Contextual advantage for state-dependent cloning

Matteo Lostaglio[1] and Gabriel Senno[1]

[1] *ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels (Barcelona), 08860, Spain*

Choosing noncontextuality as one's notion of classicality, then it is known that no-cloning cannot be regarded as a non-classical phenomenon. There are, in fact, noncontextual ontological models which reproduce large subsets of quantum theory and contain a no-cloning theorem. In this work, however, we show that the phenomenology of cloning is indeed nonclassical, but not for the reasons usually adduced. Specifically, we focus on the task of state-dependent cloning and prove that the optimal cloning fidelity predicted by quantum theory cannot be explained by any noncontextual model. We derive a noise-robust noncontextuality inequality whose violation by quantum theory not only implies a quantum advantage for the task of state-dependent cloning, but also provides an experimental witness of noncontextuality.

The no-cloning theorem [1] is widely regarded as a central result in quantum theory. Informally, the theorem states the impossibility of copying quantum information, and is contrasted with the fact that classical information, on the other hand, can be perfectly copied. More precisely, there is no machine $\mathcal{M}$ (formally, a quantum channel) that can take two distinct and non-orthogonal states $\{|\psi_i\rangle\}_{i=1}^2$ as inputs and output the corresponding copies $\{|\psi_i\rangle \otimes |\psi_i\rangle\}_{i=1}^2$ [1].

While no-cloning is often regarded as an intrinsically quantum feature, one would like to back that claim by a precise theorem stating what operational features cannot be explained within classical models. The theorem should hence define a precise notion of 'classicality' and show that such notion leads to operational predictions incompatible with the relevant quantum statistics [2].

Since we are not dealing with experiments featuring space-like separated measurements, we need a different notion of classicality from Bell's notion of locality. Hence, in this paper we take classicality to be *non-contextuality*, in the generalized sense introduced in Ref. [3]. Contextuality is related to a whole range of other notions of non-classicality (negativity of quasi-probability representations [4], anomalous weak values [5], nonlocality [3]), and has been recently identified as a resource for universal quantum computation [6, 7] and optimal state discrimination [2].

One should note that, from the point of view of contextuality, no-cloning by itself should not be regarded as a non-classical phenomenon. There are, in fact, several examples of non-contextual models with a no-cloning theorem. For example, Ref. [8] introduced a model based on classical Hamiltonian dynamics with a 'resolution restriction' on phase space. Quantum states here correspond to probability distributions over phase space and the restriction forbids the preparation of distributions that are arbitrarily sharp in both position and momentum. This non-contextual model is operationally equivalent to the Gaussian subset of quantum theory and, as such, admits a no-cloning theorem [8]. The same can be said for other non-contextual models, such as Spekken's toy theory [9], which is equivalent to stabilizer quantum mechanics in all odd dimensions [10]. The reason why a no-cloning theorem arises in these theories is that pure, non-orthogonal, quantum states $|\psi_1\rangle$, $|\psi_2\rangle$ correspond to distinct, overlapping, probability distributions $p_1(\lambda)$, $p_2(\lambda)$ over the posited set of ontological states λ. Since p_i cannot be cloned, i.e. there exists no stochastic process mapping $\{p_i\}_{i=1}^2$ to $\{p_i \otimes p_i\}_{i=1}^2$, these models provide a simple, classical explanation of the no-cloning theorem.

Since the no-cloning theorem admits non-contextual explanations, here we focus on the ultimate limits of imperfect cloning. The question of what is the best fidelity with which a given set of quantum states can be cloned has been widely studied since the pivotal work of Bužek and Hillary in 1996 [11], see, *e.g.*, [12]. We find that the optimal fidelity predicted by quantum theory cannot be reproduced by any non-contextual model. Specifically, contextuality provides an advantage to the maximum copying fidelity. This shows that quantum cloning is indeed non-classical, but not for the reasons usually adduced. Our result shows that a strong notion of non-classicality sits at the core of an important quantum information primitive and directly links contextuality to a quantum advantage.

Optimal state-dependent quantum cloning. Before we discuss our no-go theorem for the maximum copying fidelity achievable in non-contextual models, let us recall the correspondent quantum setting. One of two pure states, $|a\rangle$ and $|b\rangle$, is sent with equal probability into a cloning machine $\mathcal{M}$. Consider a cloning machine whose outputs maximise the global average fidelity

$$F_g^Q := \frac{1}{2}F(\mathcal{M}(|a\rangle\langle a|), |aa\rangle\langle aa|) + \frac{1}{2}F(\mathcal{M}(|b\rangle\langle b|), |bb\rangle\langle bb|).$$

It has been shown [13] that the optimal machine $\mathcal{M}$ is a unitary U on the input and a register. Define $|\alpha\rangle := U|a\,0\rangle$, $|\beta\rangle := U|b\,0\rangle$, where $|0\rangle$ is the initial state of the register. Optimising over the choice of U, the optimal global average fidelity reads [14]

$$F_g^{Q,\text{opt}} := \frac{1}{4}\left[\sqrt{(1+c_{ab})(1+\sqrt{c_{ab}})} + \sqrt{(1-c_{ab})(1-\sqrt{c_{ab}})}\right]^2, \tag{1}$$

where $c_{ab} = |\langle a|b\rangle|^2$.

Operational features. We now describe operationally the features of the quantum experiment above which, ultimately, will be impossible to explain within a non-contextual model (see also Fig. 1).

Let P_a, P_b denote the experimental procedures followed to prepare $|a\rangle$ and $|b\rangle$. These states go through a cloning machine, which gives new preparations P_α, P_β respectively. These finally undergo a 'test' measurement, M_{aa} or M_{bb} respectively, with outcomes in $\{0,1\}$. These are defined such that the probabilities $p(M_{aa}|P_{aa})$ of getting outcome 1 in a M_{aa} measurement (i.e., 'passing the test M_{aa}'), given the preparation P_{aa} as input, satisfies $p(M_{aa}|P_{aa}) = 1$, and the same for M_{bb}.

Operationally, denoting by $c_{ss'} = P(M_s|P_{s'})$ (called 'confusability' in Ref. [2]), the cloning fidelity is defined to be

$$F_g := \frac{1}{2}c_{\alpha aa} + \frac{1}{2}c_{\beta bb},$$

i.e. the average probability that the imperfect clones P_α, P_β, pass the corresponding test measurements for the ideal clones P_{aa}, P_{bb}. In particular, we are interested in finding bounds for the above quantity as a function of c_{ab}, which in a quantum experiment reads $c_{ab} = |\langle a|b\rangle|^2$. Quantum mechanics predicts that, in the optimal scenario, F_g is related to c_{ab} by Eq. (1).

There are some final operational constraints that exclude some trivial strategies (such as replying always 'pass' in the test measurement). In particular, there exist preparations procedures $P_{a^\perp}$, $P_{b^\perp}$ such that the $p(M_a|P_{a^\perp}) = p(M_b|P_{b^\perp}) = 0$. Furthermore, the preparation procedures $P_{a^\perp}$, $P_{b^\perp}$ can be chosen such that the mixture $P_a/2 + P_{a^\perp}/2$ (tossing a fair coin and following either P_a or $P_{a^\perp}$) cannot be distinguished from the mixture $P_b/2 + P_{b^\perp}/2$ by any measurement apparatus. We denote this *operational equivalence* as

$$P_a/2 + P_{a^\perp}/2 \simeq P_b/2 + P_{b^\perp}/2. \qquad (2)$$

In the quantum experiment, the above operational features can be seen to hold by identifying: P_a and P_b with the preparation of the pure states $|a\rangle$ and $|b\rangle$ respectively; $P_{a^\perp}$ and $P_{b^\perp}$ with the preparation of pure states $|a^\perp\rangle$ and $|b^\perp\rangle$ satisfying $\langle b|b^\perp\rangle = 0$, $|a\rangle = c_1\,|b\rangle + c_2\,|b^\perp\rangle$ and $|a^\perp\rangle = c_2^*\,|b\rangle - c_1^*\,|b^\perp\rangle$ (whose existence follows from elementary linear algebra arguments); and, finally, M_a, M_b with the POVMs $\{|a\rangle\langle a|\,, \mathbb{1} - |a\rangle\langle a|\}$ and $\{|b\rangle\langle b|\,, \mathbb{1} - |b\rangle\langle b|\}$. The same reasoning straightforwardly applies to the remaining pairs of preparations: (P_{aa}, P_{bb}), (P_{aa}, P_α) and (P_{bb}, P_β).

Non-contextuality. Non-contextuality is a restriction on the ontological models that try to explain a given statistics. In an ontological model every preparation P_s corresponds to sampling from a probability distribution $\mu_s(\lambda)$ over some set of hidden variables λ. Any quantum operation on a quantum state is represented in the ontological model by a matrix $T(\lambda'|\lambda)$ of transition probabilities ($T(\lambda'|\lambda) \geq 0$, $\sum_{\lambda'} T(\lambda'|\lambda) = 1$) acting on the corresponding probability density.

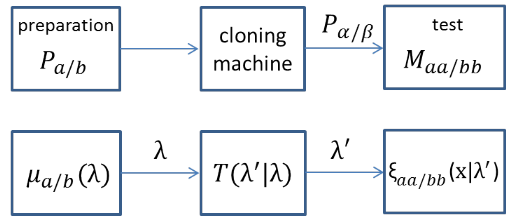

FIG. 1. *Cloning experiment.* Top: black-box of the cloning protocol; one of two preparation procedures P_x, $x = a, b$ is performed with equal probability, the resultant state is sent through a cloning machine (independent of x), which respectively prepares P_γ, $\gamma = \alpha, \beta$; a test measurement M_{xx} for the target preparation P_{xx} is performed and passed with probability $P(M_{aa}|P_\alpha)$ (or $P(M_{bb}|P_\beta)$). Bottom: ontological description of the same experiment, where preparing P_x corresponds to sampling λ with probability $\mu_x(\lambda)$, the cloning machine maps $\lambda \mapsto \lambda'$ with probability $T(\lambda'|\lambda)$ and M_{xx} gives a 'pass' outcome with probability $\xi_{xx}(1|\lambda')$.

Finally, an ontological model's predictions can be written as

$$p(x|P_s, M_{s'}) = \int d\lambda \mu_s(\lambda)\xi_{s'}(x|\lambda), \qquad (3)$$

where $\xi_{s'}(x|\lambda)$ is the response function of the measurement $M_{s'}$, giving the probability of outcome x given that the hidden variable takes the value λ.

Non-contextuality, in the generalized form introduced in [3], is the requirement that *if two procedures are operationally equivalent, they must be represented in the same way within the ontological model.* This notion can be seen as an extension of the traditional notion of Kochen-Speckers [15].

In our case the only operational equivalences are Eq. (2) and the corresponding ones for the pairs (P_{aa}, P_{bb}), (P_{aa}, P_α), (P_{bb}, P_β). Non-contextuality then requires the ontological model to satisfy the constraint

$$\frac{1}{2}\mu_a(\lambda) + \frac{1}{2}\mu_{a^\perp}(\lambda) = \frac{1}{2}\mu_b(\lambda) + \frac{1}{2}\mu_{b^\perp}(\lambda), \qquad (4)$$

and likewise for the other pairs.

Optimal cloning is contextual. We are now ready to state our main result:

Theorem 1 (Cloning is contextual – ideal scenario)**.** *Let P_α and P_β be the outcomes of a cloning process when the inputs are, respectively, P_a and P_b, and let P_{aa} (resp. P_{bb}) be the preparation of two copies of P_a (resp. P_b). Moreover, for all s in $\{a, b, aa, bb, \alpha, \beta\}$, let $P_{s^\perp}$ and M_s be preparations and test measurements satisfying*

$$p(M_s|P_s) = 1, \quad p(M_s|P_{s^\perp}) = 0. \qquad (5)$$

Then, for any non-contextual model satisfying the operational equivalences

$$\frac{1}{2}P_s + \frac{1}{2}P_{s^\perp} \simeq \frac{1}{2}P_{s'} + \frac{1}{2}P_{s'^\perp}$$

for all (s,s') *in* $\{(a,b),(aa,bb),(\alpha,aa),(\beta,bb)\}$*, we have that*

$$F_g^{\rm NC} \le 1 - \frac{c_{ab}}{2} + \frac{c_{aa,bb}}{2}. \quad (6)$$

Proof. The first part of the proof essentially follows the argument given in Ref. [3] Sec. VIIIA and reproduced in Ref. [2] Sec. IIIA, but it is slightly adapted to use the fewer assumptions of the statement. We have that, for all (k,k') in $\{(a,b),(aa,bb),(\alpha,aa),(\beta,bb)\}$,

$$1 = p(x=1|P_k,M_k) = \int_{s_k} d\lambda \mu_k(\lambda)\xi_k(\lambda), \quad (7)$$

where s_k denotes the support of μ_k. From this equation it follows that $\xi_k(\lambda)=1$ almost everywhere on s_k. Furthermore,

$$0 = p(x=1|P_{k^\perp},M_k) = \int_{s_{k^\perp}} \mu_{k^\perp}(\lambda)\xi_k(\lambda), \quad (8)$$

and, since $\xi_k(\lambda)=1$ almost everywhere on s_k, it follows that $\xi_k(\lambda)=0$ on $s_{k^\perp}$ and $s_k \cap s_{k^\perp} = \emptyset$ (modulo a measure zero set).

We are now ready to derive the relation between confusability and ℓ_1 norm in noncontextual models satisfying the above constraints. The operational equivalences imply that in a non contextual model

$$\mu_k(\lambda) + \mu_{k^\perp}(\lambda) = \mu_{k'}(\lambda) + \mu_{k'^\perp}(\lambda), \quad \forall \lambda \in \Lambda. \quad (9)$$

Since $s_k \cap s_{k^\perp} = s_{k'} \cap s_{k'^\perp} = \emptyset$, this implies $\mu_k(\lambda) = \mu_{k'}(\lambda)$ for almost all $\lambda \in s_k \cap s_{k'}$. Hence, using the facts above,

$$\|\mu_k - \mu_{k'}\| = \int_{\Lambda\setminus s_k} d\lambda \mu_k(\lambda) + \int_{\Lambda\setminus s_{k'}} d\lambda \mu_{k'}(\lambda)$$
$$= 2 - 2\int_{s_k \cap s_{k'}} d\lambda \mu_k(\lambda) = 2 - 2\int_{s_k\cap s_{k'}} d\lambda \mu_k(\lambda)\xi_{k'}(\lambda).$$

Now, note that the last integral can be extended to Λ. In fact, by contradiction suppose that $\xi_{k'}(\lambda) \neq 0$ for some nonzero measure set $s \subseteq s_k \setminus s_{k'}$. Then, from Eq. (9), it follows that $\forall\ \lambda \in s\ : 0 < \mu_k(\lambda) = \mu_{k'^\perp}(\lambda)$. However, as we discussed $\xi_{k'}(\lambda) = 0$ almost everywhere on $s_{k'^\perp}$, which gives the desired contradiction. Hence the integral can be extended to s_k and, trivially, to all Λ. In conclusion,

$$\|\mu_k - \mu_{k'}\| = 2 - 2\int_\Lambda d\lambda \mu_k(\lambda)\xi_{k'}(\lambda) = 2(1-c_{kk'}). \quad (10)$$

To complete the proof we can now use the triangular inequality,

$$\|\mu_{aa}-\mu_{bb}\| \le \|\mu_{aa}-\mu_\alpha\| + \|\mu_\alpha - \mu_\beta\| + \|\mu_\beta - \mu_{bb}\|. \quad (11)$$

By definition, $\mu_\alpha(\lambda) = \int_\Lambda T(\lambda|\lambda')\mu_a(\lambda')$, for a stochastic matrix $T(\lambda|\lambda')$. Similarly, $\mu_\beta(\lambda) = \int_\Lambda T(\lambda|\lambda')\mu_b(\lambda')$, with the same stochastic matrix. Since $\int d\lambda T(\lambda|\lambda') = 1$ and $T(\lambda|\lambda') \ge 0$, one can readily verify from the convexity of the absolute value that $\|\mu_\alpha - \mu_\beta\| \le \|\mu_a - \mu_b\|$, which implies

$$\|\mu_{aa}-\mu_{bb}\| \le \|\mu_\alpha - \mu_{aa}\| + \|\mu_a - \mu_b\| + \|\mu_\beta - \mu_{bb}\|. \quad (12)$$

Using the relation to the ℓ_1 norm derived above, the previous inequality gives

$$2(1-c_{aa,bb}) \le 2(1-c_{\alpha aa}) + 2(1-c_{ab}) + 2(1-c_{\beta bb}), \quad (13)$$

which, once rearranged, provides the final result. □

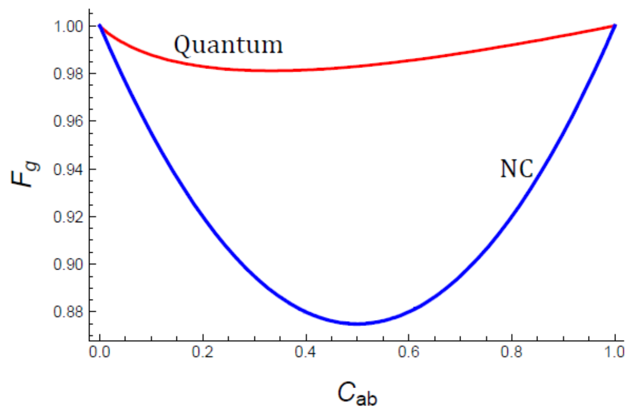

FIG. 2. Maximum tradeoff between cloning fidelity F_g and confusability c_{ab} allowed for noncontextual models (blue line, Eq. 6) versus optimal tradeoff achievable in quantum theory (red line, Eq. 1).

In Fig. 2 we compare the optimal quantum cloning (global) fidelity with the maximum non-contextual cloning fidelity, taking into account that operationally one has $c_{aa,bb} = c_{ab}^2$. One can see, for any $0 < c_{ab} < 1$, that quantum mechanics achieves higher copying fidelities than what is allowed by the principle of non-contextuality. Hence, despite the fact that no-cloning theorems can be reproduced within classical models, the phenomenology of optimal cloning is indeed strongly non-classical. Contextuality provides an advantage for the maximum copying fidelity.

Interestingly, the above derivation also gives an alternative proof of the main result of Ref. [2], since the maximum probability of distinguishing two preparations P_k and $P_{k'}$ is $1/2 + \|\mu_k - \mu_{k'}\|/4 = 1 - c_{kk'}/2$. This also shows that the non-contextual bound on cloning is not saturated by a measure and prepare strategy. In this strategy, upon successful discrimination one prepares two copies correct state, achieving confusability 1 with the target clone; upon failure, one prepares two copies of the other state, achieving a confusability that equals $c_{aa,bb}$. The resulting average fidelity is then $1 - c_{ab}/2 + c_{ab}c_{aabb}/2$, below the non-contextual bound. This fact suggests that the non-contextual limits on cloning cannot be simply understood from the non-contextual limits on state discrimination. Of course, this may be due to the fact that the bound in Eq. (6) is not tight. But, more likely, this is due to the fact that, just like in the quantum case, there is a gap between optimal cloning and the optimal measure and prepare strategy.

Beyond idealizations. Theorem 1 is a no-go result for noncontextual ontological models aimed at explaining the phenomenology of state-dependent quantum cloning. However, the inequality derived therein, Eq. (6), is not a proper noncontextuality inequality because the operational features considered reference to an idealized experiment. In any real experiment, on the other hand, one would need to confront noise and imperfections. Theorem 2 below extends Theorem 1 beyond the ideal limit, allowing for the observation of non-perfect correlations in Eq. (5).

Theorem 2 (Cloning is contextual – non ideal scenario)**.** *With the notation of Thm. 1, suppose that for all s in $\{a, b, aa, bb, \alpha, \beta\}$,*

$$p(M_s|P_s) = 1 - \epsilon_s, \quad p(M_s|P_{s^\perp}) = \epsilon_s. \tag{14}$$

Then, for any non-contextual model satisfying the operational equivalences

$$\frac{1}{2}P_s + \frac{1}{2}P_{s^\perp} \simeq \frac{1}{2}P_{s'} + \frac{1}{2}P_{s'^\perp}$$

for all (s, s') in $\{(a, b), (aa, bb), (\alpha, aa), (\beta, bb)\}$, we have that

$$F_g^{\text{NC}} \leq 1 - \frac{c_{ab}}{2} + \frac{c_{aa,bb}}{2} + \text{Err} \tag{15}$$

where $\text{Err} = \epsilon_a + \epsilon_b + \epsilon_\alpha + \epsilon_\beta + 2(\epsilon_{aa} + \epsilon_{bb})$.

The proof of Theorem 2 follows the same lines as that of Theorem 1 with the key addition of the following Lemma 3, which extends Eq. (10) to the noisy setting:

Lemma 3. *For $s \in \{a, b\}$, let P_s and $P_{s^\perp}$ be preparations procedures and M_s be measurement procedures satisfying*

$$p(M_s|P_s) = 1 - \epsilon_s, \quad p(M_s|P_{s^\perp}) = \epsilon_s.$$

Then, for any non-contextual model satisfying the operational equivalence

$$\frac{1}{2}P_a + \frac{1}{2}P_{a^\perp} \simeq \frac{1}{2}P_b + \frac{1}{2}P_{b^\perp}$$

we have that,

$$|\|\mu_a - \mu_b\| - 2(1 - c_{ab})| \leq 4(\epsilon_a + \epsilon_b).$$

Being a general result relating the ℓ_1 distance between two epistemic states and their confusability in noncontextual models satisfying Eq. (2) beyond the ideal scenario, we anticipate that Lemma 3 will be of broader use to identify quantum advantage beyond state-dependent cloning.

An explicit noise model. Having derived a noise-robust version of our noncontextual bound, the next step is to investigate whether quantum mechanics violates it. We consider a noise model in which the ideal quantum preparations and measurements are thwarted by a depolarizing channel with noise parameter v:

$$\mathcal{D}(\rho) = (1 - v)\rho + v\frac{\mathbb{I}}{d}, \qquad \mathcal{D}(E_s) = (1 - v)E_s + v\frac{\mathbb{I}}{d}.$$

It is not hard to see that, if one uses the unitary transformation which is optimal for the ideal setting, one gets a quantum strategy whose global average fidelity reads

$$F_g = F_g^{Q,\text{opt}}(1 - v)^2 + v(1/2 - v/4),$$

which coincides with the optimal for $v = 0$. For every $v > 0$, however, and unlike in the ideal case, the tradeoff between c_{ab} and F_g is not always above the noncontextual bound. For example, for $v = 0.005$, this particular quantum strategy violates Eq. (15) only for $0.18 \lesssim c_{ab} \lesssim 0.85$ and already for $v = 0.01$ the quantum value is always below. Nevertheless, a preliminary comparison with the experimental results of [16] suggests that the required low level of noise is not beyond current experiments. In fact, in terms of the parameter $C_s = 1/2\, p(M_s|P_s) + 1/2\, p(M_{s^\perp}|P_{s^\perp})$ defined in Ref. [16], $v = 0.005$ corresponds to $C_s \approx 0.9950$ for $s = a, b$ and $C_s \approx 0.9925$ for $s = aa, bb$, and Ref. [16] experimentally realized $C_s = 0.9969$.

We conjecture that using the unitary transformation coming from the optimal strategy in the ideal setting is not optimal for this noise model (while it might be realistic if one cannot fine tune the strategy to the noise). Moreover, we believe that there is still room for improvement in the error term in Eq. (15). Thus, we expect that better noise-resistant contextual violations can be extracted from our results.

Conclusions and open questions. We have shown that the optimal fidelity of a state-dependent cloner predicted by quantum theory fails to admit a noncontextual explanation. Furthermore, we have derived a noise-resistant noncontextuality inequality whose experimental violation is a witness of contextuality.

From a foundational point of view, it would be quite interesting to study whether the necessity of contextuality that we have proven for optimal state-dependent cloning extends to the other types of imperfect cloning studied in the literature, chiefly phase-covariant and/or universal cloning, as well as probabilistic cloning [12].

Finally, from an applications' point of view, one important open question is how to use our noncontextual bound to prove a contextual advantage for quantum information processing tasks which rely on optimal quantum state-dependent cloning (e.g. [17, 18]).

[1] W. K. Woottersand W. H. Zurek, Nature **299**, 802 (1982).
[2] D. Schmidand R. W. Spekkens, Physical Review X **8**, 011015 (2018).
[3] R. W. Spekkens, Physical Review A **71**, 052108 (2005).
[4] R. W. Spekkens, Physical review letters **101**, 020401 (2008).
[5] M. F. Pusey, Physical review letters **113**, 200401 (2014).
[6] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature **510**, 351 (2014).
[7] J. Bermejo-Vega, N. Delfosse, D. E. Browne, C. Okay, and R. Raussendorf, Physical review letters **119**, 120505 (2017).
[8] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Physical Review A **86**, 012103 (2012).
[9] R. W. Spekkens, Physical Review A **75**, 032110 (2007).
[10] L. Cataniand D. E. Browne, New Journal of Physics **19**, 073035 (2017).
[11] V. Bužekand M. Hillery, Physical Review A **54**, 1844 (1996).
[12] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005).
[13] A. E. Rastegin, Physical Review A **68**, 032303 (2003).
[14] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Physical Review A **57**, 2368 (1998).
[15] S. Kochenand E. P. Specker, in *The logico-algebraic approach to quantum mechanics* (Springer, 1975) pp. 293–328.
[16] M. D. Mazurek, M. F. Pusey, R. Kunjwal, K. J. Resch, and R. W. Spekkens, Nat. Commun. **7**, 11780 (2016), arXiv:1505.06244.
[17] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of modern physics **81**, 1301 (2009).
[18] P. Deuarand W. Munro, Physical Review A **62**, 042304 (2000).