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

Thomas Vidick and Stephanie Wehner

Phys. Rev. Lett. **107**, 030402 — Published 13 July 2011

DOI: 10.1103/PhysRevLett.107.030402

Does ignorance of the whole imply ignorance of the parts?
— Large violations of non-contextuality in quantum theory

Thomas Vidick[1] and Stephanie Wehner[2]
[1] *Computer Science division, UC Berkeley, USA*[*]
[2] *Center for Quantum Technologies, National University of Singapore, 2 Science Drive 3, 117543 Singapore*[†]

A central question in our understanding of the physical world is how our knowledge of the whole relates to our knowledge of the individual parts. One aspect of this question is the following: to what extent does ignorance about a whole preclude knowledge of at least one of its parts? Relying purely on classical intuition, one would certainly be inclined to conjecture that a strong ignorance of the whole cannot come without significant ignorance of at least one of its parts. Indeed, we show that this reasoning holds in any non-contextual hidden variable model (NC-HV). Curiously, however, such a conjecture is *false* in quantum theory: we provide an explicit example where a large ignorance about the whole can coexist with an almost perfect knowledge of each of its parts. More specifically, we provide a simple information-theoretic inequality satisfied in any NC-HV, but which can be *arbitrarily* violated by quantum mechanics. Our inequality has interesting implications for quantum cryptography.

In this note we examine the following seemingly innocent question: does one's ignorance about the whole necessarily imply ignorance about at least one of its parts? Given just a moments 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 non-contextual 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.

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 $y = y_0y_1$ plays the role of the whole, and y_0, y_1 are the individual parts. Let ρ_y denote an encoding of the string y into a classical or quantum state. In quantum theory, ρ_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 $\{0,\ldots,d-1\}^2$, and imagine that with probability $P_Y(y)$ we are given the state ρ_y. The optimum probability of guessing y given its encoding ρ_y, which lies in a register E, can be written as

$$P_{\rm guess}(Y|E) = \max_{\{\mathcal{M}\}} \sum_{y\in\{0,\ldots,d-1\}^2} P_Y(y)\, p(y|\mathcal{M},\mathcal{P}_y) \ , \quad (1)$$

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 POVMs $\mathcal{M} = \{M_y\}_y$ and $p(y|\mathcal{M},\mathcal{P}_y) = \mathrm{tr}(M_y\rho_y)$. The guessing probability is directly related to the conditional min-entropy $\mathrm{H}_\infty(Y|E)$ through the equation [2]

$$\mathrm{H}_\infty(Y|E) := -\log P_{\rm guess}(Y|E) \ . \quad (2)$$

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 $\mathrm{H}_\infty(Y = Y_0Y_1|E)$ (ignorance about the whole) relate to $\mathrm{H}_\infty(Y_C|EC)$, 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 Figure 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

RESULTS

An inequality valid in any NC-HV model.
We first show that classically, or more generally in any non-contextual hidden variable model [20], 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

$$\mathrm{H}_\infty(Y_C|EC) \gtrsim \frac{\mathrm{H}_\infty(Y_0Y_1|E)}{2} \ . \tag{3}$$

This inequality can be understood as an information-theoretic analogue of Bell inequalities to the question of non-contextuality. 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 [3, 4]. The proof of (3) is a straightforward extension to the case of standard NC-HV models [7, 8] of a classical technique known as min-entropy splitting first introduced by Wullschleger [3], and we defer details to the appendix.

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 $\mathrm{H}_\infty(Y_0|E) = \mathrm{H}_\infty(Y_1|E) \approx 1$, which is much less than $\mathrm{H}_\infty(Y|E) \approx \log d$. However, define C as 0 if $E = Y_1$ and 1 if $E = Y_0$. Then it is clear that $\mathrm{H}_\infty(Y_C|EC) = \log d$, 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 [5, 6], 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 (see appendix) that

$$\mathrm{H}_\infty(Y_C|EC) \gtrsim \frac{\mathrm{H}_\infty(Y_0Y_1|E)}{2} - m \ . \tag{4}$$

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 $\rho^E_{y_0y_1} = |\Psi_y\rangle\langle\Psi_y|$ 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

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

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

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

We first prove that $\mathrm{H}_\infty(Y|E) = \log d$ 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 ρ_E with essentially constant probability. More precisely, for any ccqc-state $\rho_{Y_0Y_1EC}$, with $C \in \{0,1\}$, that satisfies the consistency relation $\mathrm{tr}_C(\rho_{Y_0Y_1EC}) = \rho_{Y_0Y_1E}$, we have

$$\mathrm{H}_\infty(Y_C|EC) \approx 1 \tag{8}$$

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's more, it is not hard to show that this effect still holds even for $\mathrm{H}^\varepsilon_\infty$, for constant error ε, and a "helpful" physical model leaking $m \approx c \log d$ bits of information with $c < 1/2$. Hence, the violation of the inequality (3) has the appealing feature of being very robust.

Implications for cryptography. Our result answers an interesting open question in quantum cryptography [11], 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 [4, 12]. Our example shows that quantum min-entropy splitting is impossible.

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 appendix. Our proof proceeds in three steps: first, by computing $\mathrm{H}_\infty(Y|E)$ we show that the encoding does indeed not reveal much

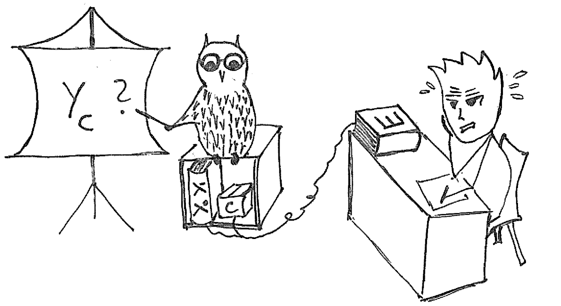

FIG. 1: One can understand our result in terms of a game between Bob and a malicious challenger, the Owl. Imagine Bob is taking a philosophy class teaching him knowledge about Y, chosen uniformly at random. Unfortunately, he never actually attended and had insufficient time to prepare for his exam. Luckily, however, he has been given an encoding E of the possible answers Y_0Y_1, hastily prepared by his old friend Alice. When entering the room, he had to submit E for inspection to the challenger who knows Y_0, Y_1 as well as the encoding Alice might use. After inspection, the challenger may secretly keep a system C, possibly correlated with E, but such that the reduced system on Y_0, Y_1 and E looks untampered with. It is immediately obvious to the challenger that Bob must be ignorant about the whole of Y_0Y_1. But can it always measure and point to a $C = c$ such that Bob is ignorant about Y_c? Classically, this is indeed possible: ignorance about the whole of Y_0Y_1 implies significant ignorance about one of the parts, Y_C. However, a quantum Bob could beat the Owl.

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 dits into a d-dimensional quantum system. To see this more explicitly, recall that $\mathrm{H}_\infty(Y|E) = \log d$ 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 (SDP)

$$\begin{array}{ll} \text{maximize} & \frac{1}{d^2}\sum_{y_0,y_1} \mathrm{tr}\left(M_{y_0y_1}|\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}|\right) \\ \text{subject to} & M_{y_0y_1} \geq 0 \text{ for all } y_0, y_1 \ , \\ & \sum_{y_0,y_1} M_{y_0,y_1} = \mathbb{I} \ . \end{array}$$

The dual SDP is easily found to be

$$\begin{array}{ll} \text{minimize} & \mathrm{Tr}(Q) \\ \text{subject to} & Q \geq \frac{1}{d^2}|\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}| \text{ for all } y_0, y_1 \ . \end{array}$$

Let v_{primal} and v_{dual} be the optimal values of the primal and dual respectively. By the property of weak duality, $v_{\text{dual}} \geq v_{\text{primal}}$ always holds. Hence, to prove our result, we only need to find a primal and dual solutions for which $v_{\text{primal}} = v_{\text{dual}} = 1/d$. It is easy to check that $\hat{Q} = \mathbb{I}/d^2$ is a dual solution with value $v_{\text{dual}} = \mathrm{tr}(\hat{Q}) = 1/d$. 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 $\sum_{y_0,y_1} M_{y_0y_1} = \mathbb{I}$, giving $v_{\text{primal}} = 1/d$.

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

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

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 $\{|y_0\rangle,\, y_0 \in \{0, \ldots, d-1\}\}$ for the eigenbasis of Z_d, and note that its Fourier transform $\{F|y_1\rangle,\, y_1 \in \{0, \ldots, d-1\}\}$ is then the eigenbasis of X_d. Exploiting the symmetries in our problem, it is straightforward to verify that for all $y_0, y_1 \in \{0, \ldots, d-1\}$

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

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

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

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 σ_{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 [21], 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

$$\rho_{Y_0Y_1EC} = \frac{1}{d^2}\sum_{y_0y_1} |y_0\rangle\langle y_0| \otimes |y_1\rangle\langle y_1| \otimes \rho^{EC}_{y_0y_1c} \ , \qquad (12)$$

for some states $\rho^{EC}_{y_0y_1c}$ 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 $tr_C(\rho^{EC}_{y_0y_1c}) = |\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}|$. Since $|\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}|$ is a pure state, this implies that $\rho^{EC}_{y_0y_1c} = |\Psi_{y_0y_1}\rangle\langle\Psi_{y_0y_1}| \otimes \sigma^C_{y_0y_1}$. 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

$$\mathrm{H}_\infty(Y_0|EC = 0) \approx \mathrm{H}_\infty(Y_1|EC = 1) \approx 1 \ . \qquad (13)$$

DISCUSSION

The first indication that something may be amiss when looking at knowledge from a quantum perspective was given by Schrödinger [13], who pointed out that one can have *knowledge* (not ignorance) about the whole, while still being ignorant about the parts [22]. 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 non-contextuality. 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 work, 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 [1].

At the heart of our result lies the fact that contextuality allows for strong forms of complementarity in quantum mechanics (often conflated with uncertainty [14]), 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 [15].

Finally, it is an interesting open question whether our inequality can be experimentally verified. Note that this 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 [23]. 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 CQT's "non-local club" 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 Figure 1. TV was supported by ARO Grant W911NF-09-1-0440 and NSF Grant CCF-0905626. SW was supported by the National Research Foundation, and the Ministry of Education, Singapore. TV and SW are grateful to CQT and the Mittag-Leffler Institute respectively.

* Electronic address: vidick@eecs.berkeley.edu
† Electronic address: wehner@nus.edu.sg

[1] R. Spekkens, Physical Review A **71**, 052108 (2005).
[2] R. König, R. Renner, and C. Schaffner, IEEE Trans. Info. **55** (2009).
[3] J. Wullschleger, in *Advances in Cryptology — EUROCRYPT '07* (Springer-Verlag, 2007), Lecture Notes in Computer Science.
[4] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptology—CRYPTO '07* (Springer-Verlag, 2007), vol. 4622 of *Lecture Notes in Computer Science*, pp. 360–378.
[5] A. Nayak, in *Proc. 40th IEEE FOCS* (1999), pp. 369–376.
[6] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, in *Proc. 31st ACM STOC* (1999), pp. 376–383.
[7] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumsovsky, Phys. Rev. Lett. **101**, 020403 (2008).
[8] A. Cabello, S. Severini, and A. Winter (2010), arXiv:1010.2163.
[9] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[10] R. Spekkens, D. Buzacott, A. Keehn, B. Toner, and G. Pryde, Phys. Rev. Lett. **102**, 010401 (2009).
[11] C. Schaffner (2007), Personal communication.
[12] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proc. 46th IEEE FOCS* (2005), pp. 449–458.
[13] E. Schrödinger, Naturwissenschaften **23**, 807,823,840 (1935).
[14] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
[15] J. Oppenheim and S. Wehner (2010), in preparation.
[16] A. J. Short and S. Wehner, New Journal of Physics **12**, 033023 (2010).
[17] R. Renner, Ph.D. thesis, ETH Zurich (2005), quant-ph/0512258.
[18] A. Bowie, *Introduction to German philosophy: from Kant to Habermas* (2003).
[19] R. Q. Odendaal and A. R. Plastino, Eur. J. of Physics **31**, 193 (2010).
[20] A non-contextual 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 non-contextual models in which the measurements are composed of deterministic effects.
[21] 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.
[22] The whole here being a maximally entangled state, and the parts being the individual (locally completely mixed) subsystems. See also [19] for an example.
[23] One could consider e.g. weak forms of oblivious transfer where one only demands security against the receiver.