Choice of mutually unbiased bases and outcome labeling affecting measurement outcome secrecy

Mirdit Doda,[1,2] Matej Pivoluska,[1,3] and Martin Plesch[1,3]

[1] *Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia*
[2] *Institute for Quantum Optics and Quantum Information – Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*
[3] *Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic*

(Received 17 June 2020; accepted 17 February 2021; published 4 March 2021)

Mutually unbiased bases (MUBs) are a crucial ingredient for many protocols in quantum information processing. Measurements performed in these bases are unbiased to the maximally possible extent, which is used to prove the randomness or secrecy of measurement results. In this work we show that certain properties of sets of MUBs crucially depend on their specific choice, including, somewhat surprisingly, measurement outcome labeling. If measurements are chosen in a coherent way, the secrecy of the result can be completely lost for specific sets of MUB measurements but partially retained for others. This could potentially impact a broad spectrum of applications where MUBs are utilized.

DOI: 10.1103/PhysRevA.103.032206

I. INTRODUCTION

One of the defining features of quantum mechanics is the impossibility to simultaneously measure a certain set of physical quantities. This fact led to the definition of the famous Heisenberg uncertainty principle [1] and understanding of the quantum model of the hydrogen atom [2]. If a simultaneous measurement of two quantities is not possible, or, in other words, if a measurement of one quantity influences the expectation of the other measurement, we call these two measurements incompatible. In this context a very natural question arises: How incompatible can a pair of measurements be? The answer to this question is simple: For any quantum system, one can find a pair of measurements where, irrespective of the starting state of the system, after performing one of the measurements the result of the other one is completely random.

A straightforward generalization is at hand: Can one form a larger set of measurements that is pairwise fully incompatible? Here again one can answer affirmatively: For each system one can find at least three such measurements, and the size of this set depends on the dimension of the system.

In order to tackle these questions more formally, the notion of *mutually unbiased bases* (MUBs) [3–6] was introduced. Two d-dimensional bases, $\{|\psi_i\rangle\}_{i=0,\dots,d-1}$ and $\{|\varphi_j\rangle\}_{j=0,\dots,d-1}$, corresponding to two full projective measurements, are mutually unbiased when

$$\forall\, i, j : |\langle\psi_i|\varphi_j\rangle| = \frac{1}{\sqrt{d}}. \qquad (1)$$

Due to their properties, mutually unbiased bases have become an important cornerstone of contemporary quantum information processing [7]. They are being used for quantum tomography [4,6], uncertainty relations [5,8,9], quantum key distribution [10–13], and quantum error correction [14], as well as for witnessing entanglement [15–21], the design of Bell inequalities [22,23], and more general forms of quantum correlations [24–26].

The natural question of the number of unbiased bases in a given dimension d turned out to be unexpectedly complicated [27,28]. While the answer is rather simple for qubits—there are three pairwise mutually unbiased bases, defined as eigenvectors of Pauli $\sigma_x, \sigma_y, \sigma_z$ operators up to unitary equivalencies—in general, the construction of MUBs is a very difficult task. It is known that the number of MUBs has to be smaller than $d+1$ for any dimension and constructions of $d+1$ MUBs are known for $d = p^r$, where p is a prime. However, for non-prime-power d only the trivial tensor product construction is known.

Fortunately, for many applications one needs to use only $k \leqslant d+1$ MUB measurements. Clearly, there are different ways to pick the subset of k out of all MUBs. In fact, it is known that different sets of MUBs are not necessarily equivalent under different mathematical operations, such as global unitary operations, changing individual vector phases, relabeling of outcomes, relabeling of moments, and introducing complex conjugation [29]. This mathematical inequivalence is, however, irrelevant in many practical applications where just satisfying the defining property (1) is required for the task.

More interestingly, it was recently shown that different subsets of MUBs of can be inequivalent operationally as well. For example, MUBs turn out to be an optimal strategy in a communication task called quantum random access coding (QRAC) [30].

In [31] it was shown that in a certain variant of QRAC, different subsets of k out of $d+1$ MUBs lead to different strategies with different average success rates. More recently, it was shown that different subsets of k out of $d+1$ MUBs behave differently under a measure called incompatibility robustness [32]. Last but not least, very specific MUBs are required to obtain Bell inequalities [22], which are maximally violated by maximally entangled states and MUBs.

The full definition of a measurement consists of specifying the basis as a set of states and labeling these states. Two measurements consisting of the same set of states are, in principle, different, even if they measure the same property and their results can be classically transformed at any later stage. From an experimental and operational point of view it makes sense to distinguish between different measurements that differ only in labeling (we call this a *classical difference*) and two measurements that differ in the states per se (*quantum difference*). One can then naturally ask to what extent the properties of MUBs do change if one makes only a classical change in them. In other words, do the properties of the subsets change by simple relabeling of their vectors? In this work, we affirmatively answer this question by introducing a quantum information task called a *guessing game*. There a subset of d out of $d+1$ MUBs is used to hide and guess information between two parties. We show that this simple choice of removing a single MUB from the full set critically affects achievable results in the game. Even more interestingly, for a suitable chosen subset of d out of $d+1$ MUBs, we observe the full spectrum of results—perfect guessing and maximal hiding—just by relabeling the measurement outcomes.

II. RESULTS

The incompatibility of measurements can be demonstrated and examined with the help of a very simple quantum game, studied in [33,34]. Here Alice realizes one of m possible measurements on a d-dimensional system and records the result a of this measurement. The task of Bob is to guess this result using the following strategy: First, he prepares the state for Alice to measure, and second, he receives information about which measurement was performed (see the next section for the full definition of the guessing game).

If the game is described by classical physics, a pure state has a determined outcome for all possible measurements. Therefore, trivially, Bob can prepare a state which leads to a deterministic outcome irrespective of the measurement performed by Alice.

One can make the scenario partially quantum by making Bob's probe state as well as the measurements quantum but keeping the information about the measurement chosen by Alice classical—we call this a *classical coin scenario*. This is the traditional way to demonstrate incompatibility of quantum measurements; for compatible measurements Bob still can guess with certainty, but with increasing incompatibility of the measurements the uncertainty of his guess increases.

In a fully quantum scenario, called the *quantum coin scenario*, depicted in Fig. 1, both the probe state and the information about the measurement chosen are quantum. Here Alice realizes the chosen measurement by first applying a coherently controlled unitary, followed by a measurement in a standard basis. Bob receives the control state and can use it to determine Alice's outcome.

The authors of [33] analyzed the guessing game for two specific MUB measurements ($m=2$). They showed that for qubits ($d=2$), in the quantum coin scenario Bob can guess Alice's outcome with certainty. In contrast, that was not the case for higher dimensions. They concluded that in the case of two measurements the control state is always a two-dimensional state and it is impossible to use it to determine a higher-dimensional outcome.

In [34] we further analyzed the guessing game with the quantum coin, and we showed that for qubits, with any number of measurements (independent of their level of compatibility) it is always possible for Bob to obtain Alice's result with a probability of 1. In contrast, for higher dimensions this is not the case, so even if Bob receives a large enough control state, he will not be able to guess the result perfectly for a *specific set of MUBs* chosen by Alice.

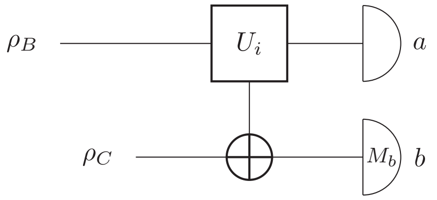

FIG. 1. Guessing-game description. Alice measures the probe state ρ_B with one out of d possible measurements. Alice's measurement choice is implemented coherently via a controlled unitary $\sum_{i=0}^{d-1} U_i^\dagger \otimes |i\rangle\langle i|$, where $U_i^\dagger$ maps the basis vectors of the ith basis onto the computational basis. Alice then measures in the computational basis, and her outcome is denoted a. Bob's goal is to guess Alice's outcome by preparing a probe state ρ_B and an optimal measurement described by POVM elements $\{M_b\}_{b=0}^{d-1}$, through which he obtains his guess b. Bob wins when $b=a$. In the *classical coin* case, the control state ρ_C is fully mixed, and in the *quantum coin* case, ρ_C is an equal superposition of computational basis vectors.

Here we analyze the problem further. We fix the number of measurements to $m=d$, which will make the size of the measurement outcomes alphabet equal to the dimension of the control state available to Bob. First, we study the quantum coin scenario with this choice for different sets of d MUBs, and for each prime d we construct a set of d MUBs which allow Bob to guess Alice's measurement outcomes with certainty. Further, with a combination of exhaustive search for $d=3$ and $d=5$ and numerical methods for higher dimensions we study Bob's guessing probability with different sets of d MUB measurements. We consider MUBs obtained by choosing d out of $d+1$ MUBs from standard Wootters-Fields (WF) construction (see [6] and Eq. (3)), followed by relabeling of their vectors in order to obtain different measurements.

Strikingly, both the lowest and highest guessing probabilities we observe are achieved by excluding the computational basis from $d+1$ WF bases and imposing different labeling of measurement outcomes on the rest of bases—the original WF labeling leads to the lowest guessing probabilities, while our construction, which is yet another outcome relabeling of this set of MUBs, leads to perfect guessing probability. More broadly, our study goes far beyond the study of the guessing game itself, as it shows that different sets of d out of $d+1$ MUBs, which differ in only a classical sense (i.e., by relabeling), exhibit very different operational properties.

III. GUESSING GAME

Here we give a formal definition of the guessing game and define a set of d out of $d+1$ MUB measurements, which allows Bob to construct a perfect guessing strategy. In the guessing game, Alice receives an initial state ρ_B of dimension d prepared by Bob. She performs a coherently controlled unitary transformation U_C defined by the set of $\{U_a^\dagger\}_{a=0}^{d-1}$ controlled by the "coin" state ρ_C. In the quantum coin scenario the pure state $\rho_C = |+\rangle\langle+|$ is used, where $|+\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle$, while in the classical coin scenario a fully mixed state $\rho_C = \frac{\mathbb{1}}{d}$ is used. After the transformation, Alice measures the state ρ_B in the computational basis and sends the control state ρ_C to Bob, who also performs a general measurement defined by positive operator-valued measure (POVM) elements $\{M_b\}_{b=0}^{d-1}$ to obtain his guess b. Bob wins if the results coincide.

The average guessing probability of Bob is defined as

$$P_g := \sum_{a=0}^{d-1} \mathrm{Tr}[(\rho_B \otimes \rho_C)U_C(|a\rangle\langle a| \otimes M_a)U_C^\dagger]. \tag{2}$$

Although there are multiple constructions of MUBs for prime dimensions, to demonstrate our result we will use a construction of Wootters and Fields [6]:

$$U_a^{\mathrm{WF}} = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1} \omega^{ai^2+ij}|i\rangle\langle j|. \tag{3}$$

In the prime dimension d, this construction defines d different bases and can be supplemented by the computational basis for the full set of $d+1$ MUBs. There are $d+1$ different ways to select the set of d bases. Additionally, for each set of d bases we will consider relabeling the vectors, which allows us to construct additional sets of d measurements used in the guessing game.

A. Classical coin scenario

In the case of a classical coin state, we have $\rho_C = \frac{\mathbb{1}}{d}$. Clearly, this is equivalent to Alice choosing the measurement uniformly at random and Bob then receiving the information about which measurement was chosen. Based on this information he has to guess the result obtained by Alice. While for qubits the optimal strategy for Bob is straightforward and easy to understand (he prepares a coherent superposition of two basis states of the two possible measurements of Alice) and yields a guessing probability of $\frac{1}{2}(1+\frac{1}{\sqrt{2}})$, for the higher-dimensional variant of the game the situation is much more complicated. In Appendix C we derive an *upper bound* in the form $\frac{1}{d}(1+\frac{d-1}{\sqrt{d}})$ valid for *any* set of MUBs (this includes relabeling since it does not influence Bob's guessing probability in the classical coin scenario), which converges to zero for high d. Furthermore, for the set of MUBs defined in (3) up to $d = 7$ we also obtain exact values. For higher d we provide numerical estimates that show that the bound obtained is not tight. These results show that without coherent information, with increasing d, Bob can obtain only negligible information about the result obtained by Alice irrespective of which set of MUBs she uses.

B. Quantum coin scenario

The situation is dramatically different for the quantum coin scenario, in which $\rho_C = |+\rangle\langle+|$. First, we show that for a specific selection of MUBs it is possible for Bob to obtain Alice's result with certainty. To achieve this, Alice needs to select both the proper d WF MUBs (quantum setting) and label the individual measurement basis vectors in a suitable way as well (classical setting). Specifically, if Alice chooses d WF bases without relabeling, Bob can never achieve perfect guessing, as we have shown in [34].

MUBs which result in Bob's perfect guessing probability are defined as

$$U_a^{DPP} = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1} \omega^{ai^2+ij-a^2i}|i\rangle\langle j|, \tag{4}$$

which can be seen as relabeling of the vectors of the bases of the WF construction: $U_a^{DPP}|j\rangle = U_a^{\mathrm{WF}}|j-a^2\rangle$.

Let us define Bob's (pure) probe state $|\psi_B\rangle$ and measurements $\{M_a\}_{a=0}^{d-1}$ as

$$\begin{aligned} |\psi_B\rangle &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{3^{d-2}k^3}|k\rangle, \\ M_a &= \frac{|\phi_a\rangle\langle\phi_a|}{\langle\phi_a|\phi_a\rangle}, \\ |\phi_a\rangle &:= \frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}\langle j|U_a^\dagger|\psi_B\rangle|a\rangle, \end{aligned} \tag{5}$$

where $|\phi_j\rangle$ are unnormalized pure states. In Appendix B we show that $\{M_a\}_{a=0}^{d-1}$ form a projective measurement. Subsequently, we show that such a measurement allows Bob to guess perfectly Alice's measurement outcomes if used in conjunction with the probe state $|\psi_B\rangle$.

Interestingly, if one of the WF bases is exchanged for the computational basis (which corresponds to a quantum difference), there is no way for Bob to achieve perfect guessing for any labeling of the individual measurements. In other words, if the computational basis is included in the set of MUBs used, we have strong numerical evidence that Alice can retain some secrecy towards Bob irrespective of the labeling used; for dimensions 3 and 5 this can be shown by an exhaustive search over all the possible relabelings; for higher dimensions we performed a randomized search (see Appendix D for details).

IV. OPTIMAL HIDING IN THE QUANTUM COIN CASE

We have shown that if Bob can influence the choice of MUBs used by Alice, he can perfectly guess her outcome. It is thus very natural to ask the complementary question: If Alice can retain full control of her measurements, what is the maximum Bob can learn about her outcome? And how does this maximum depend on the quantum setting of her measurements and actual labeling?

To answer this question fully, one would have to search through all possible MUBs, including their labeling, and find optimal values. To keep the task tractable, first, we have focused on the standard WF set of MUBs plus the computational basis (leading to $d+1$ possibilities) plus possible relabelings expressed via permutation matrices P_π, which relabel the computational basis states and leave the MUB property intact:

$$|\langle i|U_a^\dagger U_b|j\rangle| = \frac{1}{\sqrt{d}} = |\langle i|P_\pi U_a^\dagger U_b P_{\pi'}|j\rangle|.$$

Due to the intractably large number of combinations, for dimensions higher than 5 we first restricted ourselves to cyclic permutation matrices. On top of that, we have also tested randomly a large set of noncyclic permutation matrices.

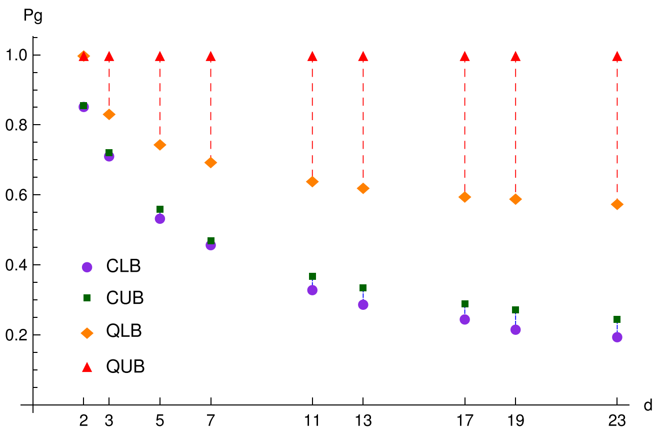

FIG. 2. Here we depict the bounds of the guessing probability for the classical and quantum coins for different dimensions. The quantum coin upper bound (QUB) is analytical and equal to 1. For d up to 5 the quantum coin lower bounds (QLBs) are over all relabeling (permutations); for higher dimensions they are over all cyclic permutations topped up by a random search. For d up to 7 the classical coin lower bounds (CLBs) are tight and obtained by an exhaustive search. The classical upper bounds (CUBs) are obtained via matrix inequalities.

For a fixed set of MUBs, we cast the problem a seesaw semidefnite programming [35] (see Appendix A for details), which allows us to obtain a lower bound on P_g. We have randomized the initial point and repeated the optimization to obtain the lower bounds as depicted in Fig. 2. As a last step, to look a bit behind the strict limit of WF construction and its relabeling, we applied the seesaw algorithm to unitaries close to the MUBs in the space of unitary matrices. In all cases we obtained values higher than the WF construction; this shows that the found values constitute (at least) a local minimum in the space of unitary matrices, while the search over permutation matrices suggests that they constitute a global minimum over the space of MUB unitary matrices as well.

While the obtained minima decrease with the dimension, they stay far above the upper bounds of the classical coin scenario. Thus, it is clear that irrespective of the selection of measurements by Alice, obtaining coherent information about her measurement allows Bob to take a more accurate guess. At the same time, in the case of the quantum coin, the maximal and minimal guessing probabilities discovered with our numerical methods change with the choice of both measurement bases and their labeling, making it critically important for Alice to carefully choose the MUBs used in the guessing game.

An analysis of the actual MUBs that lead to the obtained minimum guessing probability sheds some light on the problem. Surprisingly, it turned out that the minimal guessing probabilities we found are obtained for the standard WF construction of MUBs $\{U_a^{\mathrm{WF}}\}_{a=0}^{d-1}$. So in the case when Alice can make her choice of measurements, including the labeling, it is best for her to select the standard construction to minimize the knowledge of Bob. At the same time we could see that perfect guessing by Bob was achieved for the DPP construction defined in Eq. (4), which differs from the WF construction only by relabeling; that is, boundary values we found are achieved for MUBs that differ only by labeling.

On the contrary, if the computational basis is included in the system by exchanging it with any of the WF bases, we have strong numerical evidence that Bob cannot perfectly guess the outcome, nor can Alice hide it as well as in the WF case. This suggests that the set of d WF constructed bases including its relabeling is structurally different than any set in which the computational basis is used with $d-1$ WF bases. It is worth mentioning that this fact is not connected to the computation basis itself. One can find sets of MUBs containing computation bases that exhibit the same properties as the WF set or DPP set as defined in Eq. (4), but the remaining bases are not given by the WF construction.

V. DISCUSSION

In our work we have shown, using a simple quantum-mechanical game, that different choices of mutually unbiased bases have dramatic effects on experimentally achievable results. Interestingly, for any prime dimension d one can choose a set of d MUBs that provide the possibility of perfect guessing by Bob of the result obtained by Alice in the quantum coin scenario. At the same time, we obtained strong numerical evidence that with a set of MUBs that differs only by relabeling of the individual vectors, Alice can obtain the maximum hiding of her result that the game allows.

This result is very striking on its own, as it shows a very interesting and deep structure of the seemingly simple construction of MUBs. Even though all of the bases look very similar in their mathematical form, the subtle phase interdependences allow for some of the subsets to deliver results truly different from others.

More than that, the result is interesting from a practical viewpoint as well. While it might be considered very artificial to introduce quantum control of the measurement chosen by Alice, this is, in fact, the way how such control works, for instance, on the IBM quantum computer, where no classical control is available [36]. In the future design of quantum security elements it is possible that for technological reasons, quantum controls will be a standard procedure. In such a case, it will be very important to carefully consider the design of the quantum part so that the selected MUBs are not only secure as designed but are (reasonably) secure even in the case of coherent control and possible relabeling.

ACKNOWLEDGMENTS

We would like to thank F. Hirsch and M. T. Quintino for initial discussions and M. Farkas and J. Kaniewski for discussions about MUBs. We acknowledge funding from VEGA Project No. 2/0136/19. M. Pivoluska and M. Plesch additionally acknowledge GAMU Project No. MUNI/G/1596/2019.

APPENDIX A: OPTIMIZATION ALGORITHM

Given a MUB construction encoded by the unitaries $\{U_a\}_{a=0}^{d-1}$, we want to estimate the associated optimal strategy that Bob can use to guess Alice's outcomes in the quantum coin scenario. The optimal strategy would be the result of the following optimization:

$$\begin{aligned} P_g^{\max} &= \max_{\rho_B, \{M_a\}_{a=0}^{d-1}} \sum_{a=0}^{d-1} \mathrm{Tr}_{AB}[(\rho_B \otimes \rho_C) U_C (|a\rangle\langle a| \otimes M_a) U_C^\dagger] \\ &\text{s.t.} \quad \rho_B \geqslant 0, \\ &\mathrm{Tr}\rho_B = 1, \\ &M_a \geqslant 0 \quad \forall a \in \{0, \dots, d-1\}, \\ &\sum_{a=0}^{d-1} M_a = \mathbb{1}, \end{aligned} \tag{A1}$$

where the optimization variables are Bob's probe state ρ_B and Bob's POVM elements M_a corresponding to the outcome a. Also recall that ρ_C is the control state representing the choice of measurements, and U_C is a controlled unitary used to implement Alice's measurement settings coherently. The target function of this optimization problem is nonlinear; therefore, it cannot be solved directly by semidefinite programming (SDP). We therefore cast it as two SDPs, which we run alternatively. In the first SDP we optimize over $\{M_a\}_{a=0}^{d-1}$ with ρ_B being constant, and in the second one we optimize over ρ_B while $\{M_a\}_{a=0}^{d-1}$ are constant: For SDP 1, given ρ_B,

$$\begin{aligned} \{M_a\}_{a=0}^{d-1} &= \arg\max_{\{M_a\}_{a=0}^{d-1}} \frac{1}{d} \sum_{i,j,a=0}^{d-1} \langle i|M_a|j\rangle \langle a|U_j^\dagger \rho_B U_i|a\rangle \\ &\text{s.t.} \quad M_a \geqslant 0 \quad \forall a \in \{0, \dots, d-1\}, \\ &\sum_{a=0}^{d-1} M_a = \mathbb{1}. \end{aligned}$$

For SDP 2, given $\{M_a\}_{a=0}^{d-1}$,

$$\begin{aligned} \rho_B &= \arg\max_{\rho_B} \frac{1}{d} \sum_{i,j,a=0}^{d-1} \langle i|M_a|j\rangle \langle a|U_j^\dagger \rho_B U_i|a\rangle \\ &\text{s.t.} \quad \rho_B \geqslant 0, \\ &\mathrm{Tr}\rho_B = 1, \end{aligned}$$

where we simplified the notation with

$$\begin{aligned} &\sum_{a=0}^{d-1} \mathrm{Tr}_{AB}[(\rho_B \otimes \rho_C) U_C (|a\rangle\langle a| \otimes M_a) U_C^\dagger] \\ &\quad = \frac{1}{d} \sum_{i,j,a=0}^{d-1} \langle i|M_a|j\rangle \langle a|U_j^\dagger \rho_B U_i|a\rangle \end{aligned}$$

for

$$\begin{aligned} U_C &= \sum_{i=0}^{d-1} U_i^\dagger \otimes |i\rangle\langle i|, \\ \rho_C &= |+\rangle\langle +|, \\ |+\rangle &= \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle. \end{aligned}$$

The two SDPs are each guaranteed to converge; the seesaw, however, must stop at a "convergence parameter" ε that we set to be 10^{-6}. Explicitly, the seesaw algorithm is the following:

Algorithm 1 Seesaw

```
   Initialization: Generate a random density matrix $\rho_0$, distributed
1: according to the Hilbert-Schmidt measure. Set $P_W = 0$.
2: POVM optimization: Given $\rho_0$, solve the SDP with $\{M_a\}_{a=0}^{d-1}$ as
   a variable, and find the solution $\{M_a^*\}_{a=0}^{d-1}$.
3: State optimization: Given $\{M_a^*\}_{a=0}^{d-1}$ from step 2, solve the SDP
   with $\rho_B$ as a variable, and find the solution $\rho_B^*$ and $P_W^*$.
4: Convergence check:
     • If $P_W^* - P_W > \varepsilon$, then set $\rho_0 = \rho_B^*$ and $P_W = P_W^*$. Repeat
       from step 2.
     • If $P_W^* - P_W < \varepsilon$, stop the algorithm. The complete solution is
       given by $P_W^*$, $\rho_B^*$, $\{M_a^*\}_{a=0}^{d-1}$.
```

The algorithm is then applied to a large number of initial random points ρ_0. We observed that for small enough ε it always yields the same result P_W^*, suggesting that the seesaw algorithm tightly lower bounds the solution of (A1).

APPENDIX B: OPTIMAL STRATEGY

In the DDP construction we considered Alice's MUB measurements, defined as $U_a = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ai^2 + ij - a^2 i} |i\rangle\langle j|$. Bob's optimal strategy in this case is

$$\begin{aligned} |\psi_B\rangle &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{3^{d-2} k^3} |k\rangle, \\ M_a &= \frac{|\phi_a\rangle\langle\phi_a|}{\langle\phi_a|\phi_a\rangle}, \\ |\phi_a\rangle &= \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} \langle j|U_a^\dagger|\psi_B\rangle |a\rangle, \end{aligned}$$

where $|\psi_B\rangle$ is Bob's (pure) probe state and $\{M_a\}_{a=0}^{d-1}$ are POVM elements of the measurement he uses on the probe state $\rho_C = |+\rangle\langle +|$ to guess Alice's outcome. Note that states $|\phi_a\rangle$ are not normalized.

Here we show that $\{M_a\}_{a=0}^{d-1}$ is, indeed, a valid POVM, i.e. $M_a \geqslant 0 \ \forall a$ and $\sum_{a=0}^{d-1} M_a = \mathbb{1}$. Positivity is guaranteed by definition. To prove summation to identity we notice that M_a are projectors and span the Hilbert space of Bob if $\{\frac{|\phi_j\rangle}{\||\phi_j\rangle\|}\}_{j=0}^{d-1}$ form an orthonormal basis. Normalization is guaranteed by definition, so it remains to prove orthogonality:

$$\begin{aligned} \langle\phi_i|\phi_j\rangle &= \frac{1}{d} \sum_{a=0}^{d-1} \langle j|U_a^\dagger|\psi_B\rangle \langle\psi_B|U_a|i\rangle \\ &= \frac{1}{d^3} \sum_{a,k,l=0}^{d-1} \omega^{-(ak^2 + jk - a^2 k)} \omega^{3^{d-2} k^3} \omega^{-3^{d-2} l^3} \omega^{al^2 + il - a^2 l} \\ &= \frac{1}{d^3} \sum_{a,k,l=0}^{d-1} \omega^{-ak^2 - jk + a^2 k + 3^{d-2} k^3 - 3^{d-2} l^3 + al^2 + il - a^2 l}. \end{aligned}$$

1. Dimensions larger than 3

In what follows, we will show that for $d > 3$ ($d = 3$ and $d = 2$ are treated separately) the above expression can be simplified using quadratic Gauss sums. In order to do so, we will manipulate the exponents of ω. The key idea is to realize that since $\omega^d = 1$, we can work with its exponent modulo d. Additionally, we introduce a substitution,

$$m = l + k, \quad n = l - k,$$

and two constants,

$$\alpha = 3^{d-2} \equiv 3^{-1} \pmod{d},$$
$$\beta = 2^{d-2} \equiv 2^{-1} \pmod{d}.$$

From these definitions it follows that

$$\begin{aligned}
l &\equiv \beta(m+n) \pmod{d},\\
3\alpha &\equiv 1 \pmod{d},\\
k &\equiv \beta(m-n) \pmod{d},\\
2\beta &\equiv 1 \pmod{d},\\
l^2 - k^2 &\equiv mn \pmod{d},\\
il - jk &\equiv \beta m(i-j) + \beta n(i+j) \pmod{d},\\
l^3 - k^3 &\equiv \beta^2 n(3m^2 + n^2) \pmod{d}.
\end{aligned}$$

We will also use the quadratic Gauss sum:

$$\sum_{a=0}^{d-1} \omega^{a^2 m} = \begin{cases} \left(\frac{m}{d}\right)\varepsilon_d\sqrt{d} & \text{if } m \not\equiv 0 \ (\mathrm{mod}\ d),\\ d & \text{if } m \equiv 0 \ (\mathrm{mod}\ d),\end{cases}$$

where $(\frac{m}{d})$ is the Legendre symbol:

$$\left(\frac{m}{d}\right) = \begin{cases} 1 & \text{if } \exists n : m \equiv n^2 \ (\mathrm{mod}\ d),\\ -1 & \text{if } \nexists n : m \equiv n^2 \ (\mathrm{mod}\ d),\end{cases}$$

and

$$\varepsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \ (\mathrm{mod}\ 4),\\ i & \text{if } d \equiv 3 \ (\mathrm{mod}\ 4).\end{cases}$$

After the substitution, the expression reads

$$\begin{aligned}
&\langle\phi_i|\phi_j\rangle\\
&= \frac{1}{d^3}\sum_{a,m,n=0}^{d-1} \omega^{amn - a^2 n - \alpha\beta^2 n^3 - \beta^2 m^2 n + \beta m(i-j) + \beta n(i+j)}\\
&= \frac{1}{d^3}\sum_{m,n=0}^{d-1} \omega^{-\alpha\beta^2 n^3 - \beta^2 m^2 n + \beta m(i-j) + \beta n(i+j)} \sum_{a=0}^{d-1} \omega^{amn - a^2 n}.
\end{aligned}$$

The sum over a is a quadratic Gauss sum:

$$\begin{aligned}
\sum_{a=0}^{d-1} \omega^{-a^2 n + amn} &= \sum_{a=0} \omega^{-n(a-\beta m)^2}\omega^{\beta^2 m^2 n}\\
&= \omega^{\beta^2 m^2 n}\sum_{a=0}^{d-1}\omega^{-a^2 n}\\
&= \begin{cases} \omega^{\beta^2 m^2 n}\left(\frac{-n}{d}\right)\varepsilon_d\sqrt{d} & \text{if } n \not\equiv 0 \ (\mathrm{mod}\ d),\\ d & \text{if } n \equiv 0 \ (\mathrm{mod}\ d),\end{cases}
\end{aligned}$$

where the second equality follows from the fact that $(a - \beta m)^2$ iterates over the same values $\pmod{d}$ as a^2. Substituting this expression in the previous one, we obtain

$$\begin{aligned}
\langle\phi_i|\phi_j\rangle &= \frac{1}{d^3}\sum_{m=0}^{d-1}\omega^{\beta m(i-j)}\\
&\quad\times\left[\sum_{n=1}^{d-1}\varepsilon_d\sqrt{d}\left(\frac{-n}{d}\right)\omega^{-\alpha\beta^2 n^3 + \beta n(i+j)} + d\right]\\
&= \frac{\delta_{ij}}{d}\left[\frac{\varepsilon_d}{\sqrt{d}}\sum_{n=1}^{d-1}\left(\frac{n}{d}\right)\omega^{12^{(d-2)}n^3 - nj} + 1\right],
\end{aligned} \tag{B1}$$

which shows that they are orthogonal as requested. We then show that this construction gives a guessing probability $P_g = 1$:

$$\begin{aligned}
P_g &= \sum_{k=0}^{d-1}\mathrm{Tr}_{AB}\big[U_C^\dagger(\rho_B\otimes\rho_C)U_C(|k\rangle\langle k|\otimes M_k)\big]\\
&= \sum_{k=0}^{d-1}\mathrm{Tr}_{AB}\left(\sum_{a=0}^{d-1}U_a^\dagger\otimes|a\rangle\langle a|\right)\left(|\psi_B\rangle\langle\psi_B|\otimes\frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\right)\\
&\quad\times\left(\sum_{b=0}^{d-1}U_b\otimes|b\rangle\langle b|\right)\left(|k\rangle\langle k|\otimes\frac{|\phi_k\rangle\langle\phi_k|}{\langle\phi_k|\phi_k\rangle}\right)\\
&= \mathrm{Tr}_B\sum_{k=0}^{d-1}\left(\frac{1}{\sqrt{d}}\sum_a\langle k|U_a^\dagger|\psi_B\rangle|a\rangle\right)\\
&\quad\times\left(\frac{1}{\sqrt{d}}\sum_b\langle\psi_B|U_b|k\rangle\langle b|\right)\frac{|\phi_k\rangle\langle\phi_k|}{\langle\phi_k|\phi_k\rangle}\\
&= \mathrm{Tr}_B\sum_{k=0}^{d-1}|\phi_k\rangle\langle\phi_k|\frac{|\phi_k\rangle\langle\phi_k|}{\langle\phi_k|\phi_k\rangle}\\
&= \sum_k\langle\phi_k|\phi_k\rangle\\
&= \frac{1}{d}\sum_{a,b,k=0}^{d-1}\langle b|a\rangle\langle k|U_a^\dagger|\psi_B\rangle\langle\psi_B|U_b|k\rangle\\
&= \frac{1}{d}\sum_{a=0}^{d-1}\langle\psi_B|U_a\left(\sum_{k=0}^{d-1}|k\rangle\langle k|\right)U_a^\dagger|\psi_B\rangle\\
&= \frac{1}{d}\sum_{a=0}^{d-1}\langle\psi_B|\mathbb{1}|\psi_B\rangle = 1.
\end{aligned} \tag{B2}$$

2. Dimension 3

Above we have shown that Bob can guess with probability 1 for $d > 3$. For the case $d = 2$ the optimal strategy can be found in [33]. For $d = 3$, the proof needs to be adapted due to the fact that a multiplicative inverse $\pmod{3}$ of 3 does not exist; we then use $\omega = e^{\frac{2\pi i}{3}}$ for Alice's MUB construction $U_a = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}\omega^{ai^2+ij-a^2 i}|i\rangle\langle j|$, and with $\omega_9 = e^{\frac{2\pi i}{9}}$ we define Bob's strategy as

$$M_a = \frac{|\phi_a\rangle\langle\phi_a|}{\langle\phi_a|\phi_a\rangle},$$

$$|\phi_a\rangle = \frac{1}{\sqrt{d}}\sum_{a=0}^{2}\langle j|U_a^{\dagger}|\psi_B\rangle|a\rangle,$$

$$|\psi_B\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{2}\omega_9^{k^3}|k\rangle.$$

The proof follows exactly the same steps as (B1), with all the substitutions remaining valid, with the exception of

$$\begin{aligned}\omega_9^{k^3-l^3} &= \omega_9^{-\beta^2 n(3m^2+n^2)}\\ &= \omega^{-\beta^2 m^2 n}\omega_9^{-\beta^2 n^3}\\ &= \omega^{-\beta^2 m^2 n}\omega_9^{-7n^3},\end{aligned}$$

where we made use of the fact that $\beta = 5$ is the multiplicative inverse of 2 (mod 3) and (mod 9). We then get

$$\langle\phi_i|\phi_j\rangle = \frac{\delta_{ij}}{3}\left[\frac{\varepsilon_3}{\sqrt{3}}\sum_{n=1}^{2}\left(\frac{n}{d}\right)\omega_9^{7n^3-3nj} + 1\right],$$

concluding the proof.

APPENDIX C: CLASSICAL COIN

In the classical case, the control state is a computational basis vector $|i\rangle$, chosen uniformly at random, which selects the measurement used by Alice via the controlled unitary U_C. Therefore, it contains full information about the basis Alice measures in, which can be obtained by Bob performing a measurement in the computational basis. Any other measurement by Bob only introduces extra entropy to this information via uncertainty principle and thus decreases Bob's guessing probability. Bob's optimal guessing strategy is therefore a simple projection onto the computational basis, which reveals Alice's measurement basis i, followed by a map $\tilde{n}(i)$ that associates to each basis i the most probable outcome of Alice for that basis. Note that this also means that the maximum guessing probability in the classical scenario does not depend on the labeling of the outcomes since the labeling does not change the probability of the most probable outcome. Formally,

$$\tilde{n}(i) := \underset{j\in\{0,\dots,d-1\}}{\arg\max}\ P_A(j|U_i),$$

$$P_A(j|U_i) = \mathrm{Tr}(\rho_B U_i|j\rangle\langle j|U_i^{\dagger}),$$

$$M_i = \sum_{i=0:\tilde{n}(i)=j}^{d-1}|i\rangle\langle i|.$$

With these definitions we can state the problem as follows:

$$\begin{aligned}P_g^c &:= \max_{\rho_B,\{M_k\}_{k=0}^{d-1}}\sum_{k=0}^{d-1}\mathrm{Tr}_{AB}\left[\left(\rho_B\otimes\frac{\mathbb{1}}{d}\right)U_C(|k\rangle\langle k|\otimes M_k)U_C^{\dagger}\right]\\ &= \max_{\rho_B}\max_{n_0,n_1,\dots,n_d}\frac{1}{d}\mathrm{Tr}\left(\sum_{j=0}^{d-1}\rho_B U_j|n_j\rangle\langle n_j|U_j^{\dagger}\right)\\ &= \frac{1}{d}\max_{\rho_B}\mathrm{Tr}\left(\sum_{j=0}^{d-1}\rho_B U_j|\tilde{n}(j)\rangle\langle\tilde{n}(j)|U_j^{\dagger}\right)\\ &= \frac{1}{d}\lambda_{\max}\left[\sum_{j=0}^{d-1}U_j|\tilde{n}(j)\rangle\langle\tilde{n}(j)|U_j^{\dagger}\right],\end{aligned}$$

where $\lambda_{\max}[T]$ is the largest eigenvalue of a matrix T. For small dimensions, the maximum probability can be found by evaluating all possible mappings $\tilde{n}(j)$ (there are d^d of them). This, however, quickly becomes infeasible; therefore, we look for an upper bound:

$$P_g^c = \frac{1}{d}\left(1 + \lambda_{\max}\left[\sum_{j=0}^{d-1}U_j|\tilde{n}(j)\rangle\langle\tilde{n}(j)|U_j^{\dagger} - \mathbb{1}\right]\right);$$

to simplify the notation we define

$$T_j := U_j|\tilde{n}(j)\rangle\langle\tilde{n}(j)|U_j^{\dagger} - \frac{\mathbb{1}}{d},$$

$$T := \sum_{j=0}^{d-1}T_j,$$

which satisfy the following properties:

$$\begin{aligned}\mathrm{Tr}(T_j) &= 0 \quad \forall j\in\{0,\dots,d-1\},\\ \mathrm{Tr}(T_i^{\dagger}T_j) &= 0 \quad \forall i\neq j\in\{0,\dots,d-1\},\\ \mathrm{Tr}\big(T_j^2\big) &= \frac{d-1}{d} \quad \forall j\in\{0,\dots,d-1\},\\ \mathrm{Tr}(T^2) &= \mathrm{Tr}\left(\sum_{i,j=0}^{d-1}T_i^{\dagger}T_j\right)\\ &= \sum_{i=0}^{d-1}\mathrm{Tr}(T_i^{\dagger}T_i) + \sum_{\substack{i,j=0\\ i\neq j}}^{d-1}\mathrm{Tr}(T_i^{\dagger}T_j)\\ &= d-1.\end{aligned}$$

The guessing probability with a classical coin can then be expressed as

$$P_g^c := \frac{1}{d}(1+\lambda_{\max}[T]).$$

Since T is traceless and Hermitian, its largest eigenvalue is positive. We then use the following inequality:

$$\begin{aligned}\mathrm{Tr}(T^2) &= \lambda_{\max}^2[T]\,\mathrm{Tr}\left(\frac{T^2}{\lambda_{\max}^2[T]}\right)\\ &\geqslant \lambda_{\max}^2[T]\left(1+\min_{S\in M_{d-1}:\mathrm{Tr}S=-1}\mathrm{Tr}(S^2)\right)\\ &= \lambda_{\max}^2[T]\left(1+\frac{1}{d-1}\right)\\ &= \lambda_{\max}^2[T]\frac{d}{d-1},\end{aligned}$$

where we denoted the space of Hermitian matrices of order $d-1$ by M_{d-1}. Substituting the trace of T^2, we get the desired upper bound:

$$\lambda_{\max}[T] \leqslant \frac{d-1}{\sqrt{d}},$$

$$P_g^c \leqslant \frac{1}{d}\left(1+\frac{d-1}{\sqrt{d}}\right).$$

APPENDIX D: NUMERIC SEARCH

1. Classical coin

When considering a classical coin, the optimal strategy is given by searching over all possible maps $\tilde{n} : \mathbb{Z}_d \to \mathbb{Z}_d$ and taking the largest eigenvalue of the matrix $T = \sum_{j=0}^{d-1} U_j |\tilde{n}(j)\rangle\langle\tilde{n}(j)| U_j^\dagger - \mathbb{1}$. There are d^d such mappings, and we could perform this extensive search for $d = 2, 3, 5, 7$, obtaining exact bounds for these dimensions. In other dimensions lower bounds were obtained by applying the seesaw algorithm in Appendix A with $\rho_C = \mathbb{1}/d$ and randomized initial points. This algorithm tends to get stuck in local maxima; however, in the dimensions in which we could perform the extensive search we observed that the seesaw algorithm returned the maximum value more often than by a random sampling of $\tilde{n}$ in the space of maps $\mathbb{Z}_d \to \mathbb{Z}_d$.

2. Quantum coin

For the quantum coin, for a small enough convergence parameter ε (10^{-6}) we did not observe convergences to local maxima different from the global maximum. Differently from the classical case, the choice of unitaries changes the value of the maximum. We then search for the smallest such value among all possible unitary constructions. The space over which we search is given by choosing $d+1$ unitaries out of the $d+1$ available from the WF construction and by relabeling, i.e., applying a permutation matrix to each unitary. For $d = 3, 5$ we searched over all possible permutations; for $d = 7$ we considered only cyclic permutations, while for higher dimensions we randomly sampled over the space of permutation matrices. Each search was performed for all $d+1$ choices of unitaries. We observed that the WF unitaries give the lowest value when the excluded unitary is the identity.

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).

[2] N. Bohr, London, Edinburgh, Dublin Philos. Mag. J. Sci. **26**, 1 (1913).

[3] J. Schwinger, Proc. Natl. Acad. Sci. USA **46**, 570 (1960).

[4] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).

[5] K. Kraus, Phys. Rev. D **35**, 3070 (1987).

[6] W. K. Wootters and B. D. Fields, Ann. Phys. (NY) **191**, 363 (1989).

[7] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum Inf. **8**, 535 (2010).

[8] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[9] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).

[10] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[11] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **67**, 062310 (2003).

[12] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[13] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).

[14] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).

[15] Y. Huang, Phys. Rev. A **82**, 012335 (2010).

[16] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Phys. Rev. A **86**, 022311 (2012).

[17] L. Maccone, D. Bruß, and C. Macchiavello, Phys. Rev. Lett. **114**, 130401 (2015).

[18] E. C. Paul, D. S. Tasca, L. Rudnicki, and S. P. Walborn, Phys. Rev. A **94**, 012303 (2016).

[19] J. Řeháček, Z. Hradil, A. B. Klimov, G. Leuchs, and L. L. Sánchez-Soto, Phys. Rev. A **88**, 052110 (2013).

[20] P. Erker, M. Krenn, and M. Huber, Quantum **1**, 22 (2017).

[21] J. Bavaresco, N. Herrera Valencia, C. Klöckl, M. Pivoluska, P. Erker, N. Friis, M. Malik, and M. Huber, Nat. Phys. **14**, 1032 (2018).

[22] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, Quantum **3**, 198 (2019).

[23] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, and J. Kaniewski, Sci. Adv. **7**, eabc3847 (2021).

[24] P. Skrzypczyk and D. Cavalcanti, Phys. Rev. A **92**, 022354 (2015).

[25] D. Sauerwein, C. Macchiavello, L. Maccone, and B. Kraus, Phys. Rev. A **95**, 042315 (2017).

[26] A. C. S. Costa, R. Uola, and O. Gühne, Phys. Rev. A **98**, 050104(R) (2018).

[27] S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008).

[28] P. Jaming, M. Matolcsi, and P. Móra, Cryp. Commun. **2**, 211 (2010).

[29] S. Brierley, S. Weigert, and I. Bengtsson, Quantum Inf. Comput. **10**, 803 (2010).

[30] M. Farkas and J. Kaniewski, Phys. Rev. A **99**, 032316 (2019).

[31] E. A. Aguilar, J. J. Borkała, P. Mironowicz, and M. Pawłowski, Phys. Rev. Lett. **121**, 050501 (2018).

[32] S. Designolle, P. Skrzypczyk, F. Fröwis, and N. Brunner, Phys. Rev. Lett. **122**, 050402 (2019).

[33] F. Rozpedek, J. Kaniewski, P. J. Coles, and S. Wehner, New J. Phys. **19**, 023038 (2017).

[34] M. Plesch and M. Pivoluska, New J. Phys. **20**, 023018 (2018).

[35] M. Laurent and F. Rendl, in *Discrete Optimization*, edited by K. Aardal, G. Nemhauser, and R. Weismantel, Handbooks in Operations Research and Management Science Vol. 12 (Elsevier, Amsterdam, 2005), pp. 393.

[36] An example of using coherent control instead of classical is given in the QISKIT tutorial on quantum teleportation, doi:10.5281/zenodo.2562110.