nature portfolio

Peer Review File

Unconditional and exponentially large violation of classicality

Corresponding Author: Dr Marcello Benedetti

This manuscript has been previously reviewed at another journal. This document only contains information relating to versions considered at Nature Communications. Previous journal names are redacted.

This file contains all reviewer reports in order by version, followed by all author rebuttals in order by version.

Version 0:

Reviewer comments:

Reviewer #1

(Remarks to the Author)
I am the Reviewer #1 as denoted by the authors in the response document.

As mentioned in my previous report, the work presented in the manuscript is of high quality and of relevance to the broader scientific community. The point-to-point responses to my previous review on the manuscript addressed all of my previous comments and concerns satisfactorily.

The revised manuscript is largely similar to the one submitted to [redacted] but with revisions to address the reviewers comments. Notably, there is an entirely new section "Playing without trust in the state preparation" in an attempt to address the greatest drawback of the Complement Sampling Game (CSG), which is having to trust the state preparation of the referee. The authors analyse the gap between the optimal classical and quantum strategies of the players in "2-by-2" matrix exploring scenarios where players and referee are either trusted or not trusted. However, as written in the manuscript, the motivations of the exercise is not clear to me.

Taking a step back, the objective of this entire manuscript is to provide a test for the players. Hence, this section should analyse various scenarios of CSG through the lens of testing the "quantum-ness" of players. With that said, it is clear that ideally, the players are untrusted because they are the subjects of the test.

Next, the referee's integrity and intent must be trusted i.e. the referee is not malicious. Otherwise, we should not even trust them with the fair coin or to make a legitimate measurement on the prepared quantum state. We need to be clear that the "untrusted referee" refers to the referee's device that prepares the quantum state may prepare quantum state that deviates from the ideal state the referee intends to prepare.

In particular, my confusion stems from the following:

From line 162-166: If the referee has a separate measurement device that is characterised, it could be used to bound the fidelity of the prepared state when the coin outputs c=1. In some sense, the untrusted state preparation could be used to test untrusted players using the referee's trusted measurement device.

Everywhere else in the manuscript: The considered scenario where players are trusted and the referee is untrusted seems to suggest that the players are used to measure the prepared quantum states when c=1. (While this goes against the manuscript's motivations of testing the players, I am open a scenario where the players and referee's state preparation are probabilistically taking turns to be untrusted and tested if the authors prove that such a framework is viable i.e. c=0 untrusted players, trusted referee c=1 trusted players, untrusted referee)

In conclusion, I think that the bulk of the manuscript is well-written, high impact and suitable for publication in prestigious journals such as Nature Communications. However, the newly introduced section does present some confusion to me. Prior to giving my recommendation for publication of the revised manuscript, the authors will have to present the new section clearly and address the above-mentioned comments.

(Remarks on code availability)

Reviewer #2

(Remarks to the Author)
The revised manuscript addressed the majority of concerns raised by both reviewers or includes changes that invalidate those concerns.
Particularly, the discussion around assumptions and trust has been extended, which now provides a more complete picture. Also, the newly added rigidity score provides some clarity around the limitations under various trust assumptions.
I believe Fig. 2A now provides a better illustration of the data, while I maintain that Fig.2B provides very limited additional information. Related to this, I remain sceptical of the emphasis on the "exponential" violation, rather than focusing on the fact that this is a fairly simple (up to the referee) game that highlights the advantage of a quantum superposition over classical sampling.
Finally, since the authors state that the role of imperfect randomness is not currently known, I believe a comment should be made in the manuscript to point this out.
Other than that, I believe the manuscript is well-suited for publication in Nature Communications.

(Remarks on code availability)

Version 1:

Reviewer comments:

Reviewer #1

(Remarks to the Author)
Thank you for the point-to-point responses to my previous comments and the changes made to the manuscript. The additional sentences in the manuscript gave clarity to the newly added section. I think the current manuscript addresses all comments by both reviewers and as such, I recommend its publication in Nature Communications.

(Remarks on code availability)

Reviewer #1

I am the Reviewer #1 as denoted by the authors in the response document. As mentioned in my previous report, the work presented in the manuscript is of high quality and of relevance to the broader scientific community. The point-to-point responses to my previous review on the manuscript addressed all of my previous comments and concerns satisfactorily.

We thank Reviewer #1 for taking the time to review our work one more time.

The revised manuscript is largely similar to the one submitted to [name redacted] but with revisions to address the reviewers comments. Notably, there is an entirely new section "Playing without trust in the state preparation" in an attempt to address the greatest drawback of the Complement Sampling Game (CSG), which is having to trust the state preparation of the referee. The authors analyse the gap between the optimal classical and quantum strategies of the players in "2-by-2" matrix exploring scenarios where players and referee are either trusted or not trusted. However, as written in the manuscript, the motivations of the exercise is not clear to me.

Taking a step back, the objective of this entire manuscript is to provide a test for the players. Hence, this section should analyse various scenarios of CSG through the lens of testing the "quantum-ness" of players. With that said, it is clear that ideally, the players are untrusted because they are the subjects of the test.

Next, the referee's integrity and intent must be trusted i.e. the referee is not malicious. Otherwise, we should not even trust them with the fair coin or to make a legitimate measurement on the prepared quantum state. We need to be clear that the "untrusted referee" refers to the referee's device that prepares the quantum state may prepare quantum state that deviates from the ideal state the referee intends to prepare.

The motivation for section "Playing without trust in the state preparation" was to characterize the CSG while relaxing some of the original assumptions. The section should not be seen as limiting, but rather as expanding the scope of CSG. In particular, it shows that it is in principle possible to use CSG to test the referee state preparation device.

Perhaps Reviewer #1 is suggesting that the party being tested should *always* be called the 'player'. Unfortunately we think that this seemingly harmless relabeling would be confusing: in all our proofs and discussions we defined the referee as the party that prepares the initial state.

As Reviewer #1 says, the referee must be fair and cannot deviate from the intended behavior. Indeed we have never referred to an 'untrusted referee' in the paper. The new section was about the 'untrusted state preparation' or 'untrusted device' which may be used by the referee. Since this wasn't crystal clear, we have added a sentence to the paper.

In particular, my confusion stems from the following:

From line 162-166: If the referee has a separate measurement device that is characterised, it could be used to bound the fidelity of the prepared state when the coin outputs c=1. In some sense, the untrusted state preparation could be used to test untrusted players using the referee's trusted measurement device.

The issue with Reviewer #1's proposal is that a 'separate measurement device' cannot efficiently establish the fidelity of the state preparation solely from the rounds where $c = 1$. At

each round, a single copy of a different subset state is prepared, and so it is impossible to perform a tomographic protocol to establish the fidelity any given state.

Our results show that a *full execution* of CSG can be used to find a lower bound on the expected fidelity of the state preparation device. This version of the game has the referee flipping a coin c at each round: when $c = 0$ the state is sent to a trusted player which performs complement sampling; when $c = 1$ the referee measures the state directly. If the obtained rigidity score is $R \geq 1 - \epsilon$, then the expected fidelity is $\geq 1 - \epsilon$. Please note that we did not work out the practical details of such a state preparation certification protocol in the paper, as we focused on testing the player instead. We added a sentence in the discussion to clarify this.

Everywhere else in the manuscript: The considered scenario where players are trusted and the referee is untrusted seems to suggest that the players are used to measure the prepared quantum states when c=1. (While this goes against the manuscript's motivations of testing the players, I am open a scenario where the players and referee's state preparation are probabilistically taking turns to be untrusted and tested if the authors prove that such a framework is viable i.e. c=0 untrusted players, trusted referee c=1 trusted players, untrusted referee)

As explained in the previous reply, a full execution of CSG with both $c = 0$ and $c = 1$ would be used to test the fidelity of the state preparation. We do *not* let players and referees swap their roles, and we do *not* allow for probabilistically changing the assumptions about their devices. As already proven in Supplementary Material 3 and summarized by Table 1, there are only two interesting settings: A) the referee state preparation is trusted and a CSG is used to test the quantumness of the player; or B) the player is trusted and a CSG is used to test the fidelity of the refere's device. In the experiments and in the paper in general, we chose to focus on setting A. Again, the new sentence in the discussion should make it clear for the reader.

In conclusion, I think that the bulk of the manuscript is well-written, high impact and suitable for publication in prestigious journals such as Nature Communications. However, the newly introduced section does present some confusion to me. Prior to giving my recommendation for publication of the revised manuscript, the authors will have to present the new section clearly and address the above-mentioned comments.

Thank you for the assessment of our paper. In summary, the newly introduced section shows that CSG can be repurposed to test state preparation devices, thus expanding its original scope. We hope this point is clearer now that we have implemented minor revisions.

Reviewer #2

The revised manuscript addressed the majority of concerns raised by both reviewers or includes changes that invalidate those concerns. Particularly, the discussion around assumptions and trust has been extended, which now provides a more complete picture. Also, the newly added rigidity score provides some clarity around the limitations under various trust assumptions.

We thank Reviewer #2 for reading our paper again and providing feedback.

I believe Fig. 2A now provides a better illustration of the data, while I maintain that Fig.2B provides very limited additional information. Related to this, I remain sceptical of the emphasis on the "exponential" violation, rather than focusing on the fact that this is a fairly simple (up to the referee) game that highlights the advantage of a quantum superposition over classical sampling.

We are glad to hear that Fig. 2A has improved. Regarding our emphasis on the "exponential violation" we want to be clear: we are not attempting to hype the result here. Ours is a quantitative result supported by the theory in Supplementary Note 1, as well as simulation and experiment data in Fig 2B. Our theory in Supplementary Note 1 is based on and extends the established way to quantify "Bell inequality violations" in non-local games to our setting of a single-player game.

Finally, since the authors state that the role of imperfect randomness is not currently known, I believe a comment should be made in the manuscript to point this out. Other than that, I believe the manuscript is well-suited for publication in Nature Communications.

We have added a sentence in the Discussion to clarify that the effect of imperfect randomness in the referee state preparation remains unknown.