduction bisimulation is usually enhanced by requiring that X and Y with $(X,Y) \in \mathcal{R}$ have to have the same barbs. The definition of processes, labels, and barbs may vary for different calculi. Two terms are (weak/strong/branching labelled/reduction) bisimilar if there is a (weak/strong/branching labelled/reduction) bisimulation that relates them.

Measurement reveals the probabilistic nature of qubit states. Accordingly, the semantics of quantum based process calculi has to deal with probabilities. A transition into a probability distribution is of the form $X \xrightarrow{\alpha} \Delta$ or $X \longmapsto \Delta$, where Δ is probability distribution over terms. To capture transitions into a single term, Δ may be a point distribution consisting of a single case X with probability 1. A symmetric $\mathcal{R}$ is a strong (labelled) bisimulation if whenever $(X,Y) \in \mathcal{R}$ then $X \xrightarrow{\alpha} \Delta$ implies $Y \xrightarrow{\alpha} \Theta$ for some Θ such that $(\Delta,\Theta) \in \overline{\mathcal{R}}$. The definition of $\overline{\mathcal{R}}$ may vary. In the simplest case it requires that all cases of the two distributions are pairwise related by $\mathcal{R}$ and have the same probability. A more relaxed version requires that the two distributions split into equivalences classes modulo $\mathcal{R}$ with pairwise the same sum of probabilities. The probability to perform an action is the sum of all probabilities of all branches that perform this action, where the probability of a branch is the product of its probabilities. The other notions of bisimulation discussed above are adapted in the same way. A probabilistic transition, i.e., a transition augmented with a probability, can be used to move to one case of a probability distribution. Again the notions of bisimulation can be adapted to probabilistic transitions, where usually the same

probability is required for matching transitions. Usually measurement is the only action that leads to a probability distribution.

A relation $\mathcal{R}$ on processes is a congruence w.r.t. parallel composition $|$, if $(P, Q) \in \mathcal{R}$ implies that $(P \mid R, Q \mid R) \in \mathcal{R}$ for all R. One problem for the quantum case is the quantum register that captures the current state of qubits, but has to do that in a non-compositional way as a global view on all qubits. Because of that, the semantics of quantum process calculi is usually not defined as a relation between processes but between configurations, where a *configuration* (P, σ) is the composition of a process P and (the current state of) a quantum register σ. Consequently many behavioural relations in the quantum case are defined between configurations (or probability distributions over configurations) rather than processes, but the congruence property is defined on processes. To obtain a congruence, such relations between configurations have to be lifted to relations between processes. The main technique, denoted here as *forall-states-lifting*, works as follows: Given a relation $\mathcal{R}$ on configurations, its lifting is the relation on processes that relates the processes P and Q whenever $((P, \sigma), (Q, \sigma)) \in \mathcal{R}$ for all register σ.

QPAlg. The *Quantum Process Algebra* (QPAlg) in [31, 32] combines CCS-style value passing via classical channels with the communication of qubits via quantum channels, where no clear distinction between the different kinds of channels is imposed. Moreover, it contains a non-deterministic and a probabilistic choice, unitary transformations, measurement, and standard CCS-operators. The semantics is given as a labelled transition system between configurations with probabilities and non-determinism. There are labels for sending, receiving and the silent action τ, where in qubit communication labels contain the name of the qubit but not its state and where unitary transformations and measurement are silent. The semantics of QPAlg forbids transitions until a probability distribution over configurations as result of measurement is resolved by a probabilistic transition to a single case.

As behavioural equivalences on configurations, probabilistic branching bisimulation and probabilistic rooted branching bisimulation are introduced in [32]. The former relation is weak and probabilistic, because bisimilar processes must perform an action with the same label with the same probability. Since it is defined on configurations, probabilistic branching bisimulation in [32] is not a congruence. Also its forall-states-lifting is not a congruence.

To obtain a congruence, the latter, stricter relation is given. In particular, probabilistic rooted branching bisimulation is strong—though derivatives have to be related by the former, weak relation only—and requires that in sending/receiving a qubit also the respective states of the transmitted qubits have to be the same. Then the forall-states-lifting is claimed to be a congruence except for parallel composition. Note that entanglement is identified already in [32] as the main problem in defining a bisimulation that is a congruence with respect to parallel composition.

CQP. Communicating Quantum Processes (CQP) in [26] are a quantum extension of the π-calculus [34]. In addition to the standard constructs of the π-calculus, qubits can be transmitted, altered using unitary transformations, and measured. A static type system rules out impossible processes, that violate the no-cloning principle. Channel names can be constructed from expressions that are constructed from values, data operators, unitary transformations, and measurement. The type system ensures that such expressions refer to a channel name. The semantics is given by reductions into a probability distribution over configurations. A probabilistic transition reduces a distribution to one of its cases. In [26] there is no conditional guard to base future behaviour of processes on the outcome of measurement. As claimed such operators can be easily added and indeed a later version of CQP in [23] contains it.

Bisimulation for CQP is discussed in [14, 23]. Therefore, the bisimulations of [32] for QPAlg and [20, 52] for qCCS (see below) are reviewed and compared. In contrast to [20, 52], the bisimulation should not focus on the final states of the register and, in contrast to [32], it should better cope with parallel contexts. The resulting weak probabilistic branching bisimulation is similar to [32], but treats non-determinism differently. The application of unitary transformations and measurement are labelled by τ. Two probabilistic transitions cannot be directly subsequent without a reduction in between. Configurations are separated into probabilistic configurations, i.e., configurations that can perform a probabilistic transition, and the remaining non-deterministic configurations. Probabilistic branching bisimulation is an equivalence $\mathcal{R}$ between configurations such that $(s,t) \in \mathcal{R}$ implies that a transition of s has to be weakly simulated by t, the states of transmitted qubits have to coincide in the continuations after sending and receiving of qubits, and if s is a probabilistic configuration then the equivalence classes in s and t have to have the same probabilities. Because a context may capture the free names of a process, the forall-states-lifting of probabilistic branching bisimulation is no congruence. Instead of the forall-states-lifting, the so-called full probabilistic branching bisimilarity relates two processes if for any substitution on free qubit names and all states of the quantum register the configurations (of the respective process and the considered state) are probabilistic branching bisimilar. This relation is a congruence except for parallel composition.

To obtain a congruence (also w.r.t. parallel composition) [14, 23] then introduces *mixed configurations*, that pair a process with a weighted distribution of classical values and quantum states. The classical values instantiate the free variables of the process. Then the labelled transition system and the type system is adapted to mixed configurations. Note that measurement produces a mixed instead of a probabilistic configuration and after sending a mixed configuration reduces to a probability distribution on mixed configurations. This allows to postpone probabilistic branching until there is some visible information that distinguishes the branches. An output of classical values that may differ for the cases of a mixed configuration causes a probability distribution. Then probabilistic branching bisimulation is an equivalence $\mathcal{R}$ between mixed configurations

such that $(s,t) \in \mathcal{R}$ implies that a transition of s has to be weakly simulated by t, the states of transmitted qubits have to coincide in the continuations after sending and these continuations have to have the same probabilities with related mixed configurations, and if s is a probabilistic (mixed) configuration then the equivalence classes in s and t have to have the same probabilities. The forall-states-lifting of this relation is shown to be a congruence except for input and qubit declaration. Finally, the forall-states-lifting of full probabilistic branching bisimulation is a congruence.

qCCS. The calculus qCCS in [20–22] is a quantum extension of classical value-passing CCS [29]. In contrast to QPAlg, the syntax of qCCS rules out systems that are impossible, because they violate the no-cloning principle. Therefore, they require that a receiver of a qubit should not know this qubit before its reception, the sender loses any access to the transmitted qubit, and parallel composed processes cannot share access to the same qubits. The syntax allows to transmit classical values as well as qubits, qubits can be manipulated by unitary transformations and measurement, and there is non-deterministic choice. The semantics is again probabilistic and labelled. In contrast to QPAlg, distributions over configurations are not reduced to one case, but a subsequent transition has to be performed separately for every configuration in the distribution.

First versions of weak and strong bisimulation for qCCS are presented in [20]. Terminated configurations are strongly bisimilar only if they have the same register. Note that this requirement on terminated configurations does not fit well with recursive processes. The forall-states-lifting of strong/weak probabilistic bisimulation is shown to be a congruence but not with respect to the restriction operator and only a limited form of parallel composition. For parallel composition either the parallel context does not contain unitary transformations nor measurement or the related processes do not contain quantum input. Again, entanglement prevents the defined relations from being a congruence with respect to general parallel composition.

Another challenge for a bismulation that is a congruence with respect to parallel composition is pointed out in [52]; namely the combination of classical and quantum information. Accordingly, [52] presents a version of qCCS with pure quantum processes without any classical information. In contrast to [20], super-operators can be used. Usually measurement bridges between quantum and classical information, because the information obtained from measuring a qubit is classical. Here measurement is not a separate operator but is implemented via super-operators. Hence, measurement influences the state of the quantum register and may set a qubit to a classical value, but there is no operator to retrieve or utilize the information gained by measurement about a qubit state. As a direct consequence, the semantics of pure quantum qCCS is given by a non-probabilistic labelled transition system. Moreover, qubit manipulation by super-operators is not silent but labelled by the respective super-operator. A strong bisimulation is given, that requires the simulation of every step but (in contrast to [20]) does not require the equality of states of terminated configurations. It is shown that the forall-states-lifting of strong bisimilarity is a congruence w.r.t. all opera-

tors in pure quantum qCCS (including general parallel composition). However, the exclusion of classical data limits the applicability of pure quantum qCCS. Moreover, since labels contain applied super-operators, the discussed bisimilarity distinguishes processes that obtain the same behaviour via different sequences of super-operators. To gain more flexibility, so-called strong reduction bismilarity is introduced that allows to collapse a sequence of applications of super-operators to a single application of a super-operator. Again the forall-states-lifting is a congruence. Finally, [52] also studies a variant of approximate bisimulation using a distance between the applied super-operators.

[21] studies again qCCS with quantum and classical information, i.e., combines the calculi of [20] and [52]. The semantics is again probabilistic, measurement is a separate operation that provides classical information about states, and the application of super-operators and measurement is silent. A weak bisimulation between configurations is defined. After the reception of a qubit, bisimulation additionally requires that the two continuations Δ, Θ are related after the application of an arbitrary super-operator $\mathcal{E}$, i.e., $(\mathcal{E}\Delta, \mathcal{E}\Theta) \in \mathcal{R}$. The requirement of [20] on terminated configurations is replaced by requiring that the quantum register of all bisimular configurations have to have the same trace[4], because the latter requirement is also meaningful for non-terminating configurations and better to deal with restriction. Moreover, bisimilar configurations have to have the same set of free qubits. The forall-states-lifting of this weak bisimulation is a congruence with respect to all operators of qCCS including general parallel composition but excepting (similar to the classical case) non-deterministic choice. To also capture non-deterministic choice, an equivalence based on the bisimulation is defined, that requires that a silent transition has to be simulated by at least one silent transition. The forall-states-lifting of this equivalence is a congruence for qCCS.

The papers [16, 22, 15] relax the above congruence, i.e., they provide strictly coarser versions that also relate processes that should intuitively not be distinguished. The open bisimilarity in [16] allows to separate ground bisimulation and the closedness under super-operator applications. Open bisimularity is closed under all qCCS operators except for non-deterministic choice. [16] also presents an extension of Henessy-Milner logic with a probabilistic choice modality by a super-operator modality and atomic formulae involving projectors for dealing with quantum states. Note that all of these relaxations still require that the states in the quantum registers of bisimilar processes are equivalent. In [22] open bisimulation is lifted to a relation on probability distributions, called distribution-based bisimulation. Instead of single configurations it considers probability distribution over configurations. Moreover, a bisimulation distance is defined in [22]. Also [15] gives a distribution-based quantum bisimulation. [22] and [15] both use the technique from [17] to lift a relation on configurations to a relation on probability distributions over configurations. In contrast to [22], [15] provides a slightly coarser distribution-based quantum bisimulation.

[4] Here trace refers to a property of a quantum register that is used to compare the states of different quantum registers. See [39] for a formal definition.

Since quantum states constitute a continuum, the requirement on equivalent states that is present in all of the above bisimulation variants is a problem for algorithms that check bisimilarity. To overcome this problem, [19] presents a symbolic transition system and a bisimulation on processes without the need to check quantum states. Note that for every state of a quantum register there is a super-operator that generates this state. Moreover, several sequential applications of super-operators can be collapsed into a single super-operator. Configurations are made symbolic in [19] by replacing the state of the quantum register by a super-operator that generates it. In the symbolic semantics on symbolic configurations, transitions compute a new super-operator instead of a new state for the continuation. Symbolic (strong open) bisimulation relates symbolic configurations $(P, \mathcal{E})$ and $(Q, \mathcal{F})$ with the same free qubit variables and similar states $\mathcal{E}, \mathcal{F}$ if for all super-operators $\mathcal{G}$ transitions of $(P, \mathcal{GE})$ are simulated by $(Q, \mathcal{GF})$ such that the resulting distributions Δ, Θ are related if $\mathcal{GE}$ is applied to all states of Δ and $\mathcal{GF}$ is applied to all states of Θ. Symbolic bisimulation is shown to coincide with open bisimulation of [16] and can be split again into a ground bisimulation and super-operator applications. Since super-operators form a continuum, the closure over applications of super-operators is hard to check algorithmically, but an algorithm to check symbolic ground bisimulation is presented in [19]. Also a Henessy-Milner type model logic is given, that contains super-operators.

lqCCS. Linear quantum CCS (lqCCS) is introduced in [11] as another extension of CCS by quantum operations. It is inspired by qCCS, but (1) communication is asynchronous, i.e., senders have no continuation, (2) the process for inaction allows to keep the ownership of qubits, such that they cannot be manipulated by a context, and (3) is linearly typed, i.e., the type system ensures that every qubit is send exactly once or discarded by being claimed by an inactive process. The semantics is given via reductions into distributions over configurations. Two versions of strong, barbed bisimulation between probability distributions on configurations are presented, where barbs are the channels of unguarded senders equipped with the probability of the sender in the considered probability distribution. Hence, barbs are on classical (and probabilistic) information only.

Saturated bisimulation—that is introduced as an intermediate step—relates two distributions with the same barbs if for every observer a reduction of one observed system is answered by a reduction of the other observed system such that the resulting probability distributions are again related. An observer is here an arbitrary lqCCS process placed in parallel to the considered system, i.e., to the process of all cases of the distribution.

Constrained bisimulation is defined in the same way, but the observers are restricted. Restriction is forbidden in observers and choice is limited to input guarded choice on distinct channel names. Moreover, the semantics is revised to limit the interactions of observers. Observers can no longer reduce by communicating with themselves, which does, however, not limit their observation power, but ensures that choices of observers are decided by the sending observed process and not the observer. All choices of the observer have to be based on classical information. Also forbidding restriction does not decrease the discrim-

inating power of observers. Observers are still non-deterministic, but different non-deterministic choices can be distinguished by different indices on the reductions they produce. The forall-states-lifting of constrained bisimilarity is not a congruence w.r.t. parallel composition.

The authors [11] then compare the bisimulations on QPAlg in [32], CQP in [14], qCCS in [16] and [22], and their bisimulations on lqCCS. They observe that they disagree on several simple cases that are likely to occur in the analysis of quantum protocols. More precisely, they give counterexamples that show that the bisimulations on QPAlg in [32], CQP in [14], qCCS in [16] and [22], and constrained bisimulation on lqCCS are pairwise different notions of bisimulation. They also point out that there are no formal proofs that relate features of the before mentioned bisimulations to quantum theory and the indistinguishability it implies. We briefly review their comparison.

The first considered example consists of two systems that first receive a qubit via the same channel, then change this qubit using different unitary transformations, and then terminate. The bisimulations of QPAlg in [32] and CQP in [14] do not distinguish these systems, because they consider the state changes of the qubit as not visible. By the qCCS bisimulations in [16] and [22] the two processes are distinguished, because the resulting quantum states differ. For lqCCS this situation is avoided all together, by requiring that each qubit has to be sent or discarded exactly once. With that lqCCS ensures that all state changes to qubits are visible. If termination is replaced by the inactive process that claims the ownership of the qubit, the systems are related by all six considered bisimulations. If instead termination is replaced by sending the qubit over a new channel, then all six considered bisimulations do not relate the systems.

In quantum theory the probability distributions of quantum states should be indistinguishable if they are represented by the same density operator (see [39] for a formal definition). The bisimulation of QPAlg in [32], open bisimulation of qCCS in [16], and saturated bisimulation of lqCCS violate this principle. This is shown by an example P, Q, where a qubit is set to $|+\rangle$ in P and $|0\rangle$ in Q then measured w.r.t. the standard base in P and the Hadamard base in Q and then transmitted via the same channel in P and Q. After measurement the state of the respective qubit is with equal probability either in $|0\rangle$ or $|1\rangle$ for P and $|+\rangle$ or $|-\rangle$ for Q. These two probability distributions should be indistinguishable. That these processes are wrongly distinguished is, according to [11], caused by the combination of non-determinism and quantum features. Therefore, the non-determinism in observers is restricted for constrained bisimulation such that the mentioned two procesess are related. To show that the bisimulations of CQP in [14] and qCCS in [22], that also relate these two processes, overly constrain non-determinism, the sending of the qubit is replaced by a non-deterministic choice with two cases that both send the qubit but on different channels. The bisimulations of CQP in [14] and qCCS in [22] still relate the systems, but constrained bisimulation now distinguishes them. This is because, a context may use measurement and a boolean guard based on the result of measurement to chose between the two channels.

Ceragioli1, Gadducci, Lomurno, and Tedeschi [12] define a notion of tests for quantum processes in lqCCS [11], discussed above. Therefore, they again consider the parallel compositions of lqCCS-processes and observers. The latter contain a deadlock state to mark success, i.e., a test is successful if the system of process and observer leads to the success state. Based on this notion of successful test, a testing equivalence is defined that relates processes if they pass the same tests with the same probabilities. Their focus is on ensuring that states that should not be considered as observably equivalent are not distinguished. The interaction between nondeterministic and probabilistic choice is known, thanks to the earlier work of the authors [11], to cause issues for testing pre-orders. The latter is inherent (and possibly exacerbated) in the context of quantum processes, as demonstrated by the authors. Hence, the authors suggest a way to mitigate this problem by restricting the language of tests to deterministic ones. They prove that this restriction resolves the problem and does not distinguish between observably equivalent states.

4 Quantum Testing Pre-Orders: Requirements and Challenges

Several proposals have been put forward for defining a theory of quantum processes. In some of these proposals, a notion of behavioral equivalence or pre-order has also been provided. However, none of these seem to provide a satisfactory foundation for a testing theory of quantum processes. Below, in Section 4.1 we set forth the requirements on such a satisfactory foundation and argue why the existing proposals come short of satisfying them.

4.1 Requirements

There are several requirements for a satisfactory theory of testing for quantum process. Some basic requirements are common to discrete and probabilistic processes; these include the notion of testing being a pre-order, compositional, and having intensional and extensional representations. Although these requirements are generic, realising them in the context of quantum processes may be particularly challenging as we describe below. A requirement that is specific to the context of quantum processes is that the observational power of a notion of testing should match quantum observability.

Pre-order. A desired requirement for a formal notion of testing is that it should be reflexive, i.e., any system should pass all tests when the system itself is given as its specification. Likewise, a suitable notion of testing is expected to be transitive in order to allow for stepwise refinement. While these two properties turn out to be straightforward for many formal theories (e.g., strong bisimulation and trace equivalence), they turn out to be challenging [2] or even impossible for some others [49]. Particularly, for formal testing theories that allow for partial specifications, this became a major road block leading to a major redesign of

well-known theories, such as the notion of input-output conformance testing (ioco) [50]. As there are no current theories for quantum testing that allow for partial specification, it is unclear how challenging this requirement will turn out, but we expect the same challenges as for discrete testing theories to hold here.

Compositionality. Real world applications are usually large and often developed in a modular way. Therefore, behavioural equivalences should allow to analyse parts of systems and then conclude on the properties of the systems by composing the properties of its parts, i.e., should be a congruence in particular w.r.t. parallel composition. In the quantum based setting giving a congruence is often challenging as observed independently by several approaches discussed in Section 3.2.

Intensional and extensional representation. There are two major approaches to defining a formal testing theory:

- an intensional (white-box) definition: in this approach one assumes access to the model of both specification and implementation and an implementation conforms to a specification if all the observable behaviours that can be generated from the implementation model are included in those of the specification model.
- an extensional (black-box) definition: in this approach, one only assumes access to the model specification. Conformance is checked by generating tests from the specification model and executing them against a black-box implementation. An implementation conforms to a specification if the result of executing all such executions is a pass.

Ideally, a formal theory of testing should come with both such definitions and a proof that they coincide. The advantage of having both definitions is that they reflect different intuitions and thought processes and their coincidence provides more assurance of the suitability of the definitions. Since many approaches in the literature require the comparison of quantum states (e.g. in [32, 14, 23, 20]), they are rather intensional. A concrete intensional approach can be found in [11, 12]. They specify observers (as specifications) to be placed in parallel with the processes (implementation) and define a testing equivalence. The syntax of observers thereby provides the set of tests that can be run. We did not find any real extensional approaches to testing. Henessy-Milner logics are given in [16, 19] for qCCS, but they contain super-operators that form a continuum. Because of that the practicability of these logics in an extensional approach that may e.g. consist of buttons to test a system is limited.

Respecting quantum principles of observability. The actions of quantum systems usually combine classical actions with quantum specific actions such as the transmission of qubits, measurement, and other quantum transformations.

Observing the transmission of qubits is more difficult in quantum systems. As in classical systems, we may easily observe the channel used for the transmission and whether it was a sending or receiving action. However, we cannot observe the

state of the transmitted qubit. The reason is, that it is in general impossible to read the state of a qubit. We can only measure it and, as explained in Section 3.1, measurement provides only incomplete knowledge about the state of a qubit.

Measurement (or any other transformation of qubits) is a local operation that is not directly visible by the rest of the system, but changes the state of qubits. Hence, it is more natural to model measurement and transformations of qubits as internal and not observable actions. Accordingly, the applicability of approaches such as [52] for testing is limited. Note, however, that measurement does not only affect the state of the measured qubit but also of entangled qubits. Because of the latter, the effect of measurement is not completely local. Nonetheless, it is not directly observable. This has to be taken into account, when building a testing framework for quantum systems.

Moreover, the combination of non-determinism and quantum features can be problematic for the observable behaviour as pointed out in [11]. They explicitly restrict the non-determinism in observers to ensure that distributions on quantum states that are indistinguishable by quantum theory are not distinguished. Note also that [11] is the only approach discussed in Section 3.2 with an explicit notion of barbs and that it considers only classical available information in them.

4.2 Challenges

Stateless formulation. As explained in Section 3, quantum systems are usually modelled with an explicit and global quantum register. The current state of the quantum register influences the future behaviour of the quantum system. However, states are not directly observable and hence difficult to test. Therefore, many testing frameworks consider stateless formulations of bisimulation, but many quantum based bisimulations are not stateless (see Section 3.2).

In classical systems we may ask for the current state of a classical register to be communicated. In quantum based systems the situation is more difficult. On the one hand side, transmitting a qubit destroys its state on its original location. On the other hand side, receiving a qubit does reveal only partial information about its state, since the state can only be measured.

Analysing the congruence-relations in Section 3.2 we observe that they heavily rely comparing quantum states or super-operators. The bisimulation in [23] for CQP checks the states of transmitted qubits. In [52] for pure qCCS super-operators are used as labels and in [21] for qCCS the states of terminated configurations are compared. Symbolic approaches such as [19] may help to overcome this problem, but the closure over super-operators used in [19] is again a problem for algorithms checking bisimulation.

Another problem is pointed out in [11, 12]. The strong focus on concrete states results in equivalences that wrongly distinguish processes by different but observably equivalent states.

No-cloning principle. It is impossible to exactly copy an unknown quantum state (cf. [39]). It is possible to communicate a quantum state, i.e., to transfer it, but by doing so the original quantum state gets destroyed. Intuitively, copying a

quantum state would require a method to read a quantum state. However, quantum states cannot be read, but only measured (see Section 3.1). Since copying is impossible and since measurement destroys the current quantum state, all that we can learn by measuring is one of the possible values of the state.

As described by Larsen and Skou [33], the main idea of probabilistic testing is to approximate the probability of a test result by running the same test several times on different copies of the process. Moreover, for bisimulation it is essential that we can test different copies of an intermediate state of the system to analyse the branching structure of the system. Hence, the method described in [33] requires to copy the process at any stage of the test. Because of the no-cloning principle, this is impossible for quantum based systems or, more precisely, for the state of its quantum register.

Note that the results of measurement can be used in many of the approaches in Section 3.2 to decide on the future behaviour of the process. Hence, a separation of control in the processes and the state in the register is not trivial. We could not find any approach that supports this kind of separation and thus whether such a separation may help is an open problem. Moreover, several of the introduced notions of bisimulation require to directly compare quantum states. Hence, not analysing the state of the quantum register in testing is a challenge in its own (see *Stateless formulation*). Also a symbolic formulation of bisimulation such as in [19] does not completely overcome this problem at least not for extensional (black-box) testing. An approach similar to [33] would still require to run several tests on a concrete running system.

Compositionality and Pre-congruence. Obtaining congruences, i.e., conformance relations that are preserved under various composition operators, is very difficult in the quantum setting. The main problem is entanglement as pointed out e.g. in [32, 20]. Entanglement relates the states of qubits such that measuring one qubit may change the state of another qubit without any explicit communication. With that a context can exploit information about a system and break the compositionality of parallel composition: two processes that were testing equivalent may cease to be equivalent in a parallel context if one of them has an entangled qubit with the context. A concrete example with this property is used in [32] to explain why their notion of bisimulation is not preserved by parallel composition. Another problem is caused by the combination of classical and quantum information (see e.g. [52]). Restriction operator tends to pose further technical challenges for compositionality as observed in [19].

Non-Determinism. The combination of non-deterministic and probabilistic transitions was already identified as problematic for testing in classical systems. Since most of the approaches described in Section 3.2 combine both features, this problem reoccurs also in the quantum based setting. Also [52] point out that removing some features including probabilities simplifies the task of finding a bisimulation that is a congruence. However, the solutions found for this problem in the classical setting seem to work also for quantum based systems. We observe that e.g.

the bisimulations in [23, 21], each of them a congruence, combine probabilities and non-determinism.

More problematic are the observations made in [11, 12] on non-determinism in observers. Non-determinism may allow an observer to distinguish processes by states that should not be distinguishable. Therefore their restrict the amount of non-determinism in observers. This problem has to be taken into account than building a testing theory for quantum based systems.

Partial specifications. It is impossible to come up with a full specification of a complex system; one powerful abstraction method is to declare some steps as unobservable and define the testing theory to be oblivious ("jump over") such steps [28]. Another way is to separate different concerns and make different specifications; then the testing theory would allow for only comparing those behaviours that are specified for each partial model separately [9, 49, 50]. Since there are currently not theories for quantum testing that allow for partial specification, we at least expect the same challenges as for the classical cases. Whether on top of that the quantum based setting allows for additional meaningful ways to split specifications remains open.

5 Quantum Testing Pre-Orders: Future Roadmap

Despite the wealth of results available, there remains a significant amount of work to come up with a satisfactory notion of testing for quantum processes. Firstly, defining the set of quantum tests and quantum processes (as system under test), for which quantum bisimulation can be tested provides a much needed insight on the observability of quantum bisimulation. For larger subsets of quantum processes, defining a weaker intensional notion of testing that can be extensionally tested is the next step. Using the wealth of available results we need to prove results on logical characterisation as well as pre-order and pre-congruence properties for the developed notions. Finally, coming up with (efficient) test-case generation techniques based on the established extensional definition and applying the theory to substantial case studies will bring the theory to the practice of testing quantum systems.

6 Conclusions

In this paper, we considered the available results that can lead to a formal theory of testing for quantum processes. To this end, we reviewed the line of work that was commence by the seminal work of De Nicola and Hennessy [38] in establishing a formal framework for testing communicating systems. We particularly considered the extensions of this line of work that addressed probabilistic processes, due to their similarity to quantum processes. We also set the desirable requirements for a suitable notion of testing and the significant challenges before meeting these requirements. We studied the available literature on behavioural equivalences for quantum processes, which can further inform the design of the

testing theory. Finally, we sketched a roadmap towards a formal foundation for testing quantum processes.

Acknowledgments. Mohammad Mousavi has been partially supported by the UKRI Trustworthy Autonomous Systems Node in Verifiability, Grant Award Reference EP/V026801/2, the EPSRC project on Verified Simulation for Large Quantum Sys- tems (VSL-Q), grant reference EP/Y005244/1 and the EPSRC project on Robust and Reliable Quantum Computing (RoaRQ), Investigation 009, grant reference EP/W032635/1. Also King's Quantum grants provided by King's College London are gratefully acknowledged.

We thank the reviewers for their constructive feedback and help.

References

1. Abramsky, S.: Observation equivalence as a testing equivalence. Theoretical Computer Science **53**(2-3), 225–241 (1987)
2. Basten, T.: Branching bisimilarity is an equivalence indeed! Information Processing Letters **58**(3), 141–147 (1996). https://doi.org/https://doi.org/10.1016/0020-0190(96)00034-8, https://www.sciencedirect.com/science/article/pii/0020019096000348
3. Bennett, C.H., Brassard, G.: -. In: IEEE International Conference on Computers, Systems and Signal Processing. pp. 175–179 (1984)
4. Bernardo, M., De Nicola, R., Loreti, M.: Revisiting trace and testing equivalences for nondeterministic and probabilistic processes. In: International Conference on Foundations of Software Science and Computational Structures. pp. 195–209. Springer (2012). https://doi.org/10.1007/978-3-642-2
5. Bernardo, M., De Nicola, R., Loreti, M.: Revisiting trace and testing equivalences for nondeterministic and probabilistic processes. Logical Methods in Computer Science **10** (2014). https://doi.org/10.2168/LMCS-10(1:16)2014
6. Blunt, N.S., Camps, J., Crawford, O., Izsák, R., Leontica, S., Mirani, A., Moylett, A.E., Scivier, S.A., Sünderhauf, C., Schopf, P., Taylor, J.M., Holzmann, N.: Perspective on the current state-of-the-art of quantum computing for drug discovery applications. Journal of Chemical Theory and Computation **18**(12), 7001–7023 (12 2022). https://doi.org/10.1021/acs.jctc.2c00574, https://doi.org/10.1021/acs.jctc.2c00574
7. Bohlken, W., van der Bijl, M., Oprescu, A.: Model-based fuzzing using symbolic transition systems. In: Constantinou, E. (ed.) Proceedings of the 13th Seminar Series on Advanced Techniques & Tools for Software Evolution, Amsterdam, The Netherlands, July 1-2, 2020 (due to COVID-19: virtual event). CEUR Workshop Proceedings, vol. 2754. CEUR-WS.org (2020), https://ceur-ws.org/Vol-2754/paper1.pdf
8. van Breugel, F., Shalit, S., Worrell, J.: Testing labelled markov processes. In: Widmayer, P., Ruiz, F.T., Bueno, R.M., Hennessy, M., Eidenbenz, S.J., Conejo, R. (eds.) Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2380, pp. 537–548. Springer (2002). https://doi.org/10.1007/3-540-45465-9_46
9. Brinksma, E.: On the existence of canonical testers. Tech. rep., University of Twente, Enschede (1987)

10. Brookes, S.D., Hoare, C.A.R., Roscoe, A.W.: A theory of communicating sequential processes. J. ACM **31**(3), 560–599 (1984). https://doi.org/10.1145/828.833
11. Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G.: Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers. Proc. ACM Program. Lang. **8**(POPL), 1269–1297 (2024). https://doi.org/10.1145/3632885
12. Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G.: Testing quantum processes. In: 12th International Symposium on Leveraging Applications of Formal Methods, Track on Rigorous Engineering of Collective Adaptive Systems (REO-CAS) (2024)
13. Darondeau, P.: An enlarged definition and complete axiomatization of observational congruence of finite processes. In: Dezani-Ciancaglini, M., Montanari, U. (eds.) International Symposium on Programming, 5th Colloquium, Torino, Italy, April 6-8, 1982, Proceedings. Lecture Notes in Computer Science, vol. 137, pp. 47–62. Springer (1982). https://doi.org/10.1007/3-540-11494-7_5
14. Davidson, T.A.: Formal Verification Techniques using Quantum Process Calculus. Ph.D. thesis, University of Warwick (2012)
15. Deng, Y.: Bisimulations for probabilistic and quantum processes (invited paper). In: Schewe, S., Zhang, L. (eds.) 29th International Conference on Concurrency Theory, CONCUR 2018. LIPIcs, vol. 118, pp. 2:1–2:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2018). https://doi.org/10.4230/LIPICS.CONCUR.2018.2
16. Deng, Y., Feng, Y.: Open bisimulation for quantum processes. In: IFIP International Conference on Theoretical Computer Science. pp. 119–133. Springer (2012). https://doi.org/10.1007/978-3-642-33475-7_9
17. Deng, Y., van Glabbeek, R., Hennessy, M., Morgan, C.: Testing finitary probabilistic processes (extended abstract). In: Mario Bravetti and Gianluigi Zavattaro (ed.) Proceedings of the 20th International Conference on Concurrency Theory (CONCUR). pp. 274–288. Springer, Bologna, Italy (Aug 2009)
18. van Dommelen, X.M., van der Bijl, M., Pimentel, A.D.: Model-based testing of internet of things protocols. In: Groote, J.F., Huisman, M. (eds.) Formal Methods for Industrial Critical Systems - 27th International Conference, FMICS 2022, Warsaw, Poland, September 14-15, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13487, pp. 172–189. Springer (2022). https://doi.org/10.1007/978-3-031-15008-1_12
19. Feng, Y., Deng, Y., Ying, M.: Symbolic Bisimulation for Quantum Processes. ACM Transactions on Computational Logic (TOCL) **15**(2), 1–32 (2014). https://doi.org/10.1145/2579818
20. Feng, Y., Duan, R., Ji, Z., Ying, M.: Probabilistic bisimulations for quantum processes. Information and Computation **205**(11), 1608–1639 (2007). https://doi.org/10.1016/J.IC.2007.08.001
21. Feng, Y., Duan, R., Ying, M.: Bisimulation for quantum processes. In: Ball, T., Sagiv, M. (eds.) Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2011, Austin, TX, USA, January 26-28, 2011. pp. 523–534. ACM (2011). https://doi.org/10.1145/1926385.1926446
22. Feng, Y., Ying, M.: Toward automatic verification of quantum cryptographic protocols. In: Aceto, L., de Frutos-Escrig, D. (eds.) 26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015. LIPIcs, vol. 42, pp. 441–455. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2015). https://doi.org/10.4230/LIPICS.CONCUR.2015.441
23. Franke-Arnold, S., Gay, S.J., Puthoor, I.V.: Verification of Linear Optical Quantum Computing using Quantum Process Calculus. In: Borgström, J.,

Crafa, S. (eds.) Proceedings Combined 21st International Workshop on Expressiveness in Concurrency, EXPRESS 2014, and 11th Workshop on Structural Operational Semantics, SOS 2014. EPTCS, vol. 160, pp. 111–129 (2014). https://doi.org/10.4204/EPTCS.160.10
24. Gaudel, M.C.: Testing can be formal, too. In: Mosses, P.D., Nielsen, M., Schwartzbach, M.I. (eds.) TAPSOFT '95: Theory and Practice of Software Development. pp. 82–96. Springer Berlin Heidelberg, Berlin, Heidelberg (1995)
25. Gay, S.J.: Quantum programming languages: survey and bibliography. Mathematical Structures in Computer Science **16**(4), 581–600 (2006)
26. Gay, S.J., Nagarajan, R.: Communicating quantum processes. In: Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming languages. pp. 145–157 (2005). https://doi.org/10.1145/1040305.1040318
27. Gisin, N., Thew, R.: Quantum communication. Nature Photonics **1**(3), 165–171 (2007). https://doi.org/10.1038/nphoton.2007.22, https://doi.org/10.1038/nphoton.2007.22
28. van Glabbeek, R.J.: The linear time - branching time spectrum II. In: Best, E. (ed.) CONCUR '93, 4th International Conference on Concurrency Theory, Hildesheim, Germany, August 23-26, 1993, Proceedings. Lecture Notes in Computer Science, vol. 715, pp. 66–81. Springer (1993). https://doi.org/10.1007/3-540-57208-2_6, https://doi.org/10.1007/3-540-57208-2_6
29. Hennessy, M., Ingólfsdóttir, A.: A Theory of Communicating Processes with Value Passing. Information and Computation **107**(2), 202–236 (1993). https://doi.org/10.1006/inco.1993.1067
30. Huang, H.Y., Kueng, R., Preskill, J.: Predicting many properties of a quantum system from very few measurements. Nature Physics **16**(10), 1050–1057 (Jun 2020). https://doi.org/10.1038/s41567-020-0932-7, http://dx.doi.org/10.1038/s41567-020-0932-7
31. Jorrand, P., Lalire, M.: Toward a quantum process algebra. In: Proceedings of the 1st Conference on Computing Frontiers. pp. 111–119 (2004). https://doi.org/10.1145/977091.977108
32. Lalire, M.: Relations among quantum processes: Bisimilarity and congruence. Mathematical Structures in Computer Science **16**(3), 407–428 (2006). https://doi.org/10.1017/S096012950600524X
33. Larsen, K.G., Skou, A.: Bisimulation through probabilistic testing. Information and Computation **94**, 1–28 (1991)
34. Milner, R., Parrow, J., Walker, D.: A Calculus of Mobile Processes, Part I and II. Information and Computation **100**(1), 1–77 (1992). https://doi.org/10.1016/0890-5401(92)90008-4, 10.1016/0890-5401(92)90009-5
35. Murillo, J.M., Garcia-Alonso, J., Moguel, E., Barzen, J., Leymann, F., Ali, S., Yue, T., Arcaini, P., Castillo, R.P., de Guzmán, I.G.R., Piattini, M., Ruiz-Cortés, A., Brogi, A., Zhao, J., Miranskyy, A., Wimmer, M.: Challenges of quantum software engineering for the next decade: The road ahead (2024), https://arxiv.org/abs/2404.06825
36. Myers, G., Sandler, C., Badgett, T.: The Art of Software Testing. John Wiley & Sons (2011)
37. Nicola, R.D.: Extensional equivalences for transition systems. Acta Informatica **24**(2), 211–237 (1987). https://doi.org/10.1007/BF00264365
38. Nicola, R.D., Hennessy, M.: Testing equivalences for processes. Theor. Comput. Sci. **34**, 83–133 (1984). https://doi.org/10.1016/0304-3975(84)90113-0, https://doi.org/10.1016/0304-3975(84)90113-0

39. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press (2010)
40. Olsen, P., Foederer, J., Tretmans, J.: Model-based testing of industrial transformational systems. In: Wolff, B., Zaïdi, F. (eds.) Testing Software and Systems - 23rd IFIP WG 6.1 International Conference, ICTSS 2011, Paris, France, November 7-10, 2011. Proceedings. Lecture Notes in Computer Science, vol. 7019, pp. 131–145. Springer (2011). https://doi.org/10.1007/978-3-642-24580-0_10, https://doi.org/10.1007/978-3-642-24580-0_10
41. Phillips, I.: Refusal testing. Theor. Comput. Sci. **50**, 241–284 (1987). https://doi.org/10.1016/0304-3975(87)90117-4, https://doi.org/10.1016/0304-3975(87)90117-4
42. Pirandola, S.: Architectures for QKD networks. In: Figer, D.F. (ed.) Photonics for Quantum 2022. vol. 12243, p. 1224309. International Society for Optics and Photonics, SPIE (2022). https://doi.org/10.1117/12.2635711, https://doi.org/10.1117/12.2635711
43. Schmaltz, J., Tretmans, J.: On conformance testing for timed systems. In: Cassez, F., Jard, C. (eds.) Formal Modeling and Analysis of Timed Systems, 6th International Conference, FORMATS 2008, Saint Malo, France, September 15-17, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5215, pp. 250–264. Springer (2008). https://doi.org/10.1007/978-3-540-85778-5_18
44. Selinger, P.: A brief survey of quantum programming languages. In: International Symposium on Functional and Logic Programming. pp. 1–6. Springer (2004)
45. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. pp. 124–134 (1994). https://doi.org/10.1109/2Fsfcs.1994.365700
46. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999). https://doi.org/10.1137/2FS0097539795293172
47. Shor, P.W., Preskill, J.: Simple proof of security of the bb84 quantum key distribution protocol. Physical review letters **85**(2), 441 (2000)
48. Tilly, J., Chen, H., Cao, S., Picozzi, D., Setia, K., Li, Y., Grant, E., Wossnig, L., Rungger, I., Booth, G.H., Tennyson, J.: The variational quantum eigensolver: A review of methods and best practices. Physics Reports **986**, 1–128 (2022). https://doi.org/https://doi.org/10.1016/j.physrep.2022.08.003, https://www.sciencedirect.com/science/article/pii/S0370157322003118, the Variational Quantum Eigensolver: a review of methods and best practices
49. Tretmans, J.: Conformance testing with labelled transition systems: Implementation relations and test generation. Comput. Networks ISDN Syst. **29**(1), 49–79 (1996). https://doi.org/10.1016/S0169-7552(96)00017-7
50. Tretmans, J., Janssen, R.: Goodbye ioco. In: Jansen, N., Stoelinga, M., van den Bos, P. (eds.) A Journey from Process Algebra via Timed Automata to Model Learning - Essays Dedicated to Frits Vaandrager on the Occasion of His 60th Birthday. Lecture Notes in Computer Science, vol. 13560, pp. 491–511. Springer (2022). https://doi.org/10.1007/978-3-031-15629-8_26
51. Van Breugel, F., Mislove, M., Ouaknine, J., Worrell, J.: Domain theory, testing and simulation for labelled Markov processes. Theoretical Computer Science **333**(1-2), 171–197 (2005). https://doi.org/10.1016/j.tcs.2004.10.021
52. Ying, M., Feng, Y., Duan, R., Ji, Z.: An algebra of quantum processes. ACM Transactions on Computational Logic **10**(3), 19:1–19:36 (2009). https://doi.org/10.1145/1507244.1507249