Does Ignorance of the Whole Imply Ignorance of the Parts?
Large Violations of Noncontextuality in Quantum Theory

Thomas Vidick and Stephanie Wehner

I. INTRODUCTION

In this Letter we examine the following seemingly innocuous question: does one’s ignorance about the whole necessarily imply ignorance about at least one of its parts? Given just a moment’s thought, the initial reaction is generally to give a positive answer. Surely, if one cannot know the whole, then one should be able to point to an unknown part. Classically, and more generally for any deterministic noncontextual hidden-variable model, our intuition turns out to be correct: ignorance about the whole does indeed imply the existence of a specific part which is unknown, so that one can point to the source of one’s ignorance. However, we will show that in a quantum world this intuition is flawed.

II. THE PROBLEM

Let us first explain our problem more formally. Consider two dits $y_0$ and $y_1 \in \{0,\ldots,d-1\}$, where the string $y = y_0 y_1$ plays the role of the whole, and $y_0$, $y_1$ are the individual parts. Let $\rho_y$ denote an encoding of the string $y$ into a classical or quantum state. In quantum theory, $\rho_y$ is simply a density operator, and in a NC HV model it is a preparation $\mathcal{P}_y$ described by a probability distribution over hidden variables $\lambda \in \Lambda$. Let $P_y$ be a probability distribution over $\{0,\ldots,d-1\}$, and imagine that with probability $P_y(y)$ we are given the state $\rho_y$. The optimum probability of guessing $y$ given its encoding $\rho_y$, which lies in a register $E$, can be written as

$$P_{\text{guess}}(Y|E) = \max_{\mathcal{M}} \sum_{y \in \{0,\ldots,d-1\}} P_y(y) p(y|\mathcal{M}, \mathcal{P}_y).$$

(1)

where $p(y|\mathcal{M}, \mathcal{P}_y)$ is the probability of obtaining outcome $y$ when measuring the preparation $\mathcal{P}_y$ with $\mathcal{M}$, and the maximization is taken over all $d^2$-outcome measurements allowed in the theory. In the case of quantum theory, for example, the maximization is taken over positive operator-valued measurements $\mathcal{M} = \{M_j\}_j$ and $p(y|\mathcal{M}, \mathcal{P}_y) = \text{tr}(M_j \rho_y)$. The guessing probability is directly related to the conditional min-entropy $H_\infty(Y|E)$ through the equation [1,2]

$$H_\infty(Y|E) := -\log P_{\text{guess}}(Y|E).$$

(2)

This measure plays an important role in quantum cryptography and is the relevant measure of information in the single shot setting corresponding to our everyday experience, as opposed to the asymptotic setting captured by the von Neumann entropy. The main question we are interested in can then be loosely phrased as

How does $H_\infty(Y = Y_0 Y_1|E)$ (ignorance about the whole) relate to $H_\infty(Y_C|EC)$, for $C \in \{0, 1\}$ (ignorance about the parts)?

Here the introduction of the additional random variable $C$ is crucial, and it can be understood as a pointer to the part of $Y$ about which there is large ignorance (given a large ignorance of the whole string $Y$); see Fig. 1 for an illustration of this role. It is important to note that the choice of $C$ should be consistent with the encoding prior to its definition. That is, whereas $C$ may of course depend on $Y_0$, $Y_1$ and the encoding $E$, the reduced state on registers holding $Y_0$, $Y_1$ and $E$ after tracing out $C$ should remain the same. In particular, this condition states that $C$ cannot be the result of a measurement causing disturbance to the encoding register; if we were allowed to destroy information in the encoding we would effectively alter the original situation.
III. RESULTS

A. An inequality valid in any NC HV model

We first show that classically, or more generally in any noncontextual hidden-variable model [3], ignorance about the whole really does imply ignorance about a part. More specifically, we show that for any random variable $Y = Y_0Y_1$ and side information $E$ there exists a random variable $C \in \{0, 1\}$ such that

$$H_\infty(Y_C | EC) \geq \frac{H_\infty(Y_0Y_1 | E)}{2}. \tag{3}$$

This inequality can be understood as an information-theoretic analogue of Bell inequalities to the question of noncontextuality. Classically, this inequality is known as the min-entropy splitting inequality, and plays an important role in the proof of security of some (classical) cryptographic primitives [4,5]. The proof of (3) is a straightforward extension to the case of standard NC HV models [6,7] of a classical technique known as min-entropy splitting first introduced by Wullschleger [4]. (We refer to the Supplemental Material [8] for details of the proof.)

The fact that $C$ is a random variable, rather than being deterministically chosen, is important, and an example will help clarify its role. Consider $Y$ uniformly distributed over $\{0, \ldots, d - 1\}^2$ and $E = Y_0$ with probability $1/2$, and $Y_1$ with probability $1/2$. In this case it is easy to see that both $Y_0$ and $Y_1$ can be guessed from $E$ with average success probability $1/2 + 1/(2d)$, so that $H_\infty(Y_0 | E) = H_\infty(Y_1 | E) = 1$, which is much less than $H_\infty(Y | E) = \log d$. However, define $C$ as $0$ if $E = Y_1$ and $1$ if $E = Y_0$. Then it is clear that $H_\infty(Y_C | EC) = \log d$, as we are always asked to predict the variable about which we have no side information at all. In this case the random variable $C$ “points to the unknown” by being correlated with the side information $E$, but is entirely consistent with our knowledge about the world: by tracing out $C$ we recover the initial joint distribution on $(Y, E)$. This also highlights the important difference between the task we are considering and the well-studied random access codes [9–11], in which the requirement is to be able to predict one of $Y_0$, $Y_1$ (adversarially chosen) from their encoding; for this task it has been demonstrated that there is virtually no asymptotic difference between classical and quantum encodings.

It is interesting to note that (3) still holds if we consider a somewhat “helpful” physical model in which in addition to the encoding one might learn a small number of “leaked” bits of information about $Y$. More specifically, if the NC HV discloses $m$ extra bits of information then it follows from the chain rule for the min-entropy (cf. the Supplemental Material [8]) that

$$H_\infty(Y_C | EC) \geq \frac{H_\infty(Y_0Y_1 | E)}{2} - m. \tag{4}$$

B. Violation in quantum theory

Our main result shows that (3) is violated in the strongest possible sense by quantum theory. More specifically, we provide an explicit construction that demonstrates this violation: Let $Y = Y_0Y_1$ be uniformly distributed over $\{0, \ldots, d - 1\}^2$. Given $y = y_0y_1 \in \{0, \ldots, d - 1\}^2$, define its encoding $\rho_{y_0y_1}^E = |\Psi_y\rangle \langle \Psi_y|$ as

$$|\Psi_y\rangle := X_d^{y_0} Z_d^{y_1} |\Psi\rangle, \tag{5}$$

where $X_d$ and $Z_d$ are the generalized Pauli matrices and

$$|\Psi\rangle := \frac{1}{\sqrt{2(1 + \frac{1}{d})}}(|0\rangle + F|0\rangle), \tag{6}$$

with $F$ being the matrix of the Fourier transform over $\mathbb{Z}_d$. Since we are only interested in showing a quantum violation, we will for simplicity always assume that $d$ is prime. The system $YE$ is then described by the ccq state

$$\rho_{Y_0Y_1E} = \frac{1}{d^2} \sum_{y_0y_1} |y_0\rangle \langle y_0| \otimes |y_1\rangle \langle y_1| \otimes \rho_{y_0y_1}^E. \tag{7}$$

We first prove that $H_\infty(Y | E) = \log d$ for our choice of encoding. We then show the striking fact that, even though the encoding we defined gives very little information about the whole string $Y$, for any adversarially chosen random variable $C$ (possibly correlated with our encoding) one can guess $Y_C$ from its encoding $\rho_C$ with essentially constant probability. More precisely, for any ccq state $\rho_{Y_0Y_1EC}$, with $C \in \{0, 1\}$, that satisfies the consistency relation $tr_C(\rho_{Y_0Y_1EC}) = \rho_{Y_0E}$, we have

$$H_\infty(Y_0 | E) = H_\infty(Y_1 | E) = 1,$
for any sufficiently large $d$. This shows that the inequality (3) can be violated arbitrarily (with $d$), giving a striking example of the malleability of quantum information. What is more, it is not hard to show that this effect still holds even for $H_{\infty}$, for constant error $\epsilon$, and a helpful physical model leaking $m = c \log d$ bits of information with $c < 1/2$. Hence, the violation of the inequality (3) has the appealing feature of being very robust.

C. Implications for cryptography

Our result answers an interesting open question in quantum cryptography [12], namely, whether min-entropy splitting can still be performed when conditioned on quantum instead of classical knowledge. This technique was used to deal with classical side information $E$ in [5,13]. Our example shows that quantum min-entropy splitting is impossible.

IV. PROOF OF THE QUANTUM VIOLATION

We now provide an outline of the proof that the encoding specified in (5) leads to a quantum violation of the splitting inequality (3); for completeness, we provide a more detailed derivation in the Supplemental Material [8]. Our proof proceeds in three steps: first, by computing $H_{\infty}(Y|E)$ we show that the encoding does indeed not reveal much information about the whole. Second, we compute the optimal measurements for extracting $Y_0$ and $Y_1$ on average, and show that these measurements perform equally well for any other prior distribution on $Y$. Finally, we show that even introducing an additional system $C$ does not change one’s ability to extract $Y_C$ from the encoding.

Step 1. Intuitively, ignorance about the whole string follows from Holevo’s theorem and the fact that we are encoding 2 bits into a $d$-dimensional quantum system. To see this more explicitly, recall that $H_{\infty}(Y|E) = \log d$ is equivalent to showing that $P_{\text{guess}}(Y|E) = 1/d$. From (1) we have that this guessing probability is given by the solution to the following semidefinite program:

$$\begin{align*}
\text{maximize} & \quad \frac{1}{d^2} \sum_{y_0,y_1} \text{tr}(M_{y_0y_1}|\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}|) \\
\text{subject to} & \quad M_{y_0y_1} \succeq 0 \quad \text{for all } y_0,y_1, \\
& \quad \sum_{y_0,y_1} M_{y_0y_1} = 1.
\end{align*}$$

The dual semidefinite program is easily found to be

$$\begin{align*}
\text{minimize} & \quad \text{Tr}(Q) \\
\text{subject to} & \quad Q \succeq \frac{1}{d^2}|\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}| \quad \text{for all } y_0,y_1.
\end{align*}$$

Let $\nu_{\text{primal}}$ and $\nu_{\text{dual}}$ be the optimal values of the primal and dual, respectively. By the property of weak duality, $\nu_{\text{dual}} \geq \nu_{\text{primal}}$ always holds. Hence, to prove our result, we only need to find a primal and dual solutions for which $\nu_{\text{primal}} = \nu_{\text{dual}} = 1/d$. It is easy to check that $Q = 1/d$ is a dual solution with value $\nu_{\text{dual}} = \text{tr}(Q) = 1/d$. Similarly, consider the measurement $M_{y_0y_1} = |\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}|/d$. Using Schur’s lemma, one can directly verify that $\sum_{y_0,y_1} M_{y_0y_1} = 1$, giving $\nu_{\text{primal}} = 1/d$.

Step 2. A similar argument, exploiting the symmetries in the encoding, can be used to show that

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2\sqrt{d}}. \quad (9)$$

The measurements that attain these values are given by the eigenbases of $Z_d$ and $X_d$, respectively.

Simply computing (9) is hence insufficient for our purposes. Let us write $\{y_0, y_0 \in \{0, \ldots, d-1\}\}$ for the eigenbasis of $Z_d$, and note that its Fourier transform $\{F(y_1), y_1 \in \{0, \ldots, d-1\}\}$ is then the eigenbasis of $X_d$. Exploiting the symmetries in our problem, it is straightforward to verify that for all $y_0, y_1 \in \{0, \ldots, d-1\}$

$$|\langle y_0|\Psi_{y_0y_1}\rangle|^2 = |\langle y_1|F\rangle|\langle\Psi_{y_0y_1}|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}}. \quad (10)$$

An important consequence of this is that for any other prior distribution $P_{y_0y_1}$, measurement in the $Z_d$ eigenbasis distinguishes the states

$$\sigma_{y_0} = \sum_{y_1} P_{y_0y_1}(y_0,y_1)|\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}|, \quad (11)$$

with probability at least $1/2 + 1/(2\sqrt{d})$, even when the distribution is unknown. A similar argument can be made for the marginal states $\sigma_{y_1}$ and measurement in the $X_d$ eigenbasis.

Step 3. It now remains to show that, for any possible choice of an additional classical system $C$ [14], one can still guess $Y_C$ from the encoding with a good success probability: one cannot construct a $C$ which would "point to the unknown." Note that we may express the joint state with any other system $C$ as

$$\rho_{Y_0Y_1EC} = \frac{1}{d^2} \sum_{y_0,y_1} |y_0\rangle\langle y_0| \otimes |y_1\rangle\langle y_1| \otimes \rho_{EC}^{y_0y_1}, \quad (12)$$

for some states $\rho_{EC}^{y_0y_1}$ on registers $E$ and $C$. Since the reduced state on $Y_0$, $Y_1$ and $E$ should be the same for any $C$, we have by the fact that $Y_0$ and $Y_1$ are classical that $\text{tr}_C(\rho_{EC}^{y_0y_1}) = |\langle y_0|\Psi_{y_0y_1}\rangle|^2. \quad (13)$

Since $|\langle y_0|\Psi_{y_0y_1}\rangle| \otimes \sigma_{y_1}^C$. Now imagine that we were to perform some arbitrary measurement on $C$, whose outcome would supposedly point to an unknown substring. This merely creates a different distribution $P_{y_0y_1}$ over encoded strings, and we already know from the above that we can still succeed in retrieving either $y_0$ or $y_1$ with probability at least $1/2 + 1/(2\sqrt{d})$ by making a measurement in the $X_d$ or $Z_d$ basis, respectively. Hence for large $d$ we have a recovery probability of roughly $1/2$, implying our main claim.
V. DISCUSSION

The first indication that something may be amiss when looking at knowledge from a quantum perspective was given by Schrödinger [15, who pointed out that one can have knowledge (not ignorance) about the whole, while still being ignorant about the parts [16]. Here, we tackled this problem from a very different direction, starting with the premise that one has ignorance about the whole.

Our results show that contextuality is responsible for much more significant effects than have previously been noted. In particular, it leads to arbitrarily large quantum violations of (3), which can be understood as a Bell-type inequality for noncontextuality. This is still true even for a somewhat helpful physical model, leaking additional bits of information. To our knowledge, this is the first information-theoretic inequality distinguishing NC HV models from quantum theory. While in this Letter, we have restricted our attention to deterministic NC HVs, it is an interesting open question whether our results can be generalized to general models that distinguish between measurement and preparation contextuality [18].

At the heart of our result lies the fact that contextuality allows for strong forms of complementarity in quantum mechanics (often conflated with uncertainty [19]), which intuitively is responsible for allowing the violation of (3). Typically, complementarity is discussed by considering examples of properties of a physical system that one may be able to determine individually, but which cannot all be learned at once. We, however, approach the problem from the other end, and first demonstrate that in an NC HV ignorance about the whole always implies ignorance about a part. We then show that in a quantum world this principle is violated in the strongest possible sense, even with respect to an additional system C. One could think of this as a much more robust way of capturing the notion of complementarity [20].

Finally, it is an interesting open question whether our inequality can be experimentally verified. Note that this is made difficult by the fact that our aim would be to test ignorance rather than knowledge. However, it is conceivable that such an experiment can be performed by building a larger cryptographic protocol whose security relies on being ignorant about one of the parts of a string Y created during that protocol [21]. A quantum violation could then be observed by breaking the security of the protocol, and exhibiting knowledge (rather than ignorance) about some information that could not have been obtained if the protocol was secure.

We thank Jonathan Oppenheim, Christian Schaffner, Tony Short, Robert Spekkens, and members of CQT for useful comments. We are particularly grateful to Tony Short for pointing out that our problem could more easily be explained by means of the game depicted in Fig. 1. T. V. was supported by ARO Grant No. W911NF-09-1-0440 and NSF Grant No. CCF-0905626. S. W. was supported by the National Research Foundation, and the Ministry of Education, Singapore. T. V. and S. W. are grateful to CQT’s nonlocal group and the Mittag-Leffler Institute, respectively.

*vidick@eecs.berkeley.edu
†wehner@nus.edu.sg

[1] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory 55, 4337 (2009).
[2] R. Renner, Ph.D. thesis, ETH Zurich [arXiv:quant-ph/0512258].
[3] A noncontextual model is one in which the observable statistics of a particular measurement do not depend on the context in which the measurement is performed, and, in particular, on which other compatible measurements are possibly performed simultaneously. Here, and as is usual, we consider noncontextual models in which the measurements are composed of deterministic effects.
[4] J. Wullschleger, in Advances in Cryptology—EUROCRYPT ’07, Lecture Notes in Computer Science (Springer-Verlag, Berlin, 2007).
[5] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in Advances in Cryptology—CRYPTO ’07, Lecture Notes in Computer Science, Vol. 4622 (Springer-Verlag, Berlin, 2007), p. 360.
[6] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Phys. Rev. Lett. 101, 020403 (2008).
[7] A. Cabello, S. Severini, and A. Winter, arXiv:1010.2163.
[8] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.107.030402 for complete proofs.
[9] A. Nayak, in Proc. 40th IEEE FOCS (ACM, New York, 1999), p. 369.
[10] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, in Proc. 31st ACM STOC (IEEE, New York, 1999), p. 376.
[11] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. 102, 010401 (2009).
[12] C. Schaffner (personal communication).
[13] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in Proc. 46th IEEE FOCS (IEEE, Pittsburgh, 2005), p. 449.
[14] In principle, C could be arbitrary, but since we are only interested in the result of a 2-outcome measurement on C, we assume that C is indeed already classical and use the subscript C to denote that classical value.
[15] E. Schrödinger, Naturwissenschaften 23, 807 (1935).
[16] The whole here being a maximally entangled state, and the parts being the individual (locally completely mixed) subsystems. See also [17] for an example.
[17] R. Q. Odendaal and A. R. Plastino, Eur. J. Phys. 31, 193 (2010).
[18] R. W. Spekkens, Phys. Rev. A 71, 052108 (2005).
[19] J. Oppenheim and S. Wehner, Science 330, 1072 (2010).
[20] J. Oppenheim and S. Wehner (to be published).
[21] One could consider, e.g., weak forms of oblivious transfer where one only demands security against the receiver.