Quantum preparation uncertainty and lack of information

Rozpedek, Filip; Kaniewski, Jdrzej; Coles, Patrick J.; Wehner, Stephanie

DOI
10.1088/1367-2630/aa5d64

Publication date
2017

Document Version
Final published version

Published in
New Journal of Physics

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Quantum preparation uncertainty and lack of information

To cite this article: Filip Rozpdek *et al* 2017 *New J. Phys.* **19** 023038

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
23 August 2016

REVISED
15 January 2017

ACCEPTED FOR PUBLICATION
1 February 2017

PUBLISHED
20 February 2017

PAPER

Quantum preparation uncertainty and lack of information

Filip Rozpędek[1], **Jędrzej Kaniewski**[1,2,3], **Patrick J Coles**[4] **and Stephanie Wehner**[1]

[1] QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
[2] Centre for Quantum Technologies, 3 Science Drive 2, 117543 Singapore
[3] QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, DK-2100 Copenhagen, Denmark
[4] Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, N2L3G1 Waterloo, Ontario, Canada

E-mail: f.d.rozpedek@tudelft.nl

Keywords: uncertainty principle, measurement uncertainty, quantum guessing game, quantum information, quantum foundations, guessing probability

Abstract

The quantum uncertainty principle famously predicts that there exist measurements that are inherently incompatible, in the sense that their outcomes cannot be predicted simultaneously. In contrast, no such uncertainty exists in the classical domain, where all uncertainty results from ignorance about the exact state of the physical system. Here, we critically examine the concept of preparation uncertainty and ask whether similarly in the quantum regime, some of the uncertainty that we observe can actually also be understood as a lack of information (LOI), albeit a lack of *quantum* information. We answer this question affirmatively by showing that for the well known measurements employed in BB84 quantum key distribution (Bennett and Brassard 1984 *Int. Conf. on Computer System and Signal Processing*), the amount of uncertainty can indeed be related to the amount of available information about additional registers determining the choice of the measurement. We proceed to show that also for other measurements the amount of uncertainty is in part connected to a LOI. Finally, we discuss the conceptual implications of our observation to the security of cryptographic protocols that make use of BB84 states.

1. Introduction

The uncertainty principle forms one of the cornerstones of quantum theory. As first observed by Heisenberg [15] and then rigorously proven by Kennard [19], it is impossible to perfectly predict the measurement outcomes of both position and momentum observables. This notion was generalised by Robertson to an arbitrary pair of observables [26] showing that uncertainty is an inherent feature of any non-commuting measurements in quantum mechanics. The described uncertainty is often referred to as preparation uncertainty, because it states that it is impossible to prepare a quantum state for which one could perfectly predict the measurement outcome of both observables.

A modern way of capturing the notion of preparation uncertainty is by means of a *guessing game* [2]. Such a game makes the concept of preparation uncertainty operational and is of great use in proving the security of quantum cryptographic protocols [7]. Figure 1 summarises the game, which in its simplest form works as follows. Bob prepares system B in an arbitrary state ρ_B of his choosing and then passes it to Alice. Alice performs one of two incompatible measurements labelled by $r = 0$ and $r = 1$ according to a random coin flip contained in the register R and obtains measurement outcome X. She then informs Bob which measurement she performed by sending him the register R. Bob wins the game if he correctly guesses Alice's measurement outcome X.

To see why this captures the essence of the uncertainty principle, note that if the measurements are incompatible, then there exists no state ρ_B that Bob can prepare that would allow him to guess the outcomes for both choices of measurements with certainty. Uncertainty can thus be quantified by a bound on the average probability that Bob correctly guesses X. That is, a relation of the form

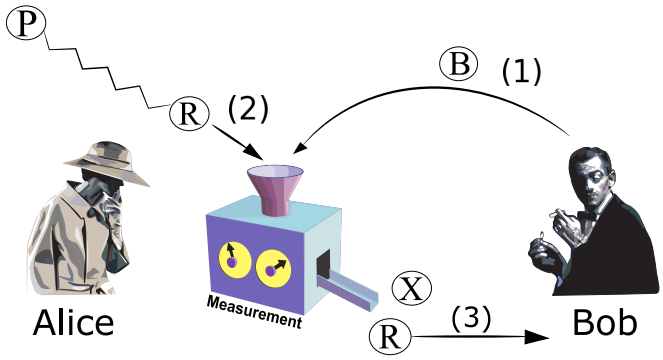

Figure 1. Uncertainty guessing game. The game runs as follows: (1) First, Bob prepares system B in a state ρ_B and sends it to Alice. We show in appendix A that Bob's best strategy is to prepare a pure state $\rho_B = |\phi\rangle\langle\phi|_B$. (2) Second, Alice measures B in a basis determined by the state of register R. (3) Finally, Alice obtains the classical outcome X and sends R to Bob. Bob can then measure R in order to help him guess X. Note that R may be initially prepared in a mixed state ρ_R, and Bob does not have access to the purifying system of ρ_R, denoted as P in the figure. Hence, P embodies Bob's lack of information in this game.

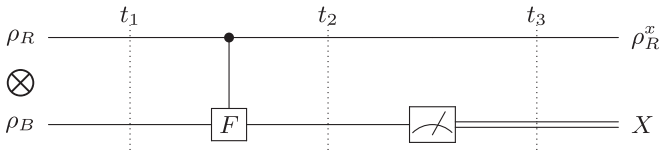

Figure 2. Quantum circuit of the uncertainty game. At time t_1, Alice's register R and Bob's system B are uncorrelated. We will assume that Alice measures in the standard basis and one additional basis depending on the state of register R. To allow for maximum intrinsic uncertainty, we take the other basis to be maximally incompatible. Here, we choose it to be the Fourier basis. Hence the two measurements correspond to measuring in two mutually unbiased bases. If B is a qubit, then this means that Alice measures in the standard and Hadamard basis, which are the two bases used in BB84 quantum key distribution. This basis choice is performed by Alice applying a controlled unitary between the two registers, leading to a correlated state at time t_2. Alice then measures B to obtain the measurement outcome X. If the register R is classical, then the two operations together correspond to performing a random measurement. If the register R contains some non-zero coherence, then those operations describe a procedure which could be understood as a 'measurement in a superposition of two bases'. After time t_3, Alice sends R to Bob. At this stage, $\rho_{RX} = \sum_x p_x \rho_R^x \otimes |x\rangle\langle x|_X$ is a qc-state. Bob can then make a measurement in order to distinguish the states ρ_R^x, i.e., to help him guess X. Note that Bob knows which states ρ_R^x he wants to distinguish since he knows the form of the initial state $|\xi_{RP}\rangle$ and the measurements Alice can perform.

$$P_{\text{guess}}(X|\text{Bob}) = p(r=0)P_{\text{guess}}(X|\text{Bob}, r=0) + p(r=1)P_{\text{guess}}(X|\text{Bob}, r=1) \leqslant 2^{-\zeta}, \tag{1}$$

for all ρ_B. Equivalently, we can relate the above defined guessing probability to the min-entropy $H_{\min}(X|\text{Bob}) = -\log P_{\text{guess}}(X|\text{Bob})$ (in this article all logarithms are base 2), so that we obtain an inequality:

$$H_{\min}(X|\text{Bob}) \geqslant \zeta. \tag{2}$$

This expression forms an uncertainty relation as long as the RHS is non-trivial (i.e. $\zeta > 0$). Analogous relations exist for other entropies [7], but here we focus on the min-entropy since it is the relevant measure for quantum cryptography and randomness generation, and it quantifies the winning probability for the aforementioned guessing game.

In this work, we seek a deeper understanding of the uncertainty principle by considering a more general scenario than the typical guessing game and observing the conditions under which Bob's uncertainty vanishes. In particular, the generalisation we consider is to allow Bob to have additional information—possibly *quantum* information—about Alice's measurement choice. This generalisation is closely related to recent proposals for quantum control experiments [5, 17]. To elaborate, we note that Alice's random measurement choice in the guessing game can be implemented by preparing a qubit R in the maximally mixed state $\rho_R = \mathbb{I}/2$ and then performing a unitary operation on B conditioned on the state of R (see figure 2 above). In the generalised game that we consider, we allow ρ_R to be a more general state, possibly with some coherence. As we discuss below, allowing for coherence in ρ_R corresponds to giving Bob more information.

Our motivation for considering this scenario is to distinguish between uncertainty that is due to Bob's lack of information (LOI) versus uncertainty that is intrinsic or unavoidable. To help clarify these notions, we remark that a classical theory admits no intrinsic uncertainty. Classical here refers to commuting measurements that are jointly diagonal in one predefined basis. If Alice employed such measurements in the aforementioned guessing game, then the only way for her to prevent Bob from winning the game would be for her to add noise to her

measurement outcomes, i.e., implement noisy measurements. Yet, we would classify Bob's uncertainty in this case as LOI uncertainty, as he simply lacks the information about the noise Alice adds. Hence, the arising uncertainty is clearly not an intrinsic feature of the measurements.

Notice that preparing the register R in the maximally mixed state $\rho_R = \mathbb{I}/2$ injects classical randomness into the protocol. It is unclear whether or not this randomness is ultimately responsible for the uncertainty principle, and this is a question we aim to answer. We emphasise that the scenario we consider differs from other variants of the uncertainty principle which derive bounds involving the purity or entropy of ρ_B [2–4, 6, 8, 9, 11–14, 21–23, 25, 27].

Interestingly we find that in the special case where Bob's system is a qubit ($d = 2$), there is no intrinsic uncertainty but all the uncertainty is due to LOI. That is, if Bob has complete knowledge about the preparation of R (i.e., R is in a pure state), then his uncertainty vanishes. In contrast, for all dimensions $d > 2$, we find that there is always some intrinsic uncertainty. That is, even with the full knowledge about the preparation of R, Bob cannot win the guessing game with unit probability. Before we discuss these results in detail, let us outline the physical setup.

2. Physical setup

2.1. Degrees of ignorance

In this section we describe the generalised guessing game shown in figure 1. Here, Alice prepares a register system R in some state ρ_R. Meanwhile Bob prepares system B in state ρ_B and sends it to Alice. Alice measures B in a basis determined by the state of R. Then she passes R to Bob, and he tries to guess her measurement outcome, possibly using the information stored in R. We are interested in understanding how much of Bob's uncertainty (i.e., his inability to win this game) is due to LOI and how much corresponds to intrinsic (or unavoidable) uncertainty.

To better understand this, let us examine what Bob does and does not have access to in figure 1. Since ρ_R is generally a mixed state, it can be purified by considering an additional system, P. Even though Bob is given access to R, we emphasise that he does not have access to P in our guessing game. Hence, we can think of P as representing Bob's LOI.

For example, consider the case when $\rho_R = \mathbb{1}/2$ is maximally mixed, which corresponds to the case where the measurement choice is a classical coin flip (i.e., the typical uncertainty game considered in the literature [2]). The purification is a maximally entangled state such as

$$|\xi_{RP}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_R|0\rangle_P + |1\rangle_R|1\rangle_P). \tag{3}$$

At the other extreme is the case where ρ_R is pure, i.e.,

$$|\xi_{RP}\rangle = |\xi_R\rangle \otimes |\xi_P\rangle \tag{4}$$

is a product state. We will take $|\xi_R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, i.e., we choose an equal superposition in correspondence with the idea that both measurements were previously chosen with equal probability. Intuitively, when the initial state is maximally entangled, then Bob will later suffer from a maximum LOI about P. However, in the case where the two systems are uncorrelated, Bob does not need P at all. In other words, there is no LOI on his part, because R is pure.

There are many ways to interpolate between these two extremes in terms of a measure of correlation between R and P. Here, we choose one that is intuitive when we think about 'how much' of P Bob is actually lacking. Concretely, we imagine that apart from the classical coin C (which is a part of R), R and P are actually comprised of many environmental subsystems $E_1, \ldots, E_n$, and we quantify Bob's LOI by the number of the environment systems that are part of P instead of part of R. Specifically, we take

$$|\xi_{RP}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_C \otimes \bigotimes_{i=1}^{n}|\alpha\rangle_{E_i} + |1\rangle_C \otimes \bigotimes_{i=1}^{n}|\beta\rangle_{E_i}\right), \tag{5}$$

where $RP = CE_1 \ldots E_n$. The environments E_j's are two-dimensional registers and $|\langle\alpha|\beta\rangle| = 1 - \epsilon$, with $\epsilon > 0$ and $\epsilon \ll 1$ so that each individual E_j holds very little information about the state of the coin C. However, we see that $\langle\alpha|\beta\rangle^n \to 0$ as $n \to \infty$. We thus see that for $n \to \infty$ and $R = C$, $P = E_1 \ldots E_n$, we approach the extreme case of R being essentially classical, and $|\xi_{RP}\rangle$ being maximally entangled. This idea of approximating the notion of a classical register by 'copying' information into a large number of environmental systems E_j is due to Zurek [30].

We can now interpolate between the two extremes by letting $R = CE_1 \ldots E_j$ and $P = E_{j+1} \ldots E_n$. We have that

$$\rho_R = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \gamma^* |0\rangle\langle 1| + \gamma |1\rangle\langle 0|), \tag{6}$$

where

$$|0\rangle_R := |0\rangle_C \otimes \bigotimes_{i=1}^{j} |\alpha\rangle_{E_i}, \tag{7}$$

$$|1\rangle_R := |1\rangle_C \otimes \bigotimes_{i=1}^{j} |\beta\rangle_{E_i}, \tag{8}$$

$$\gamma = \langle\alpha|\beta\rangle^{n-j}. \tag{9}$$

We see that $|\gamma|$ increases monotonically with j, the number of environmental subsystems contained in R, and hence the number of subsystems to which Bob is given access later on. The extreme cases $\gamma = 0$ and $\gamma = 1$ correspond respectively to $j = 0$ and $j = n$ (again note that the number of environment subsystems is very large so that we always consider the limit $n \to \infty$). In appendix A we show that for the uncertainty game it is only the modulus of γ that matters. Therefore, we will only consider the case of real and positive γ, i.e. $\gamma \in [0, 1]$.

2.2. Uncertainty game

Let us now revisit our uncertainty guessing game (see figures 1 and 2) with a more detailed description. First, Bob prepares system B in a state ρ_B and sends it to Alice. Second, Alice measures B and obtains the classical outcome X, with the measurement basis determined by the state of register R given by:

$$\rho_R = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \gamma |0\rangle\langle 1| + \gamma |1\rangle\langle 0|). \tag{10}$$

Specifically, as depicted in figure 2, states $|0\rangle$ and $|1\rangle$ on R are, respectively, associated with measuring in the standard basis and Fourier basis on B (we have chosen maximally incompatible bases to maximise the 'inherent' uncertainty). Next, Alice sends Bob the register R. Finally Bob measures R to help him produce a guess for X. This defines a two-parameter family of uncertainty games which depend on: $d \in \{2, 3, \ldots\}$, the number of possible outcomes (which fixes the dimension of the quantum state ρ_B supplied by Bob and the dimension of the Fourier transform in figure 2) and $\gamma \in [0, 1]$, describing the amount of information about R that is held in P, or equivalently the amount of coherence in R.

3. Methods

Here we provide a high level overview of the methods used to obtain the results presented in the next section. For complete analysis we refer the reader to the appendices.

After Alice has performed her measurement, at time t_3 in figure 2 the resulting qc-state between the register R and the outcome register X is:

$$\rho_{RX}(\gamma, d, \rho_B) = \sum_x \tilde{\rho}_R^x(\gamma, d, \rho_B) \otimes |x\rangle\langle x|_X, \tag{11}$$

where $\tilde{\rho}_R^x(\gamma, d, \rho_B) = p_x(d, \rho_B)\rho_R^x(\gamma, d, \rho_B)$ is the subnormalised post-measurement state of the register R corresponding to the outcome $X = x$. In terms of Bob's input state ρ_B, this state has the form:

$$\tilde{\rho}_R^x(\gamma, d, \rho_B) = \frac{1}{2}\begin{pmatrix} \langle x|\rho_B|x\rangle & \gamma\langle x|\rho_B F^\dagger|x\rangle \\ \gamma\langle x|F\rho_B|x\rangle & \langle x|F\rho_B F^\dagger|x\rangle \end{pmatrix}, \tag{12}$$

as derived in appendix A. Since Bob later gains access to register R, we see that in order to guess the resulting outcome $X = x$, Bob should try to determine which quantum state $\rho_R^x(\gamma, d, \rho_B)$ he has received. Hence, his guessing problem becomes equivalent to the problem of distinguishing quantum states $\{\rho_R^x(\gamma, d, \rho_B)\}$ occurring with probabilities $\{p_x(d, \rho_B)\}$.

The probability of Bob correctly discriminating those states with the optimal strategy, i.e., with the optimal measurement on R (described by POVM elements $\{M_x\}$), is given by [29]:

$$p_{\text{guess}}(\gamma, d, \rho_B) = \max_{\{M_x\}} \sum_{x=0}^{d-1} p_x(d, \rho_B)\mathrm{Tr}[M_x\rho_R^x(\gamma, d, \rho_B)]. \tag{13}$$

In appendix A we show that to achieve $p_{\text{guess}}^{\max}(\gamma, d)$, the guessing probability optimised over input states ρ_B, it is sufficient to consider only pure input states $\rho_B = |\phi\rangle\langle\phi|_B$. Hence, the maximum value of $p_{\text{guess}}(\gamma, d, \rho_B)$ for a given γ and d is the result of optimising the guessing probability over all input states $|\phi\rangle_B$ of Bob (for convenience we will often omit the subscript 'B' from $|\phi\rangle_B$). That is,

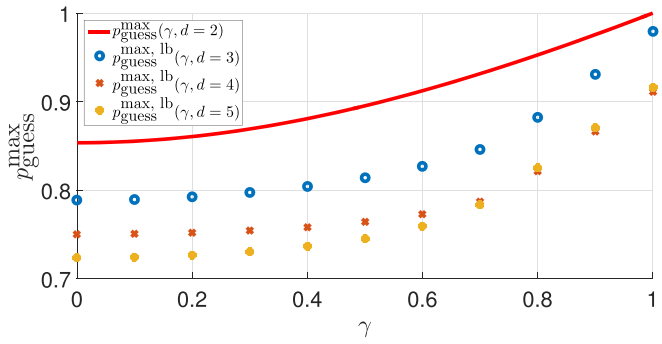

Figure 3. The optimal guessing probabilities $p^{\max}_{\text{guess}}(\gamma,\, d)$ as a function of γ for different d. The solid line corresponds to the analytical solution $p^{\max}_{\text{guess}}(\gamma,\, d=2)$ for a two-dimensional game. The remaining data corresponds to the numerical lower bounds $p^{\max,\,\text{lb}}_{\text{guess}}(\gamma,\, d)$ for $d=3,\,4,\,5$. For $\gamma=0$ the numerical values coincide with the analytical solution $p^{\max}_{\text{guess}}(\gamma=0,\, d)=\frac{1}{2}\left(1+\frac{1}{\sqrt{d}}\right)$. The crossing of the dotted lines corresponding to $d=4$ and $d=5$ is discussed in section 5.

$$p^{\max}_{\text{guess}}(\gamma,\, d)=\max_{|\phi\rangle} p_{\text{guess}}(\gamma,\, d,\, |\phi\rangle). \tag{14}$$

Solving this optimisation problem is not an easy task. Note that the function which we want to optimise over all the POVM elements $\{M_x\}$ in equation (13) is linear in those operators. Hence, for a specific input state $|\phi\rangle_B$ the optimisation can be performed using techniques of semi-definite programming. However, the above optimisation problem in equation (14) involves optimisation both over POVM elements and input states $|\phi\rangle_B$. Clearly, $\tilde{\rho}^x_R(\gamma,\, d,\, |\phi\rangle_B)$ is quadratic in $|\phi\rangle_B$. Note that this problem can be made linear in the input state by again considering optimisation over all mixed states ρ_B, i.e. our problem is then linear in ρ_B. However, the full problem of optimising over both $\{M_x\}$ and ρ_B:

$$p^{\max}_{\text{guess}}(\gamma,\, d)=\max_{\rho_B}\max_{\{M_x\}}\sum_{x=0}^{d-1} p_x(d,\, \rho_B)\,\text{Tr}[M_x\rho^x_R(\gamma,\, d,\, \rho_B)] \tag{15}$$

turns out not to be jointly concave in both of those variables and so cannot be solved using techniques of convex optimisation.

3.1. Two-dimensional game

Nevertheless, we can solve this problem analytically for $d=2$. For this case, we derived our result (stated below in theorem 1) by noting that the problem of optimising over the POVM elements in equation (13) (for fixed states $\{\rho^x_R\}$ occuring with fixed probabilities $\{p_x\}$) has been solved analytically by Helstrom [16]:

$$p_{\text{guess}}(\gamma,\, d=2,\, \rho_B)=\frac{1}{2}(1+\|\tilde{\rho}^0_R(\gamma,\, \rho_B)-\tilde{\rho}^1_R(\gamma,\, \rho_B)\|_1), \tag{16}$$

where $\|\cdot\|_1$ denotes the trace norm and we have omitted the $d=2$ argument in $\tilde{\rho}^0_R$ and $\tilde{\rho}^1_R$. In this way we obtain an expression for $p_{\text{guess}}(\gamma,\, d=2,\, \rho_B)$ which we then analytically optimise over the input states ρ_B for every value of $\gamma\in[0,\,1]$ to obtain $p^{\max}_{\text{guess}}(\gamma,\, d=2)$ (see appendix B). For completeness, we still optimise over all qubit states ρ_B, not only the pure ones. This allows us to find all the qubit input states that achieve $p^{\max}_{\text{guess}}(\gamma,\, d=2)$.

3.2. Higher-dimensional games

For $d>2$ we cannot calculate $p^{\max}_{\text{guess}}(\gamma,\, d>2)$ analytically, since there exists no known analytical expression for the probability of correctly distinguishing more than two quantum states. However, we can find $p_{\text{guess}}(\gamma,\, d,\, |\phi\rangle)$ for an arbitrary state $|\phi\rangle$ using techniques from semi-definite programming. We obtain numerical lower bounds for $p^{\max}_{\text{guess}}(\gamma,\, d)$, shown in figure 3, by solving a semi-definite programme for $p_{\text{guess}}(\gamma,\, d,\, |\phi\rangle)$ and numerically searching for local maxima of $p_{\text{guess}}(\gamma,\, d,\, |\phi\rangle)$ with respect to the input state $|\phi\rangle$ using the Nelder–Mead algorithm. We repeat the search multiple times with a randomly generated initial state in each run, that is drawn uniformly from unit vectors on $\mathbb{C}^d$.

4. Results

In section 1 we discussed that classical uncertainty arises solely from LOI. Here we show that even in the quantum case, uncertainty can in part be understood as a LOI that Bob has—namely a lack of quantum information about the register P. For the case of $d=2$ and BB84 measurements as they are used in quantum key

distribution (QKD), this effect is indeed dramatic. We find (see theorem 1 below) that there is no more uncertainty at all in the case where R is pure and P is uncorrelated, meaning that Bob does not suffer from any LOI.

First, we consider the typical uncertainty game where R is a classical coin, i.e., R and P are maximally entangled ($\gamma = 0$). In this case the maximum value of the guessing probability (for completeness derived in appendix C) is given by:

$$p_{\text{guess}}^{\max}(\gamma = 0,\, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right). \tag{17}$$

The states ρ_B that achieve the guessing probability of equation (17) are the pure states

$$|\phi_{jl}\rangle := c(|j\rangle + \omega^{jl} F^{\dagger}\,|l\rangle), \tag{18}$$

where $c = \sqrt{\sqrt{d}/(2\sqrt{d} + 2)}$ is the normalisation constant, F denotes a quantum Fourier transform defined in appendix A, ω is the dth root of unity and j and l are integer indices that lie in the range $\{0,\, 1, \ldots, d - 1\}$ so that the pure states $|j\rangle$ and $|l\rangle$ denote the corresponding eigenstates of the standard basis. The states defined in equation (18) are the states where the dominant classical outcome for the measurement is j in the standard basis and l in the Fourier basis.

Now we consider the more general case where R may have some coherence. For $d = 2$ we have found the analytical solution for all $\gamma \in [0,\, 1]$. In this case the guessing probability is equal to the probability of successfully distinguishing the two possible post-measurement states of the basis register, namely ρ_R^0 and ρ_R^1 corresponding to outcomes 0 and 1 respectively (see figure 2).

Theorem 1. *The maximum guessing probability for a two-dimensional game ($d = 2$), optimised over all input states ρ_B is given by:*

$$p_{\text{guess}}^{\max}(\gamma,\, d = 2) = \frac{1}{2}\left(1 + \frac{\sqrt{2 + 2\gamma^2}}{2}\right). \tag{19}$$

In particular, for $\gamma = 1$ one achieves perfect guessing, that is $p_{\text{guess}}^{\max}(\gamma = 1,\, d = 2) = 1$.

It is also possible to express this guessing probability in terms of the purity of the basis register:

$$p_{\text{guess}}^{\max}(\gamma,\, d = 2) = \frac{1}{2}(1 + \sqrt{\text{Tr}[\rho_R^2]}). \tag{20}$$

For all $\gamma \in [0,\, 1]$, this guessing probability can be achieved by one of two orthogonal input states of Bob, $|\phi_{01}\rangle = c(|0\rangle + |-\rangle)$ and $|\phi_{10}\rangle = c(|1\rangle + |+\rangle)$, which are mapped by the Hadamard transformation onto each other. (For $\gamma = 0$ this guessing probability can of course also be achieved by $|\phi_{00}\rangle$ and $|\phi_{11}\rangle$, as then equation (19) reduces to equation (17). For $\gamma = 1$ the optimal input states form a continuous one-parameter family, see appendix B.)

From equation (19) we see that Bob can achieve perfect guessing probability for the case when R is uncorrelated from P (and so P holds no information about R and there is no LOI about the measurement process on Bob's side). This is connected to the fact, that for $\gamma = 1$ and a suitable choice of input state ρ_B, the joint state ρ_{RB} becomes maximally entangled at time t_2 just before Alice's measurement in figure 2 (see appendix D below for discussion of this connection). The above results for $d = 2$ are derived in appendix B.

Now it is interesting to ask what happens to the measurement uncertainty in the game with more than two measurement outcomes in higher dimension. It is intuitive that the dramatic effect we see for $d = 2$ should be less prominent here. After all, Bob is trying to guess measurement outcomes that can take on d values, while R and P each remain two-dimensional and can hence only contain limited information about the outcomes. We first make this intuition precise in the following theorem.

Theorem 2. *For d-dimensional games with any $d > 2$ it is not possible to achieve perfect guessing, i.e.,*

$$p_{\text{guess}}^{\max}(\gamma,\, d > 2) < 1, \qquad \forall\ \gamma \in [0,\, 1]. \tag{21}$$

Crucially, however, coherence in register R *always* facilitates guessing.

Theorem 3. *For d-dimensional games with d being arbitrary, the maximum guessing probability when R has any non-zero amount of coherence is always strictly greater than the case of maximally mixed R. That is, for all $\gamma' > 0$*

$$p_{\text{guess}}^{\max}(\gamma = \gamma',\, d) > p_{\text{guess}}^{\max}(\gamma = 0,\, d), \qquad \forall\ d \geqslant 2. \tag{22}$$

Moreover, we show that for a subclass of the input states that are optimal for $\gamma = 0$, the guessing probability

monotonically increases with γ. Specific values of $p_{\text{guess}}^{\max}(\gamma, d)$ are lower bounded numerically. Those results are depicted in figure 3.

5. Discussion

We have shown that quantum preparation uncertainty is not always inherent to the measurement process but on the contrary it depends on the amount of information that one has about this process. In particular, for $d = 2$, if Bob has all the information about the measurement process, then he can perfectly predict the measurement outcome. In the cryptographic protocols that use BB84 states, ρ_R is a maximally mixed state. Hence, from the perspective of cryptographic security, this shows that it is important for the purification of ρ_R to remain inaccessible to the adversary. In particular, the more of the purification P becomes incorporated into R, the larger the guessing probability becomes and so the more the security of our cryptographic protocols becomes compromised. Passive encoding schemes [10], which generate the QKD signal states by performing a measurement on a quantum register (analogous to our R), would especially need to consider this issue.

On the other hand, we found that there is always some unavoidable uncertainty for guessing games in higher dimensions, $d > 2$. This result is somewhat intuitive when one considers that our guessing game allows for two measurements, and hence system R is only two-dimensional. The intuition behind this unavoidable uncertainty is that the state ρ_R, in which the information about the measurement outcome becomes encoded, is always a qubit, while the number of outcomes is d. Hence, even if Bob inputs a state that results in entanglement between the two systems, this entanglement lives in a two-dimensional subspace of the d-dimensional space $\mathcal{H}_B$. Therefore, the joint state cannot be maximally entangled and since the Fourier transformation applied to elements of the standard basis generates a basis that is unbiased to it, the correlations before the measurement of Alice do not align with the standard basis in which the measurement is performed. This fact can also be seen by noting that perfect guessing could only occur if only two of the resulting outcomes had non-zero probability and if those outcomes produced orthogonal post-measurement states of the register R. It turns out that all those conditions cannot be met simultaneously.

The crossing of the dotted lines corresponding to $d = 4$ and $d = 5$ in figure 3 is an interesting phenomenon. We have investigated it extensively using multiple methods and numerical solvers on which we now elaborate. As mentioned in section 3 the problem of optimisation over both input states and measurements is in general very hard because the optimisation problem that we face is not convex. That is we can have no guarantee that the solution that we find is the global maximum. Therefore the numerical results are just the lower bounds on the $p_{\text{guess}}^{\max}$, as they represent achievable values of $p_{\text{guess}}^{\max}$ that have been found. Nevertheless we have used multiple methods to look for these optimal bounds. Apart from the method described in section 3.2 (where part of the data was checked by rerunning the programme with multiple numerical solvers), we have tried imposing a net over the statespace and solving the semi-definite programme over the measurements for each of those states. Then the procedure was repeated with a denser net in the region where the highest guessing probability has been found. This step of 'zooming-in' has then been repeated multiple times. Finally we have also used the 'Penlab' solver, which can also provide achievability bounds for nonlinear problems. Application of those other methods however resulted in much worse bounds and so they shed no light on the nature of the crossing in figure 3.

Nevertheless, despite the fact that we only find achievable bounds, we believe that the crossing seen in figure 3 could in principle arise even for the exact solution. We note that while asymptotically we expect $p_{\text{guess}}^{\max}(\gamma, d)$ to tend to 0.5 as d tends to infinity, it is possible for $p_{\text{guess}}^{\max}(\gamma, d)$ to be larger for $d = 5$ than for $d = 4$ above some threshold $\gamma = \gamma_0$. As we mentioned earlier, the optimal guessing probability depends on the optimal correlations between two-dimensional register R and d-dimensional register B. The resulting state is asymmetric and so it is possible that certain favourable correlations are possible for $d = 5$, while not possible for $d = 4$. The complexity of the problem can be seen by looking at the Schmidt coefficients of the joint state of registers R and B at time t_2 in figure 2. For $d = 2$ and $\gamma = 1$ the optimal input states are precisely the ones that lead to a maximally entangled state between those two registers at time t_2. One might intuitively guess that also for $d > 2$ forming maximally entangled states within the two-dimensional subspace of B will lead to the optimal guessing probability for $\gamma = 1$. This turns out not be sufficient: we checked specific states that lead to maximal entanglement in dimensions $d = 3, 4, 5$ and their performance is suboptimal. At the same time, all the optimal input states found numerically that achieve $p_{\text{guess}}^{\max,\text{lb}}(\gamma = 1, d)$ for $d = 3, 4, 5$ lead to unbalanced Schmidt coefficients. While we have found multiple states that achieve $p_{\text{guess}}^{\max,\text{lb}}(\gamma = 1, d)$ for each of $d = 3, 4, 5$, all of them lead to exactly the same Schmidt coefficients of the joint state, which we list in table 1. This fact, together with the irregularity of our numerical curves, reveals the complexity of the geometry of this problem.

Table 1. Schmidt coefficients of the joint state on RB at time t_2 for the input states that achieve $p_{\text{guess}}^{\max,\text{lb}}(\gamma = 1, d)$.

	Schmidt coefficients	
$d = 3$	0.8122	0.5834
$d = 4$	0.8314	0.5556
$d = 5$	0.7415	0.6709

In future work, it would be very natural to consider games with more than two measurements. It would be interesting to investigate whether a higher dimensional register R could then encode more information about the measurement outcome. Specifically, for the scenario with d mutually unbiased measurements (if they exist) and d possible outcomes, it is reasonable to ask whether one can again achieve perfect guessing (e.g., due to the possibility of creating maximal entanglement between R and B).

Another natural extension of our game would be to provide Bob with access to a quantum memory [2]. In such a scenario an interesting task would be to investigate the effect of the trade-off between Bob's amount of accessible information about the measurement process and the quality of entanglement between B and Bob's quantum memory.

Finally, we would like to emphasise that while the described guessing game seems to be only an abstract tool that we use to investigate the connection between quantum preparation uncertainty and LOI, the game described in figure 1 could in fact be implemented experimentally, e.g., using a Mach–Zehnder interferometer for single photons. For simplicity consider the case $d = 2$, although the following discussion can be extended to $d > 2$ by considering an interferometer with more than two paths. Suppose that system R is the photon's polarisation, while B is the photon's spatial degree of freedom (the path that it takes in the interferometer). Allowing Bob to have access to the first variable beam splitter of the interferometer allows him to prepare an arbitrary pure qubit state ρ_B inside the interferometer (Bob is allowed to freely choose the reflectance and the relative phase of the beam splitter). The controlled Fourier transform in figure 2 is implemented by making the second beam splitter of the interferometer a so-called quantum balanced beam splitter [17]. That is, the photon's polarisation controls whether or not the balanced (50/50) beam splitter appears in the photon's path. Hence, this beam splitter can be effectively in a superposition of being absent and present, if one chooses the polarisation to be in a superposition. This would be a so-called quantum control experiment [5]. Let us note that such a quantum beam splitter has been implemented experimentally [18, 24, 28]. The winning condition of the game for Bob is correctly guessing which one of the two photon detectors clicked, after being able to measure the polarisation state of the photon behind the quantum beam splitter.

Acknowledgments

We would like to greatly thank Jonas Helsen and Le Phuc Thinh for help with convex optimisation techniques. We are thankful to Pim Veldhuisen and Wouter Uijens for help with semi-definite programme implementation, to Thomas Schiet and Doru Sticlet for useful discussions on numerical sampling techniques and to David Elkouss, Kenneth Goodenough, Corsin Pfister and Mark Steudtner for valuable comments on the manuscript. We are also very grateful to Dmytro Vasylyev for preparing figure 1. FR and SW are funded by STW, NWO VIDI and an ERC Starting Grant. JK is supported by Ministry of Education, Singapore and the European Research Council (ERC Grant Agreement 337603). PJC is funded by Industry Canada, Sandia National Laboratories, Office of Naval Research, NSERC Discovery Grant, and Ontario Research Fund.

Appendix A. The uncertainty game: definitions and basic derivations

A.1. Time evolution of the quantum circuit

Following the quantum circuit of the uncertainty game in figure 2 (in the main article), we derive the explicit form of the density matrices that Bob needs to distinguish in order to win the game. There are different classes of games depending on the parameter d corresponding to the dimension of the Fourier transform or equivalently, the number of possible outcomes of Alice. Bob prepares a state ρ_B of dimension d and sends it to Alice in register B. She holds another register R in a state $\rho_R(\gamma) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \gamma^* |0\rangle\langle 1| + \gamma |1\rangle\langle 0|)$, where $\gamma \in \mathbb{C}$ and $|\gamma| \leqslant 1$. This γ determines how coherent the register is. Specifically, in the later part of this appendix we show that we can restrict γ to be real and $\gamma \in [0, 1]$. Hence at the beginning (time t_1) the total state of the entire system is:

$$\rho_{RB}(\gamma,\rho_B)=\rho_R(\gamma)\otimes\rho_B=\frac{1}{2}(|0\rangle\langle 0|_R+|1\rangle\langle 1|_R+\gamma^*|0\rangle\langle 1|_R+\gamma|1\rangle\langle 0|_R)\otimes\rho_B. \tag{A1}$$

The state $\rho_R(\gamma)$ determines the measurement basis in the following way: $|0\rangle$ corresponds to the measurement in the standard basis and $|1\rangle$ to the measurement in the Fourier basis (which is represented by applying the Fourier transformation to Bob's state and then measuring in the standard basis). Hence, the choice of the measurement basis can be represented by the controlled Fourier transform:

$$U=|0\rangle\langle 0|_R\otimes\mathbb{I}_B+|1\rangle\langle 1|_R\otimes F_B. \tag{A2}$$

We adopt the following convention for the Fourier transform: $F|j\rangle=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{jk}|k\rangle$ with $\omega=\exp\left(\frac{2\pi i}{d}\right)$ being the dth root of unity. After Alice applies the above unitary, the state at time t_2 is:

$$\rho'_{RB}(\gamma,d,\rho_B)=U\rho_{RB}(\gamma,\rho_B)U^\dagger=U(\rho_R(\gamma)\otimes\rho_B)U^\dagger \tag{A3}$$

$$=\frac{1}{2}(|0\rangle\langle 0|_R\otimes\rho_B+\gamma^*|0\rangle\langle 1|_R\otimes\rho_B F_B^\dagger+\gamma|1\rangle\langle 0|_R F_B\rho_B+|1\rangle\langle 1|_R\otimes F_B\rho_B F_B^\dagger). \tag{A4}$$

Then Alice performs her measurement and the outcome is stored in the output register X. The total state after the measurement at time t_3 is:

$$\rho_{RX}(\gamma,d,\rho_B)=\sum_x \mathrm{Tr}_B[(\mathbb{I}_R\otimes|x\rangle\langle x|_B)\rho'_{RB}(\gamma,d,\rho_B)]\otimes|x\rangle\langle x|_X. \tag{A5}$$

Hence, we see that the subnormalised post-measurement states of the basis register corresponding to Alice's measurement outcome x are:

$$\begin{aligned}\tilde{\rho}_R^x(\gamma,d,\rho_B)&=p_x(d,\rho_B)\rho_R^x(\gamma,d,\rho_B)=\mathrm{Tr}_B[(\mathbb{I}_R\otimes|x\rangle\langle x|_B)\rho'_{RB}]\\&=\frac{1}{2}\begin{pmatrix}\langle x|\rho_B|x\rangle & \gamma^*\langle x|\rho_B F^\dagger|x\rangle\\ \gamma\langle x|F\rho_B|x\rangle & \langle x|F\rho_B F^\dagger|x\rangle\end{pmatrix},\end{aligned} \tag{A6}$$

where $p_x(d,\rho_B)=\mathrm{Tr}[\tilde{\rho}_R^x(\gamma,d,\rho_B)]$ is the probability that Alice observes outcome $x\in\{0,1,\ldots,d-1\}$. Note that p_x does not depend on γ, which only appears in the off-diagonal elements of $\tilde{\rho}_R^x$. These subnormalised $\tilde{\rho}_R^x$'s are the states to which Bob has access and so his ability to predict Alice's measurement outcome $|x\rangle$ is determined by how well he can distinguish the quantum states $\{\rho_R^x\}$ occurring with probabilities $\{p_x\}$.

A.2. Simplifying lemmas

In the second part of this appendix we prove two lemmas, which allow us to restrict the coherence parameter γ to real and positive numbers and the input state ρ_B to pure states.

Lemma 1. *In our problem, we can describe all the possible qualitatively different games just with $\gamma\in[0,1]$. That is, all games corresponding to $\gamma\in\mathbb{C}$, $|\gamma|\leqslant 1$ are equivalent to some game with $\gamma\in[0,1]$.*

Proof. Let $\gamma=|\gamma|\,e^{i\theta}$. Then:

$$\tilde{\rho}_R^x(\gamma,d,\rho_B)=\frac{1}{2}\begin{pmatrix}\langle x|\rho_B|x\rangle & |\gamma|\,e^{-i\theta}\langle x|\rho_B F^\dagger|x\rangle\\ |\gamma|\,e^{i\theta}\langle x|F\rho_B|x\rangle & \langle x|F\rho_B F^\dagger|x\rangle\end{pmatrix}. \tag{A7}$$

Let $V(\theta)$ denote the rotation matrix in the xy plane of the Bloch sphere by angle θ. That is:

$$V(\theta)=\begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}. \tag{A8}$$

Then it can be easily verified that:

$$\tilde{\rho}_R^x(\gamma,d,\rho_B)=V(\theta)\tilde{\rho}_R^x(|\gamma|,d,\rho_B)V^\dagger(\theta), \tag{A9}$$

where $|\gamma|\in[0,1]$. Hence all the output states $\tilde{\rho}_R^x(\gamma,d)$ up to a unitary rotation $V(\theta)$ are the same as the corresponding states $\tilde{\rho}_R^x(|\gamma|,d)$. Clearly, rotating all the output states of register R by a fixed angle θ does not affect their distinguishability. Hence, it is sufficient to consider real and positive $\gamma\in[0,1]$. □

The probability of successfully discriminating states $\rho_R^x(\gamma,d,\rho_B)$, optimised over all measurements is [29]:

$$p_{\mathrm{guess}}(\gamma,d,\rho_B)=\max_{\{M_x\}}\sum_{x=0}^{d-1}p_x(d,\rho_B)\mathrm{Tr}[M_x\rho_R^x(\gamma,d,\rho_B)]=\max_{\{M_x\}}\sum_{x=0}^{d-1}\mathrm{Tr}[M_x\tilde{\rho}_R^x(\gamma,d,\rho_B)], \tag{A10}$$

where $\{M_x\}$ is a POVM. Here, by p_{guess} we denote the guessing probability optimised over all POVM's but for a specific input state ρ_B, while later we will use $p_{\mathrm{guess}}^{\max}$ to denote the guessing probability p_{guess} optimised over all

inputs states of Bob. Both p_{guess} and $p^{\max}_{\text{guess}}$ are calculated for a specific game parameterised by $d \geqslant 2$ and for a specific $\gamma \in [0,\ 1]$. Hence, we have $p^{\max}_{\text{guess}}(\gamma,\ d) = \max_{\rho_B} p_{\text{guess}}(\gamma,\ d,\ \rho_B)$.

Lemma 2. *To achieve $p^{\max}_{\text{guess}}$ it is sufficient for Bob to consider pure input states.*

Proof. Firstly, let us consider the case when not only does Bob hold no quantum memory, but he also does not have any classical memory. Consider then a scenario in which Bob sends Alice a mixed state $\rho_B = \sum_i q_i\ |\phi_i\rangle\langle\phi_i|$, where he is given freedom to choose the probabilities $\{q_i\}$. Then using equation (12):

$$\begin{aligned}\tilde{\rho}^x_R(\gamma,\ d,\ \rho_B) &= \sum_i q_i \frac{1}{2}\begin{pmatrix} |\langle x|\phi_i\rangle|^2 & \gamma\langle x|\phi_i\rangle\langle\phi_i|F^\dagger|x\rangle \\ \gamma\langle\phi_i|x\rangle\langle x|F|\phi_i\rangle & |\langle x|F|\phi_i\rangle|^2\end{pmatrix} \\ &= \sum_i q_i \tilde{\rho}^x_{R,i}(\gamma,\ d,\ |\phi_i\rangle),\end{aligned} \tag{A11}$$

where $\tilde{\rho}^x_R(\gamma,\ d,\ |\phi_i\rangle)$ denotes a post-measurement register state $\tilde{\rho}^x_R(\gamma,\ d,\ \rho_B)$ corresponding to Bob inputting a pure state $\rho_B = |\phi_i\rangle\langle\phi_i|$. In this case the guessing probability from equation (A10) becomes:

$$\begin{aligned}p_{\text{guess}}(\gamma,\ d,\ \rho_B) &= \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}\left[M_x \sum_i q_i \tilde{\rho}^x_R(\gamma,\ d,\ |\phi_i\rangle)\right] \leqslant \sum_i q_i \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}[M_x \tilde{\rho}^x_R(\gamma,\ d,\ |\phi_i\rangle)] \\ &= \sum_i q_i\ p_{\text{guess}}(\gamma,\ d,\ |\phi_i\rangle) \leqslant \max_i p_{\text{guess}}(\gamma,\ d,\ |\phi_i\rangle) = p_{\text{guess}}(\gamma,\ d,\ |\phi_m\rangle),\end{aligned} \tag{A12}$$

where $p_{\text{guess}}(\gamma,\ d,\ |\phi_i\rangle) = \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}[M_x \tilde{\rho}^x_R(\gamma,\ d,\ |\phi_i\rangle)]$ and by index m we denote the largest of all $p_{\text{guess}}(\gamma,\ d,\ |\phi_i\rangle)$ over all i's. Hence it is optimal for Bob to prepare a state $\rho_B = \sum_i q_i\ |\phi_i\rangle\langle\phi_i| = |\phi_m\rangle\langle\phi_m|$ (so that $q_i = \delta_{i,m}$), such that $|\phi_m\rangle \in \{|\phi_i\rangle\}$ and $p_{\text{guess}}(\gamma,\ d,\ |\phi_m\rangle) = \max_i p_{\text{guess}}(\gamma,\ d,\ |\phi_i\rangle)$.

Now, if we allow Bob to have classical memory, he could then prepare a mixed state ρ_B which is classically correlated to this memory. Then for each of the states ρ^i_B, corresponding to the state of the classical memory $|i\rangle_M$, we need to solve a separate optimisation problem given by equation (A10). Hence, if Bob prepares a state:

$$\rho_{BM} = \sum_i s_i \rho^i_B \otimes |i\rangle\langle i|_M \tag{A13}$$

according to the probability distribution $\{s_i\}$, then the guessing probability will be a weighted average of the individual guessing probabilities corresponding to each of the states ρ^i_B, namely:

$$p_{\text{guess}}(\gamma,\ d,\ \rho_B) = \sum_i s_i p_{\text{guess}}(\gamma,\ d,\ \rho^i_B) \leqslant p_{\text{guess}}(\gamma,\ d,\ \rho^k_B), \tag{A14}$$

where ρ^k_B is the input state that gives the highest guessing probability out of all the states $\{\rho^i_B\}$. Hence, classical memory does not allow us to achieve guessing probability higher than individual ρ^k_B, for which (as we have just seen) the guessing probability is upper bounded by its value corresponding to the optimal pure state $|\phi_m\rangle$ in the decomposition $\rho^k_B = \sum_i q_i\ |\phi_i\rangle\langle\phi_i|$. □

Hence we will restrict our attention to scenarios in which Bob prepares a pure state $|\phi\rangle_B$. In this case the post-measurement states of the basis register are:

$$\tilde{\rho}^x_R(\gamma,\ d,\ |\phi\rangle_B) = \frac{1}{2}\begin{pmatrix} |\langle x|\phi\rangle|^2 & \gamma\langle x|\phi\rangle\langle\phi|F^\dagger|x\rangle \\ \gamma\langle x|F|\phi\rangle\langle\phi|x\rangle & |\langle x|F|\phi\rangle|^2\end{pmatrix}. \tag{A15}$$

Appendix B. Guessing probability for two-dimensional game ($d = 2$)

In this appendix we prove theorem 1. That is, we derive the analytical formula for the maximum guessing probability as a function of $\gamma \in [0,\ 1]$, for a game with two-dimensional Fourier transform (Hadamard transform) in our circuit and two possible outcomes. In this game the state ρ_B that Bob prepares is a qubit. The two possible outcomes for Alice are: 0 and 1. We firstly restate this theorem below.

Theorem 1. *The maximum guessing probability for a two-dimensional game ($d = 2$), optimised over all input states ρ_B is given by:*

$$p^{\max}_{\text{guess}}(\gamma,\ d = 2) = \frac{1}{2}\left(1 + \frac{\sqrt{2 + 2\gamma^2}}{2}\right). \tag{B1}$$

In particular, for $\gamma = 1$ one achieves perfect guessing, that is $p^{\max}_{\text{guess}}(\gamma = 1,\ d = 2) = 1$.

Proof. The guessing probability is determined by how well Bob can distinguish states $\tilde{\rho}_R^0$ and $\tilde{\rho}_R^1$ defined in equation (A15) (for convenience we will omit writing out explicitly the dependence on γ and d). The problem of distinguishing two states has been solved by Helstrom [16] and the guessing probability is:

$$p_{\text{guess}} = \frac{1}{2}(1 + \|G\|_1), \tag{B2}$$

where $G = \tilde{\rho}_R^0 - \tilde{\rho}_R^1 = p_0\rho_R^0 - p_1\rho_R^1$ and $\|\cdot\|_1$ denotes the trace-norm of the matrix. Firstly we note that for $d = 2$, $F = F^\dagger = H$. Secondly, since ρ_B is a qubit, it is convenient to use the Bloch sphere representation:

$$\rho_B = \frac{1}{2}\left(\mathbb{I} + \sum_i c_i\sigma_i\right), \tag{B3}$$

with $c_x^2 + c_y^2 + c_z^2 \leqslant 1$. Although we have already shown in appendix A that the optimal guessing probability $p_{\text{guess}}^{\max}$ will be achieved for a pure input state ρ_B, here we are interested in all the qubit states that achieve this maximum guessing probability (under the assumption of Bob having no classical memory; if Bob had access to some classical memory, then any mixture of such optimal states correlated with this memory would also be an optimal state). Hence, in this appendix we again assume ρ_B to be an arbitrary (possibly mixed) qubit state. Plugging the Bloch sphere representation of ρ_B into equation (12), we can first calculate $\tilde{\rho}_R^0$ and $\tilde{\rho}_R^1$ and then G:

$$G = \frac{1}{2}\begin{pmatrix} c_z & \frac{\gamma(1 - \mathrm{i}\cdot c_y)}{\sqrt{2}} \\ \frac{\gamma(1 + \mathrm{i}\cdot c_y)}{\sqrt{2}} & c_x \end{pmatrix}. \tag{B4}$$

The eigenvalues of G are:

$$\lambda = \frac{(c_x + c_z) \pm \sqrt{(c_x - c_z)^2 + \gamma^2(1 + c_y^2)}}{4}. \tag{B5}$$

Now, let us consider two cases:

(a) $\lambda_1 \cdot \lambda_2 \geqslant 0$.
Then $\|G\|_1^{\text{a}} = |\lambda_1| + |\lambda_2| = |c_x + c_z|/2$ (the superscript 'a' labels the case $\lambda_1 \cdot \lambda_2 \geqslant 0$). We are interested in the maximum possible value of $\|G\|_1^{\text{a}}$ for a given γ. Hence we want to maximise the expression $|c_x + c_z|$ subject to the constraint $c_x^2 + c_y^2 + c_z^2 \leqslant 1$. Clearly, this gives us $|c_x + c_z| \leqslant \sqrt{2}$. And so $\|G\|_1^{\text{a,max}} \leqslant \frac{\sqrt{2}}{2}$. In particular, this bound is tight for $c_y = 0$ and $c_x = c_z = \pm\frac{1}{\sqrt{2}}$ (those states clearly satisfy the condition $\lambda_1 \cdot \lambda_2 \geqslant 0$). Hence, $\|G\|_1^{\text{a,max}} = \frac{\sqrt{2}}{2}$.

(b) $\lambda_1 \cdot \lambda_2 < 0$.
Then:

$$\lambda_1 = \frac{(c_x + c_z) + \sqrt{(c_x - c_z)^2 + 2\gamma^2(1 + c_y^2)}}{4} > 0, \tag{B6}$$

$$\lambda_2 = \frac{(c_x + c_z) - \sqrt{(c_x - c_z)^2 + 2\gamma^2(1 + c_y^2)}}{4} < 0. \tag{B7}$$

Hence in this case:

$$\|G\|_1^{\text{b}} = \lambda_1 - \lambda_2 = \frac{\sqrt{(c_x - c_z)^2 + 2\gamma^2(1 + c_y^2)}}{2}. \tag{B8}$$

Now we need to optimise this expression subject to the constraint $c_x^2 + c_y^2 + c_z^2 \leqslant 1$. Let us use a substitution $a = \frac{c_x - c_z}{\sqrt{2}}$ $b = \frac{c_x + c_z}{\sqrt{2}}$. Then the constraint becomes: $a^2 + c_y^2 + b^2 \leqslant 1$ and the norm of G is:

$$\|G\|_1^{\text{b}} = \frac{\sqrt{2a^2 + 2\gamma^2(1 + c_y^2)}}{2}. \tag{B9}$$

Clearly, since the term c_y^2 is scaled by the positive factor $2\gamma^2 \leqslant 2$, while a^2 is scaled by a factor of exactly 2, optimising this expression corresponds to setting a^2 to its maximum possible value which is 1 (so that $c_x = -c_z = \pm\frac{1}{\sqrt{2}}$). Then $c_y = b = 0$ (one can easily verify that those values satisfy the condition of (b) $\lambda_1 \cdot \lambda_2 < 0$, for all $\gamma \in [0,\ 1]$). This gives:

$$\|G\|_1^{\mathrm{b,max}} = \frac{\sqrt{2+2\gamma^2}}{2}, \tag{B10}$$

Clearly $\|G\|_1^{\mathrm{b,max}} \geqslant \|G\|_1^{\mathrm{a,max}}$ for all $\gamma \in [0,\ 1]$ (the equality relation holds only for $\gamma = 0$). Hence:

$$\|G\|_1^{\mathrm{max}} = \frac{\sqrt{2+2\gamma^2}}{2}. \tag{B11}$$

Using $\|G\|_1^{\mathrm{max}}$, for every γ we can now calculate the maximum value of the guessing probability:

$$p_{\mathrm{guess}}^{\mathrm{max}}(\gamma,\ d=2) = \frac{1}{2}(1+\|G\|_1^{\mathrm{max}}) = \frac{1}{2}\left(1+\frac{\sqrt{2+2\gamma^2}}{2}\right). \tag{B12}$$

We see also that for a fully coherent register with $\gamma = 1$, we obtain $p_{\mathrm{guess}}^{\mathrm{max}} = 1$. □

In order to find the optimal states we need to consider 3 separate cases depending on the value of γ.

- $\gamma = 0$. In this case $\|G\|_1^{\mathrm{max}} = \frac{\sqrt{2}}{2}$. This value occurs for two classes of states. One of them satisfies $a^2 = 1$ and $b = c_y = 0$ which gives two solutions: $c_x = -c_z = \pm\frac{1}{\sqrt{2}}$. Hence we obtain two states: $(c_x,\ c_y,\ c_z) = \left(\frac{1}{\sqrt{2}},\ 0,\ -\frac{1}{\sqrt{2}}\right)$ and $(c_x,\ c_y,\ c_z) = \left(-\frac{1}{\sqrt{2}},\ 0,\ \frac{1}{\sqrt{2}}\right)$. The other class can be seen by noticing that $\|G\|_1^{\mathrm{max}} = \frac{\sqrt{2}}{2} = \|G\|_1^{\mathrm{a,max}}$ and so it can also be obtained from the case (a) for two states that achieve this value: $(c_x,\ c_y,\ c_z) = \left(\frac{1}{\sqrt{2}},\ 0,\ \frac{1}{\sqrt{2}}\right)$ and $(c_x,\ c_y,\ c_z) = \left(-\frac{1}{\sqrt{2}},\ 0,\ -\frac{1}{\sqrt{2}}\right)$.
- $\gamma \in (0,\ 1)$. Here we only have the class $a^2 = 1$ and $b = c_y = 0$, that is the states: $(c_x,\ c_y,\ c_z) = \left(\frac{1}{\sqrt{2}},\ 0,\ -\frac{1}{\sqrt{2}}\right)$ and $(c_x,\ c_y,\ c_z) = \left(-\frac{1}{\sqrt{2}},\ 0,\ \frac{1}{\sqrt{2}}\right)$.
- $\gamma = 1$. Now $\|G\|_1^{\mathrm{b}} = \frac{\sqrt{2a^2+2(1+c_y^2)}}{2}$, and so this expression subject to the Bloch sphere normalisation is maximised by the pure states satisfying $a^2 + c_y^2 = 1$ and $b = 0$. These are all pure states with $c_z = -c_x$ and $c_y = \pm\sqrt{1-2c_x^2}$. We can use angular parametrisation of those coefficients, in which case we can write this entire family of states as $(c_x,\ c_y,\ c_z) = (\sin(\theta),\ \pm\sqrt{\cos(2\theta)},\ -\sin(\theta))$ for all $\theta \in [-\frac{\pi}{4},\ \frac{\pi}{4}]$. Geometrically, these states correspond to all pure states on the Bloch sphere that lie in the plane perpendicular to the Hadamard rotation axis and Hadamard transformation rotates them by π rad to their orthogonal complement.

From equation (B12) we see that the lowest value of $p_{\mathrm{guess}}^{\mathrm{max}}$ occurs for $\gamma = 0$ and it is $p_{\mathrm{guess}}^{\mathrm{max}} = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)$. As the basis register state is becoming more pure by letting γ grow, the $p_{\mathrm{guess}}^{\mathrm{max}}$ grows, until $p_{\mathrm{guess}}^{\mathrm{max}} = 1$ for $\gamma = 1$. We can also rephrase the guessing probability in terms of the purity of the basis register:

$$\mathrm{Tr}[\rho_R^2] = \frac{1}{4}\mathrm{Tr}\left[\begin{pmatrix}1 & \gamma\\ \gamma & 1\end{pmatrix}\begin{pmatrix}1 & \gamma\\ \gamma & 1\end{pmatrix}\right] = \frac{1}{4}\mathrm{Tr}\left[\begin{pmatrix}1+\gamma^2 & 2\gamma\\ 2\gamma & 1+\gamma^2\end{pmatrix}\right] = \frac{1+\gamma^2}{2}. \tag{B13}$$

Hence:

$$p_{\mathrm{guess}}^{\mathrm{max}}(\gamma,\ d=2) = \frac{1}{2}(1+\sqrt{\mathrm{Tr}[\rho_R^2]}). \tag{B14}$$

Appendix C. Guessing probability for the *d*-dimensional game

We have already seen that in two dimensions utilising entanglement allows for guessing with probability equal to 1. In higher dimensions however, we show that this is not possible. This fact is expressed in theorem 2 in the main text. We restate and prove this theorem below.

Theorem 2. *For d-dimensional games with any $d > 2$ it is not possible to achieve perfect guessing, i.e.,*

$$p_{\mathrm{guess}}^{\mathrm{max}}(\gamma,\ d>2) < 1, \qquad \forall\,\gamma. \tag{C1}$$

Proof. We construct a proof by contradiction. Let us assume that there exists $d > 2$ and $\gamma \in [0,\ 1]$, such that $p_{\text{guess}}^{\max}(\gamma,\ d) = 1$. Since the states $\tilde{\rho}_R^x(\gamma,\ d,\ |\phi\rangle)$ are two-dimensional, it is only possible to perfectly distinguish at most 2 such states (if they are orthogonal). Hence, that means that to achieve $p_{\text{guess}}^{\max}(\gamma,\ d) = 1$ it is required that at least $d - 2$ output states ρ_R^x occur with probability zero. Hence, $\tilde{\rho}_R^x \neq 0$ for at most two values of x. Let us denote those two values of $x \in \{0,\ 1, \ldots, d-1\}$ for which it is possible that $\tilde{\rho}_R^x \neq 0$ by x_0 and x_1. We assume that those values are distinct so that $x_0 \neq x_1$. Specifically, let us assume that $\tilde{\rho}_R^{x_0} \neq 0$, while $\tilde{\rho}_R^{x_1}$ may or may not be equal to zero. Then let us define $\mathcal{P} = \{0,\ 1, \ldots, d-1\} \setminus \{x_0,\ x_1\}$. Therefore we require that $\tilde{\rho}_R^x = 0$ for all $x \in \mathcal{P}$. Thus we obtain the following two requirements:

(1) $\langle x|\phi\rangle = 0$ for all $x \in \mathcal{P}$,

(2) $\langle x|F|\phi\rangle = 0$ for all $x \in \mathcal{P}$.

The requirement (1) implies that the physical input state of Bob must be of the form:

$$|\phi\rangle = \alpha_0\ |x_0\rangle + \alpha_1\ |x_1\rangle, \tag{C2}$$

with

$$|\alpha_0|^2 + |\alpha_1|^2 = 1. \tag{C3}$$

In this framework, the scenario in which only $\tilde{\rho}_R^{x_0} \neq 0$ would require $\alpha_1 = 0$. Now, note that:

$$F^\dagger\ |j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{-jk}\ |k\rangle, \tag{C4}$$

where $\omega = \exp\left(\frac{2\pi \mathrm{i}}{d}\right)$ and so:

$$\langle\phi|\ F^\dagger\ |x\rangle = \frac{1}{\sqrt{d}}(\alpha_0^* \omega^{-xx_0} + \alpha_1^* \omega^{-xx_1}). \tag{C5}$$

Then (2) implies that:

$$\alpha_0^* + \alpha_1^* \omega^{x(x_0 - x_1)} = 0, \qquad \forall x \in \mathcal{P}. \tag{C6}$$

Equation (C6) together with equation (C3) require that α_0 and α_1 are of the form:

$$\alpha_0 = \frac{1}{\sqrt{2}} \mathrm{e}^{\mathrm{i}\theta_0}, \tag{C7}$$

$$\alpha_1 = \frac{1}{\sqrt{2}} \mathrm{e}^{\mathrm{i}\theta_1}. \tag{C8}$$

The above requirement shows that α_1 cannot be zero, which in turn means that the scenario in which only $\tilde{\rho}_R^{x_0} \neq 0$ is not possible. Plugging the above forms of α's into equation (C6) and using the fact that ω is the dth root of unity, we obtain the following requirement:

$$\theta_0 \equiv \theta_1 + \pi + 2\pi \left[\frac{x}{d}(x_1 - x_0)\right] (\mathrm{mod}\ 2\pi), \qquad \forall x \in \mathcal{P}. \tag{C9}$$

Note that for $d = 3$, this expression can be easily satisfied since in this case $|\mathcal{P}| = 1$, so e.g. $\theta_0 = \theta_1 + \pi + 2\pi \left[\frac{x_\mathcal{P}}{d}(x_1 - x_0)\right]$, where $x_\mathcal{P} \in \mathcal{P}$ satisfies equation (C9). Hence the case $d = 3$ needs to be analysed separately. For $d > 3$ this equation can be satisfied if and only if:

$$\frac{x_1 - x_0}{d} \in \mathbb{Z}, \tag{C10}$$

where $\mathbb{Z}$ denotes the set of integers. However, $x_0,\ x_1 \in \{0,\ d-1\}$ and $x_0 \neq x_1$. Therefore this equation cannot be satisfied. Hence, for $d > 3$, it is not possible to have $p_{\text{guess}}(\gamma,\ d) = 1$. Now, let us consider the case $d = 3$. Equation (C2) and equations (C7)–(C9) imply that

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|x_1\rangle - \omega^{x_\mathcal{P}(x_1 - x_0)}\ |x_0\rangle), \tag{C11}$$

where we fix the global phase by setting $\theta_1 = 0$. Since $x_\mathcal{P},\ x_0,\ x_1$ must be all different, there are 6 possible states $|\phi\rangle$ corresponding to the above expression. Let $|\psi_{kl}\rangle = \frac{1}{\sqrt{2}}(|l\rangle - \omega^{x_\mathcal{P}(l-k)}\ |k\rangle)$. Then note that for every value of $x_\mathcal{P}$, the state $|\phi\rangle = |\psi_{kl}\rangle$ with $x_0 = k$, $x_1 = l$ and the state $|\phi\rangle = |\psi_{lk}\rangle$ with $x_0 = l$, $x_1 = k$ up to the global phase correspond to exactly the same state, since:

$$|\psi_{kl}\rangle = \frac{1}{\sqrt{2}}(|l\rangle - \omega^{x_\mathcal{P}(l-k)}\ |k\rangle) = -\omega^{x_\mathcal{P}(l-k)} \frac{1}{\sqrt{2}}(-\omega^{x_\mathcal{P}(k-l)}\ |l\rangle + |k\rangle) = -\omega^{x_\mathcal{P}(l-k)}\ |\psi_{lk}\rangle. \tag{C12}$$

Hence, we need only to consider 3 separate cases:

- For $x_{\mathcal{P}} = 0$, $x_0 = 1$, $x_1 = 2$, that is when $\tilde{\rho}_R^0 = 0$, we have:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |1\rangle). \tag{C13}$$

Then:

$$F\,|\phi\rangle = \mathrm{i}\frac{1}{\sqrt{2}}(|2\rangle - |1\rangle) = \mathrm{i}\,|\phi\rangle. \tag{C14}$$

This means that if we define a matrix

$$\rho_c(\gamma) = \frac{1}{2}\begin{pmatrix} 1 & -\mathrm{i}\gamma \\ \mathrm{i}\gamma & 1 \end{pmatrix}, \tag{C15}$$

then $\tilde{\rho}_R^0 = 0$, $\tilde{\rho}_R^1 = |\langle 1|\phi\rangle|^2\rho_c(\gamma)$, $\tilde{\rho}_R^2 = |\langle 2|\phi\rangle|^2\rho_c(\gamma)$. Hence, $\tilde{\rho}_R^1 = \tilde{\rho}_R^2 = \frac{1}{2}\rho_c(\gamma)$ and so we see that $\tilde{\rho}_R^1$ and $\tilde{\rho}_R^2$ correspond to the same state $\rho_c(\gamma)$ occurring with probability 0.5. This means that guessing probability in this case is 0.5 for all $\gamma \in [0,\ 1]$.

- For $x_{\mathcal{P}} = 1$, $x_0 = 2$, $x_1 = 0$ with $\tilde{\rho}_R^1 = 0$ the input state is:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \omega^{-2}\,|2\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - \omega\,|2\rangle). \tag{C16}$$

Then:

$$F\,|\phi\rangle = \frac{1}{\sqrt{6}}(1-\omega)(|0\rangle - \omega^2\,|2\rangle). \tag{C17}$$

Hence,

$$\tilde{\rho}_R^0 = \frac{1}{4}\begin{pmatrix} 1 & \gamma\frac{1}{\sqrt{3}}(1-\omega^*) \\ \gamma\frac{1}{\sqrt{3}}(1-\omega) & 1 \end{pmatrix}, \tag{C18}$$

$$\tilde{\rho}_R^1 = 0, \tag{C19}$$

$$\tilde{\rho}_R^2 = \frac{1}{4}\begin{pmatrix} 1 & \gamma\frac{1}{\sqrt{3}}(1-\omega^*)\omega^* \\ \gamma\frac{1}{\sqrt{3}}(1-\omega)\omega & 1 \end{pmatrix}. \tag{C20}$$

One can now show that $\mathrm{Tr}[\tilde{\rho}_R^0\tilde{\rho}_R^2] \neq 0$ for all $\gamma \in [0,\ 1]$. Hence those states are not orthogonal and perfect guessing is not possible.

- For $x_{\mathcal{P}} = 2$, $x_0 = 0$, $x_1 = 1$, with $\tilde{\rho}_R^1 = 0$ the input state is:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|1\rangle - \omega^2\,|0\rangle). \tag{C21}$$

Then:

$$F\,|\phi\rangle = \frac{1}{\sqrt{6}}((1-\omega^2)|0\rangle + \sqrt{3}\mathrm{i}\,|1\rangle). \tag{C22}$$

Hence,

$$\tilde{\rho}_R^0 = \frac{1}{4}\begin{pmatrix} 1 & \gamma\frac{1}{\sqrt{3}}(1-\omega^*) \\ \gamma\frac{1}{\sqrt{3}}(1-\omega) & 1 \end{pmatrix}, \tag{C23}$$

$$\tilde{\rho}_R^1 = \frac{1}{2}\rho_c(\gamma), \tag{C24}$$

$$\tilde{\rho}_R^2 = 0. \tag{C25}$$

Again $\mathrm{Tr}[\tilde{\rho}_R^0\tilde{\rho}_R^1] \neq 0$ for all $\gamma \in [0,\ 1]$. Hence also in this case perfect guessing is not possible.

We have shown that perfect guessing in $d = 3$ case is not possible either. Therefore we conclude that for all $d > 2$ and for all $\gamma \in [0,\ 1]$, $p_{\mathrm{guess}}^{\max}(\gamma,\ d) < 1$. □

The case $\gamma = 0$ is a special case and can be solved analytically for all $d \geqslant 2$.

Proposition 1. *For $\gamma = 0$ the maximal guessing probability is:*

$$p_{\text{guess}}^{\max}(\gamma = 0,\, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right), \tag{C26}$$

and under assumption of Bob having no classical memory, it is achieved if and only if Bob's input state ρ_B belongs to the following family of pure states:

$$|\phi_{jl}\rangle = c\,(|j\rangle + \omega^{jl}F^{\dagger}\,|l\rangle), \tag{C27}$$

where $\omega = \exp\left(\frac{2\pi \mathrm{i}}{d}\right)$, $j,\, l \in \{0,\, 1, \ldots, d-1\}$ and $c = \sqrt{\frac{\sqrt{d}}{2\sqrt{d}+2}}$.

Proof. If one measures in the standard basis, the guessing probability for a fixed input state ρ_B is:

$$p_{\text{guess}}^{\text{standard}}(d,\, \rho_B) = \max_l \mathrm{Tr}[|l\rangle\langle l|\,\rho_B]. \tag{C28}$$

If one measures in the Fourier basis:

$$p_{\text{guess}}^{\text{Fourier}}(d,\, \rho_B) = \max_l \mathrm{Tr}[|l\rangle\langle l|\,F\rho_B F^{\dagger}] = \max_l \mathrm{Tr}[F^{\dagger}\,|l\rangle\langle l|\,F\rho_B]. \tag{C29}$$

Since each measurement occurs with probability 50% and in the classical game the register R only tells Bob which measurement basis was used, the guessing probability optimised over all input states of Bob is:

$$p_{\text{guess}}^{\max}(\gamma = 0,\, d) = \frac{1}{2}\max_{\rho_B}(p_{\text{guess}}^{\text{standard}}(d,\, \rho_B) + p_{\text{guess}}^{\text{Fourier}}(d,\, \rho_B)) = \frac{1}{2}\max_{\rho_B}\max_{j,l}\mathrm{Tr}[(|j\rangle\langle j| + F^{\dagger}\,|l\rangle\langle l|\,F)\rho_B] \tag{C30}$$

$$= \frac{1}{2}\max_{j,l}\,\|\,|j\rangle\langle j| + F^{\dagger}\,|l\rangle\langle l|\,F\,\|_{\infty}, \tag{C31}$$

where $\|\cdot\|_{\infty}$ denotes the infinity norm. The matrix whose infinity norm we need to find is a rank-2 matrix. Let $p_{\text{guess}} = \frac{1}{2}\,\|M\|_{\infty}$ and $M = |\alpha\rangle\langle\alpha| + |\beta\rangle\langle\beta|$ be a rank-2 matrix. The largest eigenvalue of such a matrix is $\|M\|_{\infty} = \lambda_{\max} = 1 + |\langle\alpha|\beta\rangle|$. In our case: $|\alpha\rangle = |j\rangle$ and $|\beta\rangle = F^{\dagger}\,|l\rangle$. This means that $\|M\|_{\infty} = 1 + \frac{1}{\sqrt{d}}$ and so:

$$p_{\text{guess}}^{\max}(\gamma = 0,\, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right). \tag{C32}$$

The eigenstate corresponding to this eigenvalue $\lambda_{\max}$ is:

$$|\phi_{jl}\rangle = c\,(|j\rangle + \omega^{jl}F^{\dagger}\,|l\rangle). \tag{C33}$$

Hence only the states of this form will give us the maximum guessing probability. □

We will now show that for a subclass of the states of this form Bob will be guessing always either j or l, for all $\gamma \in [0,\, 1]$ and all $d \geqslant 2$, since those 2 outcomes have much higher probabilities of occurrence $p_j(d,\, |\phi_{jl}\rangle)$ and $p_l(d,\, |\phi_{jl}\rangle)$ than all other outcomes (i.e. we will show that for input state $|\phi_{jl}\rangle = c\,(|j\rangle + \omega^{jl}F^{\dagger}\,|l\rangle)$ such that $j \neq l$ the optimal strategy aims at distinguishing only the two states $\tilde{\rho}_R^{j}(\gamma,\, d,\, |\phi_{jl}\rangle)$ and $\tilde{\rho}_R^{l}(\gamma,\, d,\, |\phi_{jl}\rangle)$).

Lemma 3. *For all $d \geqslant 2$, for all $\gamma \in [0,\, 1]$ and for all states $|\phi_{jl}\rangle = c\,(|j\rangle + \omega^{jl}F^{\dagger}\,|l\rangle)$, such that $j,\, l \in \{0,\, 1, \ldots, d-1\}$ and $j \neq l$, the optimal guessing probability can be achieved by Bob if his measurement on the state of register R is a POVM with only two occurring outcomes, that is the matrix elements of this POVM are: $M_j \neq 0$, $M_l \neq 0$, $M_k = 0$, for all $k \in \mathcal{P}$, where $\mathcal{P} = \{0,\, 1, \ldots, d-1\} \setminus \{j,\, l\}$.*

Proof. The case $d = 2$ is trivial, since then there are only two output states.

Now considering the general case, let $\lambda_{\min}(\gamma,\, d,\, |\phi_{jl}\rangle)$ denote the guessing probability corresponding to this restricted POVM. The 'min' subscript indicates that this guessing probability is a lower bound on $p_{\text{guess}}(\gamma,\, d,\, |\phi_{jl}\rangle)$, the guessing probability optimised over all POVMs. That is: $\lambda_{\min}(\gamma,\, d,\, |\phi_{jl}\rangle) \leqslant p_{\text{guess}}(\gamma,\, d,\, |\phi_{jl}\rangle)$. We then have:

$$\lambda_{\min}(\gamma,\, d,\, |\phi_{jl}\rangle) = \max_{M_j, M_l}\mathrm{Tr}[M_j\tilde{\rho}_R^{j}(\gamma,\, d,\, |\phi_{jl}\rangle)] + \mathrm{Tr}[M_l\tilde{\rho}_R^{l}(\gamma,\, d,\, |\phi_{jl}\rangle)], \tag{C34}$$

Effectively this is again the problem of distinguishing 2 states solved by Helstrom [16], the only difference is that this time $p_j(d,\, |\phi_{jl}\rangle) + p_l(d,\, |\phi_{jl}\rangle) \leqslant 1$. Hence

$$\lambda_{\min}(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}[\|G(\gamma, d, |\phi_{jl}\rangle)\|_1 + p_j(d, |\phi_{jl}\rangle) + p_l(d, |\phi_{jl}\rangle)], \tag{C35}$$

where $G(\gamma, d, |\phi_{jl}\rangle) = \tilde{\rho}_R^j(\gamma, d, |\phi_{jl}\rangle) - \tilde{\rho}_R^l(\gamma, d, |\phi_{jl}\rangle)$. Now we will show that this bound is tight, i.e. we will show that the above $\lambda_{\min}(\gamma, d, |\phi_{jl}\rangle)$ is in fact also an upper bound on $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle)$. For this purpose let us consider the dual programme [29] in which we consider all matrices

$$\begin{aligned} &Q(\gamma, d, |\phi_{jl}\rangle) \in \mathcal{Z}, \text{ where } \mathcal{Z} = \{Q \in \mathbb{C}^{2\times 2} : Q = Q^\dagger \wedge \forall k \in \{0, 1, \ldots, d-1\}, \\ &Q(\gamma, d, |\phi_{jl}\rangle) \geqslant \tilde{\rho}_R^k(\gamma, d, |\phi_{jl}\rangle)\}. \end{aligned} \tag{C36}$$

Then for each $Q \in \mathcal{Z}$ we define $\lambda_{\max}^Q(\gamma, d, |\phi_{jl}\rangle) = \text{Tr}[Q(\gamma, d, |\phi_{jl}\rangle)]$. From this it follows that $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle) \leqslant \lambda_{\max}^Q(\gamma, d, |\phi_{jl}\rangle)$ for all $Q \in \mathcal{Z}$ [29] and so $\lambda_{\max}^Q(\gamma, d, |\phi_{jl}\rangle)$ is an upper bound on $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle)$. For simplicity, we will now omit writing explicitly the dependence on γ, d and $|\phi\rangle$. Consider a hermitian matrix:

$$Q' = \frac{1}{2}(\tilde{\rho}_R^j + \tilde{\rho}_R^l + |G|). \tag{C37}$$

Then:

$$\text{Tr}[Q'] = \frac{1}{2}(p_j + p_l + \|G\|_1) = \lambda_{\min}. \tag{C38}$$

Now, if Q' satisfies $Q' \geqslant \tilde{\rho}_R^k$, $\forall k$, then $Q' \in \mathcal{Z}$ and so $\text{Tr}[Q'] = \lambda_{\max}^{Q'}$. And since then $\text{Tr}[Q'] = \lambda_{\min} = \lambda_{\max}^{Q'}$, this means that $\text{Tr}[Q'] = p_{\text{guess}}$. Hence, we will now prove that $\forall\, d \geqslant 3$, $\gamma \in [0, 1]$ we have $Q' \in \mathcal{Z}$.

Consider

$$Q' - \tilde{\rho}_R^j = \frac{1}{2}(-\tilde{\rho}_R^j + \tilde{\rho}_R^l + |G|) = \frac{1}{2}(-G + |G|). \tag{C39}$$

Note that $|G| \geqslant G$ and so $Q' - \tilde{\rho}_R^j \geqslant 0$. Hence $Q' \geqslant \tilde{\rho}_R^j$. Analogously

$$Q' - \tilde{\rho}_R^l = \frac{1}{2}(\tilde{\rho}_R^j - \tilde{\rho}_R^l + |G|) = \frac{1}{2}(G + |G|). \tag{C40}$$

Clearly: $|G| \geqslant -G$ and so $Q' - \tilde{\rho}_R^l \geqslant 0$. Hence $Q' \geqslant \tilde{\rho}_R^l$.

Now we need to prove that $Q' \geqslant \tilde{\rho}_R^k$, $\forall k \in \mathcal{P}$ and for all $\gamma \in [0, 1]$, $d \geqslant 3$. In order to do that, we need to explicitly calculate all the output states of the register R. Those states are:

$$\tilde{\rho}_R^j(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}\begin{pmatrix} A^2 & \gamma AB\omega^{-j^2} \\ \gamma AB\omega^{j^2} & B^2 \end{pmatrix}, \tag{C41}$$

$$\tilde{\rho}_R^l(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}\begin{pmatrix} B^2 & \gamma AB\omega^{-l^2} \\ \gamma AB\omega^{l^2} & A^2 \end{pmatrix}, \tag{C42}$$

$$\tilde{\rho}_R^k(\gamma, d, |\phi_{jl}\rangle) = \frac{B^2}{2}\begin{pmatrix} 1 & \gamma\omega^{jl-jk-kl} \\ \gamma\omega^{jk+kl-jl} & 1 \end{pmatrix}, \tag{C43}$$

where $A = c\left(1 + \frac{1}{\sqrt{d}}\right)$, $B = \frac{c}{\sqrt{d}}$, $k \in \mathcal{P}$. Then $Q' - \tilde{\rho}_R^k = \frac{1}{2}(\tilde{\rho}_R^j + \tilde{\rho}_R^l - 2\tilde{\rho}_R^k + |G|)$. Consider the operator:

$$D = \tilde{\rho}_R^j + \tilde{\rho}_R^l - 2\tilde{\rho}_R^k = \frac{1}{2}\begin{pmatrix} A^2 - B^2 & \gamma B(A\omega^{-j^2} + A\omega^{-l^2} - 2B\omega^{jl-jk-kl}) \\ \gamma B(A\omega^{j^2} + A\omega^{l^2} - 2B\omega^{jk+kl-jl}) & A^2 - B^2 \end{pmatrix}. \tag{C44}$$

We will now show that for all $k \in \mathcal{P}$ we have $D \geqslant 0$. Note that for 2×2 matrices, $D \geqslant 0$ if and only if $\text{Tr}[D] \geqslant 0$ and $\text{Det}(D) \geqslant 0$. Firstly, we see that $\text{Tr}[D] = A^2 - B^2 \geqslant 0$, $\forall\, d \geqslant 3$. Secondly, the determinant of D is:

$$\begin{aligned} \text{Det}(D) = \frac{1}{4}\Bigg[&(A^2 - B^2)^2 - \gamma^2 B^2\Bigg(2A^2 + 4B^2 + 2A^2\cos\left(\frac{2\pi(j^2 - l^2)}{d}\right) \\ &- 4AB\cos\left(\frac{2\pi(j^2 - jk - kl + jl)}{d}\right) - 4AB\cos\left(\frac{2\pi(l^2 - jk - kl + jl)}{d}\right)\Bigg)\Bigg]. \end{aligned} \tag{C45}$$

Now we want to show that $\text{Det}(D) \geqslant 0$ for all $j, l \in \{0, 1, \ldots, d-1\}$, $k \in \mathcal{P}$, $\gamma \in [0, 1]$, $d \geqslant 3$. From the above expression we see that $\text{Det}(D)$ is monotonic in $\gamma \in [0, 1]$. Clearly for $\gamma = 0$, $\text{Det}(D) = \frac{1}{4}(A^2 - B^2)^2 \geqslant 0$. For $\gamma = 1$, we have:

$$\mathrm{Det}(D) = \frac{1}{4}\Bigg[A^4 - 3B^4 - 4A^2B^2 - 2A^2B^2\cos\left(\frac{2\pi(j^2-l^2)}{d}\right) + 4AB^3\cos\left(\frac{2\pi(j^2-jk-kl+jl)}{d}\right) + 4AB^3\cos\left(\frac{2\pi(l^2-jk-kl+jl)}{d}\right)\Bigg]. \tag{C46}$$

Note that $A = B(1+\sqrt{d})$. Thus we see that:

$$\begin{aligned}\mathrm{Det}(D) &= \frac{B^4}{4}\Bigg[(1+\sqrt{d})^4 - 3 - 4(1+\sqrt{d})^2 - 2(1+\sqrt{d})^2\cos\left(\frac{2\pi(j^2-l^2)}{d}\right) \\ &\quad + 4(1+\sqrt{d})\cos\left(\frac{2\pi(j^2-jk-kl+jl)}{d}\right) + 4(1+\sqrt{d})\cos\left(\frac{2\pi(l^2-jk-kl+jl)}{d}\right)\Bigg] \\ &\geqslant \frac{B^4}{4}[(1+\sqrt{d})^4 - 3 - 4(1+\sqrt{d})^2 - 2(1+\sqrt{d})^2 - 4(1+\sqrt{d}) - 4(1+\sqrt{d})] \\ &= \frac{B^4}{4}(d^2 + 4d\sqrt{d} - 16\sqrt{d} - 16).\end{aligned} \tag{C47}$$

Let

$$y(d) = (d^2 + 4d\sqrt{d} - 16\sqrt{d} - 16), \tag{C48}$$

then $\mathrm{Det}(D) \geqslant \frac{B(d)^4}{4}y(d)$. Clearly $B(d) \geqslant 0$, $\forall\, d \geqslant 3$ and $y(d) \geqslant 0$, $\forall\, d \geqslant 4$. Hence $\mathrm{Det}(D) \geqslant 0$, $\forall\, d \geqslant 4$. For $d = 3$ we use the exact expression from the first part of equation (C47) and we find that for all the cases $j \neq l$, $\forall\, k \in \mathcal{P}$, $\mathrm{Det}(D) \geqslant 0$. Hence $\mathrm{Det}(D) \geqslant 0$, $\forall\, d \geqslant 3$. Since both $\mathrm{Det}(D) \geqslant 0$ and $\mathrm{Tr}[D] \geqslant 0$, $D \geqslant 0$ and so $Q' \geqslant \tilde{\rho}_R^k$, $\forall\, k \in \{0, 1, \ldots, d-1\}$ and for all $\gamma \in [0, 1]$, $d \geqslant 3$. Therefore $Q' \in \mathcal{Z}$ and

$$\mathrm{Tr}[Q'] = \lambda^{\mathrm{Q}}_{\max}(\gamma, d, |\phi_{jl}\rangle) = \lambda_{\min}(\gamma, d, |\phi_{jl}\rangle) = p_{\mathrm{guess}}(\gamma, d, |\phi_{jl}\rangle). \tag{C49}$$

□

Now, knowing that the strategy of distinguishing only the two most probable outcomes for the input state $|\phi_{jl}\rangle = c(|j\rangle + \omega^{jl}F^\dagger|l\rangle)$, such that $j \neq l$ is actually an optimal strategy for those states, we can calculate the guessing probability for these states for all $d \geqslant 2$ and for all $\gamma \in [0, 1]$:

$$\begin{aligned}p_{\mathrm{guess}}(\gamma, d, |\phi_{jl}\rangle) &= \frac{1}{2}(p_j + p_l + \|G\|_1) \\ &= \frac{1}{4(d+\sqrt{d})}\left(2 + 2\sqrt{d} + d + \sqrt{d(2+\sqrt{d})^2 + 2\gamma^2(1+\sqrt{d})^2\left(1 - \cos\left(\frac{2\pi(j^2-l^2)}{d}\right)\right)}\right).\end{aligned} \tag{C50}$$

Clearly for $\gamma = 0$ the above expression reduces to equation (C32). That is $p_{\mathrm{guess}}(\gamma = 0, d, |\phi_{jl}\rangle) = p^{\max}_{\mathrm{guess}}(\gamma = 0, d)$, since the states for which we have evaluated $p_{\mathrm{guess}}(\gamma, d)$ above are the optimal states for $\gamma = 0$. Note that $A^2 = p^{\max}_{\mathrm{guess}}(\gamma = 0, d)$ and so it is easy to see that for $\gamma = 0$ the optimal measurement is:

$$M_j = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \qquad M_l = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, \qquad M_k = 0, \qquad \forall\, k \in \mathcal{P}. \tag{C51}$$

We can also see that for the game with $d = 2$, the two cases $j = 0$, $l = 1$ and $j = 1$, $l = 0$ correspond to the two optimal states for all $\gamma \in [0, 1]$. Hence, for these cases the above equation reduces to equation (B12).

Lemma 4. *There exist states for which* $p_{\mathrm{guess}}(\gamma_1, d, |\phi\rangle) > p_{\mathrm{guess}}(\gamma_2, d, |\phi\rangle) > p^{\max}_{\mathrm{guess}}(\gamma = 0, d)$, *for* $\gamma_1 > \gamma_2 > 0$, $\forall\, d \geqslant 2$.

Proof. Consider all input states of the form $|\phi_{jl}\rangle = c(|j\rangle + \omega^{jl}F^\dagger|l\rangle)$ such that $\frac{j^2-l^2}{d} \notin \mathbb{Z}$ and $\forall\, d \geqslant 2$. Then firstly, $j \neq l$ and so the guessing probability corresponding to those states is given by equation (C50) and secondly the coefficient in front of γ^2 is positive. Hence in these cases $p_{\mathrm{guess}}(\gamma, d, |\phi_{jl}\rangle)$ is monotonically increasing in $\gamma \in [0, 1]$, $\forall\, d \geqslant 2$. Hence, $\forall\, d \geqslant 2$, for all input states $|\phi_{jl}\rangle = c(|j\rangle + \omega^{jl}F^\dagger|l\rangle)$ such that $\frac{j^2-l^2}{d} \notin \mathbb{Z}$ we have $p_{\mathrm{guess}}(\gamma_1, d, |\phi_{jl}\rangle) > p_{\mathrm{guess}}(\gamma_2, d, |\phi_{jl}\rangle) > p^{\max}_{\mathrm{guess}}(\gamma = 0, d)$, for $\gamma_1 > \gamma_2 > 0$. □

Theorem 3 follows directly from the above lemma by noting that $p^{\max}_{\mathrm{guess}}(\gamma, d) \geqslant p_{\mathrm{guess}}(\gamma, d, |\phi\rangle)$, for all $\gamma \in [0, 1]$, $d \geqslant 2$ and for all states $|\phi\rangle$.

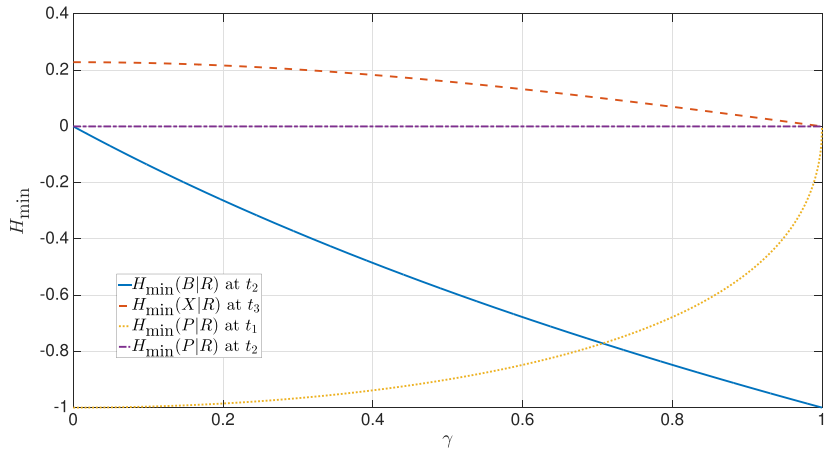

Figure C1. Conditional min-entropies as a function of γ for the two-dimensional game ($d = 2$) with Bob's input state $|\phi_{01}\rangle = c(|0\rangle + |-\rangle)$ or $|\phi_{10}\rangle = c(|1\rangle + |+\rangle)$. The blue solid line corresponds to the $H_{\min}(B|R)$ at time t_2 in figure 2. The red dashed line shows $H_{\min}(X|R)$ at time t_3 after Alice's measurement, where the state is averaged over all the outcomes, as Bob does not have access to the measurement result. The yellow dotted line corresponds to $H_{\min}(P|R)$ at time t_1 and hence shows the initial quantum correlations between R and its purification P. The correlations between those systems at time t_2 are illustrated by the purple dash-dotted flat line $H_{\min}(P|R) = 0$. By comparing the blue solid and red dashed lines, one can see that for $\gamma = 1$ the increase of the conditional entropy between $H_{\min}(B|R)$ and $H_{\min}(X|R)$ due to the measurement on B is the greatest possible, that is, it is equal to 1. The reason is that the measurement is the most destructive in this case, as it destroys all the quantum correlations of a maximally entangled state. On the other end of the spectrum, if $\gamma = 0$, there are no quantum correlations between B and R present and so the measurement has a relatively small influence on the system. It only affects the classical correlations, which are not aligned with the standard basis in which the measurement performed by Alice takes place (the final measurement in the circuit in figure 2). Hence, in this case the increase of conditional entropy is small. Comparing the yellow dotted and blue solid lines we see that decreasing the amount of entanglement between P and R results in the increase in the amount of entanglement between B and R that can be generated using the controlled Fourier transform. Finally, from the flat purple dash-dotted line we see that independently of the coherence of R and its initial correlations with P, the correlations between those two systems at time t_2 can be only classical. All the above entropies are derived in appendix E.

One can also see that for the input states $|\phi_{jl}\rangle = c(|j\rangle + \omega^{jl}F^{\dagger}|l\rangle)$ with $j \neq l$ but with $\frac{j^2 - l^2}{d} \in \mathbb{Z}$, equation (C50) reduces to $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right) = p^{\max}_{\text{guess}}(\gamma = 0, d)$. That is for those states $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle)$ stays constant in γ for all d.

Appendix D. Coherence and quantum correlations

To give a deeper insight into the relation between the guessing probability and the coherence γ, we also look at the correlations between the registers B, R and P (the initial purification of R), at times t_1, t_2 and t_3 in figure 2 (in the main article). Specifically, we focus on the two-dimensional game with optimal input states. We then quantify the arising correlations using min-entropy and the results are depicted in figure C1. It needs to be noted that independently of the dimension of our game, Bob's requirements for perfect guessing are perfect classical correlations between R and X, the classical register denoting the measurement outcome after Alice has performed her measurement on the system B at time t_3 in figure 2. However, classical correlations are basis dependent and effectively the measurement of Alice involves two mutually unbiased bases. Hence it is impossible to have perfect guessing with just classically correlating the two systems before the measurement. From the perspective of the quantum circuit in figure 2, those perfect classical correlations that arise after the conditional Fourier transform will never be perfectly aligned with the measurement basis of Alice (standard basis). As a result, even if the system is classically perfectly correlated before the measurement, the correlations are no longer maximal after the measurement on B. For two-dimensional game, this can be seen in figure C1 where for $\gamma = 0$, $H_{\min}(B|R) = 0$, but $H_{\min}(X|R) > 0$. The advantage for Bob coming from the quantum coherence in register R and the resulting quantum correlations is that for maximal entanglement (which is possible if $d = 2$), independently of the basis in which the system B has been measured, the outcomes of that measurement are maximally correlated with the state of the register R. Hence, if the two systems become maximally entangled ($H_{\min}(B|R) = -1$ for $\gamma = 1$), then the post-measurement state becomes classically maximally correlated ($H_{\min}(X|R) = 0$) enabling perfect guessing.

Appendix E. Conditional min-entropies for the two-dimensional game

The controlled Fourier transform in the circuit in figure 2 (in the main article) results in (quantum) correlations between the two systems B and R. These correlations are exploited by Bob in order to guess the measurement outcome on the state ρ_B. However, this measurement has a destructive effect on these correlations. Here we quantify this destructive effect of the measurement using min-entropy. The conditional min-entropy will be calculated using the definition presented in [20]. Firstly let us define a correlation measure:

$$q_{\text{corr}}(B|R) = d \max_{\mathcal{E}} F((\mathcal{E}_R \otimes \mathbb{1}_B)(\rho_{RB}), |\Psi\rangle\langle\Psi|_{RB})^2, \tag{E1}$$

where F is fidelity defined using the trace norm as $F(\rho, \sigma) = ||\sqrt{\rho}\sqrt{\sigma}||_1$ (when one of the states is pure, that is when $\sigma = |\Psi\rangle\langle\Psi|$, the fidelity reduces to $F(\rho, \sigma) = \sqrt{\langle\Psi|\ \rho\ |\Psi\rangle}$), d is the dimension of subsystem B, $\mathcal{E}$ is a local operation described by a trace-preserving completely positive map and $|\Psi\rangle$ is a maximally entangled state (note that $q_{\text{corr}}(B|R)$ is independent of which maximally entangled state we use, since all such states are the same up to a unitary rotation on one of the qudits; this rotation can always be compensated on ρ_{RB} by the corresponding rotation on system R as part of the local operation $\mathcal{E}$). Then one can calculate the conditional min-entropy of a quantum–quantum (qq) state as $H_{\min}(B|R) = -\log(q_{\text{corr}}(B|R))$. Note that for classical–quantum (cq) states, $q_{\text{corr}}(X|R)$ becomes the guessing probability $p_{\text{guess}}(X|R)$ (here X denotes the classical subsystem) [20].

We are interested in the relation between the min-entropy $H_{\min}(B|R)$ of a qq-state (the min-entropy of the input state ρ_B before Alice's measurement, given access to R) and the min-entropy $H_{\min}(X|R)$ of the cq-state after the measurement has been performed (the min-entropy of the classical outcome X after Alice's measurement, given access to ρ_R). For that purpose we will investigate the tightness of the inequality derived in [4]:

$$H_{\min}(X|R) \leqslant H_{\min}(B|R) + \log(d), \tag{E2}$$

where d is the dimension of the outcome space. This inequality tells us that for two-dimensional states, the increase of the conditional min-entropy due to the measurement cannot exceed 1.

For $d = 2$ we will now calculate both of those entropies explicitly starting with $H_{\min}(B|R)$. In our calculation let us pick one of the two states which give us the maximum guessing probability for all values of γ, namely $|\phi_{10}\rangle$ which in the Bloch sphere representation can be expressed as $(c_x, c_y, c_z) = \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right)$ [one can analogously show that the other state $|\phi_{01}\rangle$ or equivalently $(c_x, c_y, c_z) = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ will give exactly the same $H_{\min}(B|R)$]. For this input state, the overall state $\rho'_{RB}(\gamma, d = 2, |\phi\rangle)$ before the measurement at time t_2 in figure 2 is:

$$\begin{aligned}\rho'_{RB}(\gamma, d = 2, |\phi\rangle) = \frac{1}{4}\Bigg(|0\rangle\langle 0|_R \otimes \left(\mathbb{I} + \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z)\right) + \gamma\Bigg[|0\rangle\langle 1|_R \otimes \left(H_B + \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z)H_B\right) \\ + |1\rangle\langle 0|_R \otimes \left(H_B + \frac{1}{\sqrt{2}}H_B(\sigma_x - \sigma_z)\right)\Bigg] + |1\rangle\langle 1|_R \otimes \left(\mathbb{I} + \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)\right)\Bigg).\end{aligned} \tag{E3}$$

We can now diagonalise this state so that we obtain:

$$\rho'_{RB}(\gamma, d = 2, |\phi\rangle) = \frac{1+\gamma}{2}\ |\psi_1\rangle\langle\psi_1| + \frac{1-\gamma}{2}\ |\psi_2\rangle\langle\psi_2|, \tag{E4}$$

where the eigenstates written in their Schmidt bases are:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0'\rangle_R\ |1\rangle_B + |1'\rangle_R\ |0\rangle_B), \tag{E5}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0''\rangle_R\ |1\rangle_B + |1''\rangle_R\ |0\rangle_B). \tag{E6}$$

The Schmidt bases: $\{|0'\rangle, |1'\rangle\}$ and $\{|0''\rangle, |1''\rangle\}$ are given by:

$$|0'\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2-\sqrt{2}}}\ |0\rangle - \frac{1}{\sqrt{2+\sqrt{2}}}\ |1\rangle\right), \tag{E7}$$

$$|1'\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2+\sqrt{2}}}\ |0\rangle + \frac{1}{\sqrt{2-\sqrt{2}}}\ |1\rangle\right), \tag{E8}$$

$$|0''\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2-\sqrt{2}}}\,|0\rangle + \frac{1}{\sqrt{2+\sqrt{2}}}\,|1\rangle\right), \tag{E9}$$

$$|1''\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2+\sqrt{2}}}\,|0\rangle - \frac{1}{\sqrt{2-\sqrt{2}}}\,|1\rangle\right). \tag{E10}$$

The states $|\psi_1\rangle$ and $|\psi_2\rangle$ are mutually orthogonal maximally entangled states. To calculate $H_{\min}(B|R)$ we use the formulation of the min-entropy in terms of the semi-definite programmes, as expressed in [20]. The primal, as stated before, is $H_{\min}(B|R) = -\log(q_{\text{corr}}(B|R))$ where $q_{\text{corr}}(B|R)$ is given in equation (E1). The dual problem is:

$$H_{\min}(B|R) = -\log \min_{\substack{\sigma_R \geqslant 0 \\ \sigma_R \otimes \mathbb{I}_B \geqslant \rho_{RB}}} \text{Tr}(\sigma_R). \tag{E11}$$

For the primal programme, let us consider a local transformation $\mathcal{E}$ acting on subsystem R which performs a rotation such that the state will now be diagonal in the basis that includes $|\Psi\rangle_{RB}$, with maximal probability in this mixture corresponding to the state $|\Psi\rangle_{RB}$. This feasible solution gives:

$$\max_{\mathcal{E}} F((\mathcal{E} \otimes \mathbb{1}_B)(\rho'_{RB}), |\Psi\rangle\langle\Psi|_{RB}) \geqslant \sqrt{\frac{1+\gamma}{2}}. \tag{E12}$$

Hence:

$$q_{\text{corr}}(B|R) \geqslant 1 + \gamma, \tag{E13}$$

and so:

$$H_{\min}(B|R) = -\log q_{\text{corr}}(B|R) \leqslant -\log(1+\gamma). \tag{E14}$$

Similarly, for the dual programme, let us consider a matrix $\sigma_R = \left(\frac{1+\gamma}{2}\right)\mathbb{I}_R \geqslant 0$. Then $\sigma_R \otimes \mathbb{I}_B = \left(\frac{1+\gamma}{2}\right)\mathbb{I}_{4\times 4}$. Clearly $\sigma_R \otimes \mathbb{I}_B \geqslant \rho'_{RB}$, so that we obtain:

$$H_{\min}(B|R) \geqslant -\log\text{Tr}[\sigma_R] = -\log(1+\gamma). \tag{E15}$$

Combining the results from the primal and dual programmes allows us to conclude that $H_{\min}(B|R) = -\log(1+\gamma)$ for all $\gamma \in [0, 1]$.

The min-entropy after the measurement is related to the guessing probability as $H_{\min}(X|R) = -\log p_{\text{guess}}(X|R)$ and so it is:

$$H_{\min}(X|R) = -\log\left(\frac{1}{2}\left(\frac{\sqrt{2+2\gamma^2}}{2} + 1\right)\right) = 1 - \log\left(\frac{\sqrt{2+2\gamma^2}}{2} + 1\right). \tag{E16}$$

Hence:

$$H_{\min}(X|R) - H_{\min}(B|R) = 1 - \log\left(\frac{\sqrt{2+2\gamma^2}+2}{2(1+\gamma)}\right). \tag{E17}$$

We then see that $H_{\min}(X|R) - H_{\min}(B|R)$ monotonically increases with $\gamma \in [0, 1]$ until it reaches the value of one for $\gamma = 1$. Hence the inequality (E2) is tight for $\gamma = 1$ which corresponds to the greatest possible increase of the conditional min-entropy during the measurement performed on a qubit (see figure C1).

We also compute the min-entropy $H_{\min}(P|R)$ to get some insight into the correlations between basis register R and its purification P as a function of γ. For that purpose, let us redefine the way we label the states of registers R and P with respect to the labelling and notation used in equations (5) to (9). Specifically, let $|\alpha\rangle$, $|\beta\rangle$ be now the two states of the entire register P (joint states of all the environmental subsystems E_i that are in P) corresponding to the states $|0\rangle$, $|1\rangle$ of the register R respectively. The real parameter $\gamma \in [0, 1]$, that quantifies the amount of information that P holds about R, satisfies now:

$$\langle\alpha|\beta\rangle = \gamma, \tag{E18}$$

so that the joint state of registers R and P can be written as:

$$|\xi(\gamma)\rangle_{RP} = \frac{1}{\sqrt{2}}(|0\rangle_R\,|\alpha\rangle_P + |1\rangle_R\,|\beta\rangle_P). \tag{E19}$$

Note that the state $|\xi(\gamma)\rangle_{RP}$ defined in equation (E19) is pure. Then $H_{\min}(P|R) = -\log(\text{Tr}[\sqrt{\rho_R}])^2 = -\log(\text{Tr}[\sqrt{\rho_P}])^2$. Note that $\text{Tr}[\sqrt{\rho_R}] = \text{Tr}[\sqrt{\rho_P}]$ is the sum of the Schmidt coefficients of the state $|\xi(\gamma)\rangle_{RP}$. The eigenvalues of $\rho_R(\gamma)$ defined in equation (6) (with real and positive γ) are $\lambda_1 = \frac{1+\gamma}{2}$ and $\lambda_2 = \frac{1-\gamma}{2}$. Hence:

$$H_{\min}(P|R) = -\log\left(\sqrt{\frac{1+\gamma}{2}} + \sqrt{\frac{1-\gamma}{2}}\right)^2 = -\log(1+\sqrt{1-\gamma^2}). \tag{E20}$$

Similarly we calculate $H_{\min}(P|R)$ after the conditional Fourier transform in figure 2 has been applied, to quantify the effect of this operation on the correlations between R and P. Firstly we need to calculate ρ_{RP} at time t_2. That is, again following the circuit in figure 2 but now including the purification P, the initial state at time t_1 is $|\Phi(\gamma, d, |\phi\rangle)\rangle_{RPB} = |\xi(\gamma)\rangle_{RP} \otimes |\phi\rangle_B$. Then the state at time t_2 is $|\Phi'(\gamma, d, |\phi\rangle)\rangle_{RPB} = U\,|\Phi(\gamma, d, |\phi\rangle)\rangle_{RPB}$, where U is given by:

$$U = |0\rangle\langle 0|_R \otimes \mathbb{I}_P \otimes \mathbb{I}_B + |1\rangle\langle 1|_R \otimes \mathbb{I}_P \otimes F_B. \tag{E21}$$

Hence:

$$|\Phi'(\gamma, d, |\phi\rangle)\rangle_{RPB} = \frac{1}{\sqrt{2}}(|0\rangle_R\,|\alpha\rangle_P\,|\phi\rangle_B + |1\rangle_R\,|\beta\rangle_P F_B\,|\phi\rangle_B). \tag{E22}$$

We can now trace out B.

$$\begin{aligned}\rho'_{RP}(\gamma, d, |\phi\rangle) = \frac{1}{2}(&|0\rangle\langle 0|_R \otimes |\alpha\rangle\langle\alpha|_P + \langle\phi|\,F^\dagger\,|\phi\rangle\,|0\rangle\langle 1|_R \otimes |\alpha\rangle\langle\beta|_P \\ &+ \langle\phi|\,F\,|\phi\rangle\,|1\rangle\langle 0|_R \otimes |\beta\rangle\langle\alpha|_P + |1\rangle\langle 1|_R \otimes |\beta\rangle\langle\beta|_P).\end{aligned} \tag{E23}$$

Now let us consider the two-dimensional game again with $|\phi\rangle_B$ being one of the two states that achieve $p^{\max}_{\text{guess}}(\gamma, d=2)$ for all $\gamma \in [0, 1]$ (these are the states $|\phi\rangle = |\phi_{10}\rangle$ and $|\phi\rangle = |\phi_{01}\rangle$). Then $\langle\phi|\,F\,|\phi\rangle = 0$, so the state on R and P at t_2 is:

$$\rho_{RP}(\gamma, d=2, |\phi\rangle) = \frac{1}{2}(|0\rangle\langle 0|_R \otimes |\alpha\rangle\langle\alpha|_P + |1\rangle\langle 1|_R \otimes |\beta\rangle\langle\beta|_P). \tag{E24}$$

To calculate $H_{\min}(P|R)$ we again use the formulation of min-entropy in terms of the semi-definite programmes [20]. For the dual programme in equation (E11), note that ρ_{RP} has eigenvalues $\left\{\frac{1}{2}, \frac{1}{2}, 0, 0\right\}$. Hence $\sigma_R = \frac{\mathbb{I}_R}{2}$ clearly satisfies the constraints, as then $\sigma_R \otimes \mathbb{I}_P = \frac{\mathbb{I}_{4\times 4}}{2}$ and so $\sigma_R \geqslant 0$ and $\sigma_R \otimes \mathbb{I}_P \geqslant \rho_{RP}$. The corresponding solution is $H_{\min}(P|R) \geqslant 0$. Similarly, in equation (E1), let us consider $\mathcal{E}$ to be a quantum channel acting on R with Krauss operators $\{M_i\}$, where $M_0 = |\alpha\rangle\langle 0|$ and $M_0 = |\beta\rangle\langle 1|$. Then:

$$\rho'_{RP} = (\mathcal{E} \otimes \mathbb{1}_P)(\rho_{RP}) = \frac{1}{2}(|\alpha\rangle\langle\alpha|_R \otimes |\alpha\rangle\langle\alpha|_P + |\beta\rangle\langle\beta|_R \otimes |\beta\rangle\langle\beta|_P). \tag{E25}$$

Since $\langle\alpha|\beta\rangle = \gamma$, we have $\langle\alpha^\perp|\beta\rangle = e^{i\phi}\sqrt{1-\gamma^2}$ for some phase ϕ, where $\langle\alpha|\alpha^\perp\rangle = 0$. Now, let $|\Psi\rangle_{RP}$ be a maximally entangled state of the form $|\Psi\rangle_{RP} = \frac{1}{\sqrt{2}}(|\alpha\rangle_R\,|\alpha\rangle_P + e^{2i\phi}\,|\alpha^\perp\rangle_R\,|\alpha^\perp\rangle_P)$. Therefore:

$$\begin{aligned}q_{\text{corr}}(P|R) &= 2F(\rho'_{RP}, |\Psi\rangle\langle\Psi|_{RP})^2 \\ &= \frac{1}{2}(\langle\alpha|_R\langle\alpha|_P + e^{-2i\phi}\langle\alpha^\perp|_R\langle\alpha^\perp|_P)(|\alpha\rangle\langle\alpha|_R \otimes |\alpha\rangle\langle\alpha|_P \\ &\quad + |\beta\rangle\langle\beta|_R \otimes |\beta\rangle\langle\beta|_P)(|\alpha\rangle_R\,|\alpha\rangle_P + e^{2i\phi}\,|\alpha^\perp\rangle_R\,|\alpha^\perp\rangle_P) \\ &= \frac{1}{2}(1 + |\langle\alpha|\beta\rangle|^4 + |\langle\alpha^\perp|\beta\rangle|^4 + e^{2i\phi}(\langle\alpha|\beta\rangle)^2(\langle\beta|\alpha^\perp\rangle)^2 + e^{-2i\phi}(\langle\beta|\alpha\rangle)^2(\langle\alpha^\perp|\beta\rangle)^2) \\ &= \frac{1}{2}(1 + \gamma^4 + (1-\gamma^2)^2 + 2\gamma^2(1-\gamma^2)) \\ &= 1.\end{aligned} \tag{E26}$$

Hence the corresponding solution is $H_{\min}(P|R) \leqslant 0$. Therefore combining the results from the primal and dual programmes we conclude that $H_{\min}(P|R) = 0$ for all $\gamma \in [0, 1]$.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. on Computer System and Signal Processing* (Piscataway, NJ: IEEE)

[2] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 The uncertainty principle in the presence of quantum memory *Nat. Phys.* **6** 09

[3] Berta M, Coles P J and Wehner S 2014 Entanglement-assisted guessing of complementary measurement outcomes *Phys. Rev.* A **90** 062127

[4] Berta M, Fawzi O and Wehner S 2014 Quantum to classical randomness extractors *IEEE Trans. Inf. Theory* **60** 1168–92

[5] Céleri L C, Gomes R M, Ionicioiu R, Jennewein T, Mann R B and Terno D R 2014 Quantum control in foundational experiments *Found. Phys.* **44** 576

[6] Christandl M and Winter A 2005 Uncertainty, monogamy, and locking of quantum correlations *IEEE Trans. Inf. Theory* **51** 3159–65

[7] Coles P J, Berta M, Tomamichel M and Wehner S 2017 Entropic uncertainty relations and their applications *Rev. Mod. Phys.* **89** 015002

[8] Coles P J, Colbeck R, Yu L and Zwolak M 2012 Uncertainty relations from simple entropic properties *Phys. Rev. Lett.* **108** 210405

[9] Coles P J, Yu L, Gheorghiu V and Griffiths R B 2011 Information-theoretic treatment of tripartite systems and quantum channels *Phys. Rev.* A **83** 062338
[10] Curty M, Ma X, Lo H-K and Lütkenhaus N 2010 Passive sources for the Bennett–Brassard 1984 quantum-key-distribution protocol with practical signals *Phys. Rev.* A **82** 052325
[11] Dupuis F, Fawzi O and Wehner S 2015 Entanglement sampling and applications *IEEE Trans. Inf. Theory* **61** 1093–112
[12] Frank R L and Lieb E H 2013 Extended quantum conditional entropy and quantum uncertainty inequalities *Commun. Math. Phys.* **323** 487–95
[13] Furrer F, Berta M, Tomamichel M, Scholz V B and Christandl M 2014 Position-momentum uncertainty relations in the presence of quantum memory *J. Math. Phys.* **55** 122205
[14] Hall M J W 1995 Information exclusion principle for complementary observables *Phys. Rev. Lett.* **74** 3307–11
[15] Heisenberg W 1927 Über den anschaulichen Inhalt der quantentheoretischen Kinematik und mechanik *Z. Phys.* **43** 172
[16] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)
[17] Ionicioiu R and Terno D R 2011 Proposal for a quantum delayed-choice experiment *Phys. Rev. Lett.* **107** 230406
[18] Kaiser F, Coudreau T, Milman P, Ostrowsky D B and Tanzilli S 2012 Entanglement-enabled delayed-choice experiment *Science* **338** 637
[19] Kennard E H 1927 Zur Quantenmechanik einfacher Bewegungstypen *Z. Phys.* **44** 326
[20] Konig R, Renner R and Schaffner C 2009 The operational meaning of min- and max-entropy *IEEE Trans. Inf. Theory* **55** 4337–47
[21] Korzekwa K, Lostaglio M, Jennings D and Rudolph T 2014 Quantum and classical entropic uncertainty relations *Phys. Rev.* A **89** 042122
[22] Liu S, Mu L-Z and Fan H 2015 Entropic uncertainty relations for multiple measurements *Phys. Rev.* A **91** 042133
[23] Luo S L 2005 Quantum versus classical uncertainty *Theor. Math. Phys.* **143** 681–8
[24] Peruzzo A, Shadbolt P, Brunner N, Popescu S and O'Brien J L 2012 A quantum delayed-choice experiment *Science* **338** 634
[25] Renes J M and Boileau J-C 2009 Conjectured strong complementary information tradeoff *Phys. Rev. Lett.* **103** 020402
[26] Robertson H P 1929 The uncertainty principle *Phys. Rev.* **34** 163
[27] Sánchez-Ruiz J 1995 Improved bounds in the entropic uncertainty and certainty relations for complementary observables *Phys. Lett.* A **201** 125–31
[28] Tang J-S, Li Y-L, Li C-F and Guo G-C 2013 Revisiting Bohr's principle of complementarity with a quantum device *Phys. Rev.* A **88** 014103
[29] Watrous J 2011 https://cs.uwaterloo.ca/~watrous/CS766/LectureNotes/08.pdf
[30] Zurek W H 2003 Decoherence, einselection, and the quantum origins of the classical *Rev. Mod. Phys.* **75** 715