Three-player entangled XOR games are NP-hard to approximate

Thomas Vidick*

Abstract

We show that for any $\varepsilon > 0$ the problem of finding a factor $(2-\varepsilon)$ approximation to the entangled value of a three-player XOR game is NP-hard. Equivalently, the problem of approximating the largest possible quantum violation of a tripartite Bell correlation inequality to within any multiplicative constant is NP-hard. These results are the first constant-factor hardness of approximation results for entangled games or quantum violations of Bell inequalities shown under the sole assumption that P$\neq$NP. They can be thought of as an extension of Håstad's optimal hardness of approximation results for MAX-E3-LIN2 (JACM'01) to the entangled-player setting.

The key technical component of our work is a soundness analysis of a point-vs-plane low-degree test against entangled players. This extends and simplifies the analysis of the multilinearity test by Ito and Vidick (FOCS'12). Our results demonstrate the possibility for efficient reductions between entangled-player games and our techniques may lead to further hardness of approximation results.

1 Introduction

In quantum mechanics, two or more spatially isolated systems are said to be *entangled* if no complete description of their joint state can be obtained solely from the combination of individual descriptions of each of the sub-systems. This intuitive definition is due to Schrödinger,[1] who first coined the term "entangled" in reaction to Einstein, Podolsky and Rosen's criticism of quantum mechanics as an incomplete theory [EPR35]. It is only through the work of Bell [Bel64], thirty years later, that a mathematically sound and (at least in principle) experimentally verifiable theory for the quantification of the nonlocal effects of entanglement first arose. Bell proposed the use of what are now known as "Bell inequalities". Suppose that each subsystem can be locally observed using any one among a set of possible measurements Q, each producing outcomes in A. For any choice of settings $(q_1,\ldots,q_r) \in Q^r$ the measurements' outcomes can be described by a joint distribution $p(a_1,\ldots,a_r|q_1,\ldots,q_r)$. A *Bell inequality* is a linear inequality in the A^rQ^r variables $p(a_i|q_i)$ that is satisfied by any product distribution.[2] A state is entangled if and only if there exists a choice of local measurements on its subsystems that give rise to a collection of distributions violating a Bell inequality [Gis91].

The use of Bell inequalities has taken an increasingly central role in all aspects of quantum mechanics, from the study of its foundations to applications in quantum computing and cryptography. Somewhat

*Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology. Supported by the National Science Foundation under Grant No. 0844626.

[1] "When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives have become entangled." [Sch35]

[2] By linearity, the inequality will automatically be satisfied by any *convex combination* of product distributions as well.

ignored in the immediate aftermath of Bell's work, interest was revived after the discovery by Clauser et al. [CHSH69] of the first simple inequality that could realistically lead to an experiment (indeed, the experiment was successfully performed by Aspect [ADR82] some thirteen years later). Their inequality, the "CHSH inequality", applies to two systems on each of which two binary measurements can be made. It can be stated as follows:

$$\left|\frac{1}{4}\sum_{(q_1,q_2)\in\{0,1\}^2}\sum_{(a_1,a_2)\in\{0,1\}^2}(-1)^{a_1\oplus a_2=q_1\wedge q_2}p(a_1,a_2|q_1,q_2)\right| \leq \frac{3}{4}. \quad (1)$$

Quantum mechanics predicts that there exists four measurements (two on the first subsystem and two on the second) which when applied to a system initialized in the joint state $|\Psi\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ result in a distribution for which the left-hand side of (1) evaluates to $1/2 + \sqrt{2}/4 \approx 0.85$. Many Bell inequalities have since been introduced. More than 40 years of investigation, including the extensive use of numerical methods, have led to thousands of papers.[3] These investigations, however, have for the most part been confined to the study of small-scale examples, typically involving at most three subsystems and three or four measurement settings per system. This limitation reflects both the richness of entanglement and the difficulty of obtaining asymptotic results. It raises an obvious question: *What is the computational complexity of Bell inequalities?*

Surprisingly, it is only relatively recently that the question was first precisely formulated by Cleve et. al [CHTW04], who gave a re-interpretation of Bell inequalities in terms of *multiplayer games*. From their use in zero-knowledge proof systems [GMR85] to their role in the proof of the PCP theorem [AS98, ALM+98] multiplayer games have played a central role in computational complexity and cryptography throughout the past quarter century. A multiplayer game is run by the "referee", a trusted classical party, who interacts with $r \geq 2$ "players". The referee chooses questions $(q_1, \ldots, q_r) \in Q^r$ according to a distribution π, and sends question q_i to player i. The players each have to provide an answer a_i to the referee. The referee accepts or rejects the answers he receives according to a criterion $V(a_i|q_i) \in \{0,1\}$. The rules of the game, including π and V, are public and known to the players, who cooperate in order to win the game. The only restriction on their strategies is that the players are not allowed to exchange any information once the game has started.

In parallel to their use in complexity, multiplayer games have turned out to provide a surprisingly rich framework in which to pursue the study of entanglement initiated by Bell. The "no communication" condition placed upon the players has traditionally been interpreted as the formal requirement that the distribution $p(a_i|q_i)$ on answers that they generate should be a (convex combination of) product distributions. As demonstrated by Bell, however, entanglement *does not* allow for supraluminal communication (quantum mechanics does not violate relativity), but it *does* allow for the generation of distributions that cannot be expressed as the convex combination of product distributions. The violation of Bell inequalities by quantum mechanics implies the following: there exists games for which entangled-player strategies are strictly more powerful than classical (shared randomness) strategies. Denoting by $\omega^*(G)$ the *entangled value* of a game G (the maximum success probability of entangled-player strategies) and by $\omega(G)$ its *classical value* (the maximum success probability of classical players, restricted to using shared randomness as their sole source of correlation), we now know of games for which $\omega^*(G) = 1$ but $\omega(G)$ can be arbitrarily small [Ara02, Raz98].

The question formulated above can thus be restated as follows: *What is the complexity of computing $\omega^*(G)$?* An answer to this question for the case of the classical value $\omega(G)$ is precisely the content of the PCP theorem: $\omega(G)$ is NP-hard to approximate within a multiplicative constant, even for games with

[3] Google Scholar finds over 7000; more than 500 papers contain "Bell inequality"' in their title on the quant-ph arXiv alone.

two players and binary answers — in fact, it is even hard for so-called XOR games in which the referee's criterion V only depends on the parity of the two answers he receives [Hås01].[4] For the case of the entangled value, however, for a long time little was known. Indeed, nothing can be deduced directly from the classical case, as the sole fact that $\omega(G) \leq \omega^*(G) \leq 1$ does not obviously make the problem any easier or harder.

Interestingly, a series of works have pointed to the entangled problem being *easier* than the classical one, at least for restricted classes of two-player games. Cleve et al., building on work of Tsirelson [Tsi80], gave a polynomial-time algorithm based on the use of semidefinite programming for the exact computation of $\omega^*(G)$ for the case of XOR games [CHTW04]. Kempe et al. [KRT10] also used semidefinite programming to show the existence of an algorithm giving a factor 6 approximation to $1 - \omega^*(G)$ for the case of unique games. If one allows so-called *no-signalling* strategies, in which the distribution $p(a_i|q_i)$ is only limited by the condition that the marginal distribution on each subset of players' answers be independent from questions to the other players, then there is again a polynomial-time algorithm, this time based on a linear programming formulation of the problem [Pre07].

Could the computation, or at least approximation, of $\omega^*(G)$ be in BPP? In [KKM$^+$11, IKM09] it was shown that *exact* computation is NP-hard, even for two-player games with answers of length 2 from each player. Recently the first strong hardness of approximation result was obtained: the problem of approximating $\omega^*(G)$ to within inverse polylogarithmic accuracy for games with three players is NP-hard under quasi-polynomial reductions [IV12]. This result was obtained as a corollary of the complexity class inclusion NEXP $\subseteq$ MIP*, an entangled-prover analogue of the celebrated NEXP $\subseteq$ MIP [BFL91]. (Here MIP* is the class of languages that have multiprover interactive proof systems with entangled provers.)

The initial discovery of the power of multiple provers, characterized by the equation MIP = NEXP, quickly led to the first hardness of approximation results for problems such as clique and independent set [FGL$^+$96]. Obtaining tight hardness results for constraint satisfaction problems such as 3-SAT [Hås01], however, required much further work and the development of techniques such as low-degree tests [AS98, RS96], composition of verifiers [AS98], and the use of gadgets [BGS98]. Our main contribution is the extension of some of the most important of these techniques to the setting of entangled-player games.[5] We prove soundness of a variant of the low-degree test against entangled players, provide techniques enabling the composition of verifiers sound against entangled players, and analyze specific gadgets. Motivated by the goal of obtaining strong hardness of approximation results for the simplest possible classes of games, we show the following main result.

Theorem 1. *Let $\varepsilon > 0$ be an arbitrary constant. Given a 3-player XOR game G it is NP-hard to distinguish between $\omega(G) \geq 1 - \varepsilon$ and $\omega^*(G) \leq 1/2 + \varepsilon$. (Here the size of a game is measured as the number of possible triples of questions in the game.)*

As mentioned above, the inclusion NEXP $\subseteq$ MIP* [IV12] can readily be scaled down to a result on the hardness of approximating $\omega^*(G)$. Theorem 1 improves on this in the following ways. First, in [IV12] hardness is only obtained for approximation factors $(1 + 1/\operatorname{poly}(\log n))$. Amplifying this gap to a constant requires sequentially repeating the game a poly-logarithmic number of times and induces a corresponding blow-up in its size. Second, the scaling down from MIP* results in games which have questions and answers of length $\operatorname{poly}(\log n)$ and hence size, as measured by the total number of questions and answers, that is

[4] Here the input G is always given by an explicit table of values for the distribution π and the predicate V.

[5] Classically multiplayer games and PCPs provide two views on the same object. In the presence of entanglement the equivalence is less clear, and we prefer to work with games. See however [KRR13] for a possible definition of "no-signalling PCP" which naturally leads to a notion of "entangled PCP" equivalent to the games studied here.

super-polynomial. The games for which NP-hardness is established in Theorem 1 have questions of length $O(\log n)$ and answers consist of a single bit each.

In terms of Bell inequalities, our main theorem gives the optimal hardness of approximation for inequalities involving three or more systems; indeed no simpler form for such inequalities can be thought of than *correlation inequalities*, which are the equivalent of XOR games. Since such inequalities measure the bias $\beta^*(G) = 2\omega^*(G) - 1$ of a given XOR game, we can state the following immediate corollary of our main theorem.

Corollary 1.1. *Given an explicit description of a tripartite Bell correlation inequality, it is NP-hard to give any constant factor multiplicative approximation to the largest possible value that is allowed by quantum mechanics.*

In addition to the above-mentioned results we also show that for any constant $\delta > 0$ it is NP-hard to distinguish between $\omega(G) = 1$ and $\omega^*(G) < \delta$ for games with three players, constant (depending on δ) answer size, and such that furthermore the referee only asks questions to two out of the three players and the constraint he verifies is a projection constraint (the answer from one of the two players whom received questions completely determines a unique valid answer for the second).

We note that all our results only apply to games with three or more players. For the case of XOR games the above-mentioned result of Cleve et al. [CHTW04] shows that unless P=NP no hardness result can be expected when there are only two players. Showing hardness of approximation of $\omega^*(G)$ for two-player non-XOR games (even games with answers of length $O(\log n)$) remains a tantalizing open question (see "soundness of the low-degree test" below for additional discussion).

Techniques and proof overview

Our approach to proving hardness of approximation for entangled-player games is based on two main components. The first is a notion of *equivalence* (or, closeness) of entangled-player strategies that is appropriate to *composition*. In analyzing the soundness of a certain game, or test, our goal is to make a statement of the form "any *generic* strategy with success $1 - \varepsilon$ in the test must be ε'*-equivalent* to an *ideal* strategy", where the ideal strategy has precisely the type of structure that the test is trying to enforce (for instance, a strategy answering all questions according to a fixed low-degree polynomial). In the case of classical deterministic strategies it is natural to define strategies to be ε'-equivalent when they provide the same answer to all but a fraction at most ε' of questions. In the case of entangled — indeed, even randomized — strategies it is less obvious what the correct notion should be. In particular, it a priori seems impossible to consider single-player strategies by themselves, as e.g. the marginal distribution on answers that they induce could very well be perfectly uniform, for every possible question. In addition, the notion of equivalence chosen should be appropriate for composition: if one test (for instance, the low-degree test) calls another test as a sub-procedure (for instance, instead of checking directly a constraint $\varphi(x_1, \ldots, x_{10})$, the referee transforms φ into a 3-SAT formula over 10 variables and calls a sub-test specially designed for the efficient verification of small 3-SAT formulas), then it should be possible to effortlessly combine a soundness analysis of each of the two tests in a soundness analysis of the global test. We give a notion of equivalence that satisfies these requirements, demonstrating "by the example" that it is well-suited to composition.

The second component is a soundness analysis of the plane-vs-point low-degree test from [RS97] with entangled players. Establishing soundness of this test is crucial to obtaining an NP-hardness result for games of polynomial size, rather than quasi-polynomial as in [IV12]. Our analysis follows the same outline

as in [RS97],[6] but it requires substantial additional work. In particular, the key step of "consolidation" performed in almost all known soundness analyses of the low-degree test requires a deep overhaul, and its extension to entangled-player strategies is one of our main technical contributions.

We briefly expand on each of these two components below, pointing to the aspects of our proof that most differ from previous work done in the classical setting. We note that both components borrow heavily from techniques introduced in [IV12], and our contribution consists in an important extension and simplification of these techniques. We also note that our results make use of a recent parallel repetition theorem for entangled games [KV11], as well as (and independently from its use to obtain parallel repetition) of an "orthonormalization lemma" that played an important role in the proof of the parallel repetition theorem.

Equivalence of entangled-player strategies. Suppose given a certain game, or test, in which the players are required to answer questions $q \in Q$ with answers $a \in A$. For convenience we focus on a two-player game in which we can assume that both players use the same strategy, defined by a symmetric bipartite state $|\Psi\rangle$ and measurements $\{A_q^a\}_{a\in A}$ for every $q \in Q$. Let $\mathcal{F} \subseteq \{f : Q \to A\}$ be a set of functions having a certain desirable property (for instance, we could have $Q = \mathbb{F}^m$, $A = \mathbb{F}$, and $\mathcal{F}$ the family of all low-degree polynomials). Suppose the test is designed to verify that both players have the following ideal form: there exists a fixed $f \in \mathcal{F}$ such that, upon receiving question q, either player answers it with $f(q)$. Note that if the players are allowed the use of entanglement (or even shared randomness) then it is not realistic to hope for the existence of a *single* f underlying their strategy. Indeed, the players could use shared randomness to select a random $f \in \mathcal{F}$ before computing their answer $f(q)$; no test will distinguish this from an ideal deterministic strategy. We are thus led to the following natural broadening of what is allowed in terms of ideal strategy: there should exist a *self-consistent* measurement $M = \{M^f\}_{f\in\mathcal{F}}$ such that the players are *equivalent* to players whom first, measure their respective systems using M, obtaining an outcome f, and second, answer their question q with $f(q)$.

We define *consistent* and *equivalent*. The two notions are related. The measurement $\{M^f\}$ is said to be ε-self-consistent if the following holds:

$$\sum_f \langle\Psi|M^f \otimes M^f|\Psi\rangle \;\geq\; 1-\varepsilon.$$

What this means is simply that, whenever the two players each measure their respective systems using $\{M^f\}$, they get the same outcome except with probability ε. This is a natural requirement; indeed we are trying to mimic the deterministic case in which both players apply the same fixed function. To define a notion of equivalence we follow the approach from [IV12] and say that a generic strategy $(|\Psi\rangle, A)$ for the players is ε-equivalent to the ideal strategy $\{M^f\}$ if the following holds:

$$\mathrm{E}_{q\in Q} \sum_{a\in A} \sum_{f\in\mathcal{F}:\, f(q)\neq a} \langle\Psi|A_q^a \otimes M^f|\Psi\rangle \;\leq\; \varepsilon. \tag{2}$$

Note that (2) can be interpreted as requiring that both strategies, generic and ideal, are ε-consistent. At least two arguments point to this notion of equivalence through consistency being the "right" notion.

First, as should be obvious from the definition, a relation such as (2) can be directly linked to quantities that arise naturally in the analysis of a game or test. For instance, success in the plane-vs-point low-degree

[6] In contrast to [RS97], which was mostly concerned with obtaining a test with sub-constant error, we only analyze the low-error regime. Nevertheless, the analysis given in [RS97] (as detailed and refined in [MR08]) is well-suited to an extension to the case of entangled players.

test immediately implies consistency between the two families of measurements that define a generic entangled strategy for the players: a "points" measurement, designed to answer questions made of a single point, and a "planes" measurement, designed to answer questions about the restriction of the low-degree polynomial to a whole plane (we refer to Section 3 for more details). This makes the notion of equivalence defined through (2) particularly well-suited to the analysis of multiplayer games.

Second, equivalence obtained through consistency composes well. Suppose given a game obtained from the composition of two tests. In the game each player is asked a pair of questions (q_1, q_2). The first test is meant to verify that for every pair of questions (q_1, q_2) the players answer according to $f_{q_1} \in \mathcal{F} \subseteq \{f : Q_2 \to A\}$. The second step checks that the function f_{q_1} is obtained as $g(q_1)$ for some $g \in \mathcal{G} \subseteq \{g : Q_1 \to \mathcal{F}\}$. The composed test is meant to verify that the players each answer (q_1, q_2) with $(g(q_1))(q_2)$. That this will hold is clear if the players are deterministic and both tests are sound against deterministic strategies. We show (indeed it is a simple calculation) that it is also the case when the players may apply entangled strategies, provided the soundness analysis of each subtest is based on the notion of equivalence defined by (2).

Soundness of the low-degree test with entangled players. Recall that in the plane-vs-point low-degree test the referee chooses a uniformly random affine plane p in $\mathbb{F}^m$, where $\mathbb{F}$ is a large finite field and m an integer, sends p to one player and a uniformly random $\boldsymbol{x} \in p$ to the second, and expects as answers the description of a polynomial f of total degree at most d defined on p and a point $a \in \mathbb{F}$ respectively such that $f(\boldsymbol{x}) = a$. (See Figure 1 for a more detailed description of the test.) The goal of the soundness analysis is to show that any generic strategy for the players succeeding with probability at least $1 - \varepsilon$ in the test, for some small fixed $\varepsilon > 0$, is $\mathrm{poly}(\varepsilon)$-equivalent to an ideal strategy in which the set of functions $\mathcal{F}$ is the set $\mathcal{F}_{m,d}$ of m-variate polynomials over $\mathbb{F}$ with total degree at most d. The proof is by induction. First we show that for most lines $\ell \subseteq \mathbb{F}^m$ the players' strategy, when restricted to questions from ℓ, must be $\mathrm{poly}(\varepsilon)$-equivalent to an ideal strategy using polynomials in $\mathcal{F}_{1,d}$. Then we proceed to prove a similar statements for planes, cubes, etc., until the final statement is obtained for $\mathbb{F}^m$. This outline is common to most analyses of the low-degree test; details on the induction are given in Section 6.

Here we concentrate on a key difficulty that arises when analyzing entangled-player strategies. In all known proofs by induction of the low-degree test the closeness parameter ε blows up exponentially.[7] (The degree also increases, but we do not discuss this issue here.) In the classical, deterministic setting it is possible to argue directly using "robustness" properties of low-degree polynomials that δ-closeness for some sufficiently small δ implies ε'-closeness for some ε' depending only on ε (the failure probability in the test) but independent of δ (the error parameter reached after a number of induction steps). In the entangled-player setting such a statement does not hold. Intuitively, the reason for this is that while a given low-degree polynomial cannot be corrupted at a substantial fraction of points without drastically increasing its degree, for any δ it is possible to "corrupt" a measurement by any arbitrary amount δ, say by performing a small global rotation of the measurement operators. More precisely, (2) can fail for a number of reasons. While the measurement $\{M^f\}$ always outputs a low-degree polynomial, it does so probabilistically; hence the final probabilistic outcome $f(q)$ can fully agree with the first players' answer (when she measures using $\{A_q^a\}$) for most questions q, or partially agree for all q, or any combination in-between the two.

As a result, the measurements constructed throughout the induction must be modified at each step by performing an *active* correction procedure. Such a procedure was already the most technically challenging step in the proof of [IV12]. Here we build upon their work, but considerably improve and simplify their

[7] A notable exception is the proof technique from [AS97], which does not use induction but a more direct "bootstrapping" argument.

proof. The main idea is to define the "improved" measurement as the optimum of a particular semidefinite program — roughly, one that seeks to minimize (2) over all possible measurements $\{M^f\}$. Our analysis makes an important use of duality properties of that semidefinite program. As a result we are able to argue that, provided a reasonably good measurement exists (the one constructed by induction), then there must also exist a much better measurement, in the sense of having much higher consistency properties. However, the resulting measurement may not be defined on the whole Hilbert space (it is not hard to see that this is unavoidable). To overcome this we need to add a layer of recursion by performing the whole analysis again on the parts of the Hilbert space in which the previous step had resulted in un-recoverable failure. Further details on the consolidation procedure are given in Section 5.

We note that of all our analysis it is only the consolidation procedure that requires the presence of three players (indeed, the low-degree test itself can be defined for two players only). If its correctness was extended to the case of two players one would automatically obtain a hardness result for two-player entangled games. We were unable to achieve this: the fact that the players' entangled state is a tripartite symmetric state seems essential for our proof technique to go through.

Organization of the paper. We start with some useful preliminaries in Section 2. In Section 3 we introduce the main tests that we analyze: the low-degree test, its self-composition, a simple linearity test, and standard tests geared respectively at the verification of 3-SAT formulas and systems of quadratic equations. In Section 4 we prove Theorem 1 and other hardness of approximation results for entangled-player games, assuming the soundness analysis of the low-degree tests. Section 5 contains the consolidation procedure required to carry out the induction in the proof of soundness of the low-degree test. The latter is given in Section 6.

Acknowledgments. I am grateful to Dana Moshkovitz for helping me make my way through the classical literature on PCPs, including invaluable advice on the shortest path to obtaining constant-factor hardness of approximation results.

2 Preliminaries

2.1 Notation

For an integer K, denote $\{1,\ldots,K\}$ by $[K]$. Given a finite set X and an integer n, we sometimes use bold font to denote tuples $\boldsymbol{x} = (x_1,\ldots,x_n) \in X^n$. We also write $\boldsymbol{x}_{\leq i}$ for $(x_1,\ldots,x_i) \in X^i$, as well as $\boldsymbol{x}_{<i}$, $\boldsymbol{x}_{\geq i}$, etc. for the obvious tuples. When T is a finite set, we write $\mathrm{E}_{x\in T}$ for the expectation over a uniformly random element x of T. log denotes the logarithm taken in base 2. If B is a boolean variable, 1_B is 1 if B evaluates to true and 0 otherwise. We also let -1_B be 1 if B evaluates to true and 1 otherwise.

It will often be convenient to express "approximate inequalities" as

$$(E) \approx_\delta (F),$$

where here (E), (F) are two expressions that evaluate to complex numbers and $\delta > 0$ a parameter. What this means is that there exists a universal constant C (the constant may be different every time the symbol $\approx$ is used) such that $|(E) - (F)| \leq C\,\delta$.

Polynomials and finite fields. $\mathbb{F}$ will always denote a finite field. $\mathbb{F}_2$ is the finite field with two elements. For an integer m we let $z = (z_1, \ldots, z_m) \in \mathbb{F}^m$ denote a point, and $\vec{y} = (y_1, \ldots, y_m) \in \mathbb{F}^m$ a vector (the distinction is only semantic; in particular we allow $\vec{y} = 0$). Given z and $\vec{y}_i$ we let $(z; \vec{y}_i)$ denote the affine subspace of $\mathbb{F}^m$ containing all points of the form $z + \sum_i \alpha_i \vec{y}_i$, for $\alpha_i \in \mathbb{F}$. Given any such subspace we fix a canonical representation for it, and an associated coordinate system that makes it isomorphic to $\mathbb{F}^d$, where d is the dimension of the space spanned by the $\vec{y}_i$.

For an affine subspace s of $\mathbb{F}^m$ of dimension k and any $0 \leq j \leq k$ we let $\mathcal{S}_j(s)$ be the set of all j-dimensional affine subspaces of s. When s is clear from context (e.g. $s = \mathbb{F}^m$) we simply write $\mathcal{S}_j$ for $\mathcal{S}_j(s)$. For any affine space s, $\mathcal{P}_d(s)$ is the set of all degree-d polynomials defined on s (in particular, $\mathcal{P}_d(\mathbb{F}^m)$ is the set of all degree-d polynomials in m variables over $\mathbb{F}$). Any such polynomial can be represented by the list of its at most $(d+1)^m$ coefficients over $\mathbb{F}$. We recall the Schwartz-Zippel lemma [Zip79, Sch80], which we will use repeatedly.

Lemma 2.1 (Schwartz-Zippel)**.** *Let $d, m \geq 1$ be integers and p a non-zero polynomial in m variables of total degree at most d defined over the finite field $\mathbb{F}$. Then p has at most $d|\mathbb{F}|^{m-1}$ zeros.*

States and measurements. We use calligraphic letters, such as $\mathcal{H}$, to denote finite dimensional Hilbert spaces. For $z \in \mathcal{H}$, $\|z\|$ denotes its Euclidean norm. A *state* is a vector with unit norm. Given an integer $r \geq 1$ and a state $|\Psi\rangle \in \mathcal{H}^{\otimes r}$, we say that $|\Psi\rangle$ is permutation-invariant if $\sigma|\Psi\rangle = |\Psi\rangle$, where σ is the linear operator corresponding to any permutation of the r copies of $\mathcal{H}$ (sometimes also called "registers").

Given a permutation-invariant state $|\Psi\rangle$, we will often abuse notation and use the symbol ρ for the reduced density of $|\Psi\rangle$ on any one of the registers (permutation-invariance implies that all single-system reduced densities are identical), but also on any two, three, etc. registers. In particular, we also write $\rho = |\Psi\rangle\langle\Psi|$. It will always be clear from context which number of registers is meant. Given a density σ, we write $\mathrm{Tr}_\sigma(A)$ as shorthand for $\mathrm{Tr}(A\sigma)$. Hence, for instance we have the following equivalent ways of writing the same expression:

$$\langle\Psi| A \otimes \mathrm{Id} \otimes \cdots \otimes \mathrm{Id} |\Psi\rangle \;=\; \mathrm{Tr}_\rho\big(A \otimes \mathrm{Id} \otimes \cdots \otimes \mathrm{Id}\big) \;=\; \mathrm{Tr}_\rho\big(\mathrm{Id} \otimes A\big) \;=\; \mathrm{Tr}_\rho(A).$$

Let $\mathrm{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$, and $\|\cdot\|$ the operator norm on $\mathrm{L}(\mathcal{H})$. $\mathrm{Id} = \mathrm{Id}_{\mathrm{L}(\mathcal{H})}$ is the identity operator on $\mathcal{H}$. A *sub-measurement* on $\mathcal{H}$ is a finite set $A = \{A_i\}$ of non-negative definite operators on $\mathcal{H}$ such that $\sum_i A_i \leq \mathrm{Id}$. A *measurement* requires that $\sum_i A_i = \mathrm{Id}$.

Let $r \geq 2$ and $|\Psi\rangle$ be a permutation-invariant state on $\mathcal{H}^{\otimes r}$, i.e. $|\Psi\rangle$ is invariant under any permutation of its r subsystems. To $|\Psi\rangle$ we associate a bilinear form on $\mathrm{L}(\mathcal{H}) \times \mathrm{L}(\mathcal{H})$ by defining

$$\langle A, B\rangle_\Psi \;:=\; \langle\Psi| A \otimes B \otimes \mathrm{Id}^{\otimes(r-2)} |\Psi\rangle \;\in \mathbb{C} \tag{3}$$

for every $A, B \in \mathrm{L}(\mathcal{H})$. The permutation-invariance of $|\Psi\rangle$ implies that this expression is independent of the exact registers on which the A and B operators are applied (provided they are distinct). We also introduce a norm on $\mathrm{L}(\mathcal{H})$ by defining

$$\|A\|_\Psi \;:=\; \big(\langle\Psi| AA^\dagger \otimes \mathrm{Id}^{\otimes(r-1)} |\Psi\rangle\big)^{1/2}.$$

We note that the order $AA^\dagger$ matters, and one can define an inequivalent norm by ${}_\Psi\|A\|^2 := \langle\Psi| A^\dagger A \otimes \mathrm{Id}^{\otimes(r-1)} |\Psi\rangle$. We then have the following Cauchy-Schwarz inequality

$$\big|\langle A, B\rangle_\Psi\big| \;\leq\; \min\big\{\, \|A\|_\Psi \cdot {}_\Psi\|B\|\,,\, {}_\Psi\|A\| \cdot \|B\|_\Psi \big\} \;\leq\; \min\big\{\, \|A\|_\Psi \cdot \|B\|,\, \|B\|_\Psi \cdot \|A\| \big\}. \tag{4}$$

The following inequality will also prove useful: for any $A, X \in \mathrm{L}(\mathcal{H})$,

$$\|AX\|_\Psi \;\leq\; \|A\|_\Psi \cdot \|X\|. \tag{5}$$

Finally, we record the following claim for future use.

Claim 2.2. *Let $|\Psi\rangle$ be a permutation-invariant state on $r \geq 3$ registers, and $\{A^a\}$, $\{B^a\}$ two single-register measurements with outcomes in the same set A. Then*

$$\sum_a \big\|A^a - B^a\big\|_\Psi^2 \;\leq\; O\big(\sqrt{\delta}\big),$$

where

$$\delta := 1 - \sum_a \big\langle A^a, B^a \big\rangle_\Psi.$$

Proof. Expand

$$\sum_a \big\|A^a - B^a\big\|_\Psi^2 \;=\; \sum_a \Big(\mathrm{Tr}_\rho\big((A^a)^2\big) + \mathrm{Tr}_\rho\big((B^a)^2\big) - 2\,\Re\big(\mathrm{Tr}_\rho\big(A^aB^a\big)\big)\Big) \;\leq\; 2 - 2\sum_a \Re\big(\mathrm{Tr}_\rho\big(A^aB^a\big)\big).$$

It will suffice to lower bound the third term. We have

$$\begin{aligned}
\sum_a \mathrm{Tr}_\rho\big(A^aB^a\big) &= \sum_{a,b,c} \mathrm{Tr}_\rho\big(A^aB^a \otimes B^b \otimes A^c\big) \\
&\approx_{\sqrt{\delta}} \sum_a \mathrm{Tr}_\rho\big(A^aB^a \otimes B^a \otimes A^a\big) \\
&\approx_{\sqrt{\delta}} \sum_a \mathrm{Tr}_\rho\big(\,\mathrm{Id} \otimes B^a \otimes A^a\big) \\
&= 1 - \delta,
\end{aligned}$$

where the two approximate equalities follow by using the Cauchy-Schwarz inequality and the definition of δ twice each. □

Consistency parameters. The following definition will play an important role in the analysis.

Definition 2.3. *Let V be a set, for every $v \in V$ $\{A_v^a\}$ a sub-measurement with outcomes in $\mathbb{F}$, and $\{M^g\}$ a sub-measurement with outcomes in $\{g : V \to \mathbb{F}\}$. Let $M := \sum_g M^g$. We will say that*

- *M is δ-consistent with A if $\mathrm{E}_{v\in V} \sum_{g,a:\, g(v)\neq a} \mathrm{Tr}_\rho\big(M^g \otimes A_v^a\big) \;\leq\; \delta$,*
- *M is γ-projective if $\mathrm{Tr}_\rho\big(M \otimes (\mathrm{Id} - M)\big) \;\leq\; \gamma$,*
- *M is η-complete if $\mathrm{Tr}_\rho(M) \geq 1 - \eta$.*

2.2 Multiplayer games

We study one-round games played by $r \geq 2$ cooperative players against a referee.

Definition 2.4. *A game $G = G(r, \pi, V)$ is given by finite sets Q of* questions *and A of* answers*, together with a distribution $\pi : Q^r \to [0,1]$, and a function $V : A^r \times Q^r \to \{0,1\}$.*[8] *The* size *of the game is defined as $|G| = |Q||A|$.*[9]

The game G is played as follows: The referee samples $(q_1, \ldots, q_r)$ from Q^r according to π, and sends question q_i to player i. The players each reply with an answer $a_i \in A$. We say that the players win the game if $V(a_1, \ldots, a_r | q_1, \ldots, q_r) = 1$; otherwise they lose. The *value* of a game is the maximum winning probability of the players. The players can agree on a strategy before the game starts, but are not permitted to communicate after receiving their questions. We distinguish two different values, depending on the types of strategies allowed for the players: the *classical value* $\omega(G)$, corresponding to the maximum success probability of players using a classical deterministic strategy, and the *entangled value* $\omega^*(G)$, corresponding to the maximum success probability of quantum players allowed to use entanglement.

Definition 2.5. *Let $G = G(r, \pi, V)$ be a multi-player game. The classical value of G is defined as*

$$\omega(G) := \sup_{f_1,\ldots,f_r : Q \to A} \sum_{(q_1,\ldots,q_r) \in Q^r} \pi(q_1, \ldots, q_r) V\big(f_1(q_1), \ldots, f_r(q_r) | q_1, \ldots, q_r\big).$$

The entangled value of G is defined as

$$\omega^*(G) := \sup_{|\Psi\rangle, \{A^a_{i,q}\}} \sum_{(q_1,\ldots,q_r) \in Q^r} \pi(q_1, \ldots, q_r) \sum_{(a_1,\ldots,a_r) \in [A]^r} V(a_1, \ldots, a_r | q_1, \ldots, q_r) \langle \Psi | A^{a_1}_{1,q_1} \otimes \cdots \otimes A^{a_r}_{r,q_r} | \Psi \rangle,$$

where the supremum is taken over all finite-dimensional r-partite states $|\Psi\rangle$ and measurements (POVM) $\{A^a_{i,q}\}_{a \in A}$ for every $i \in [r]$ and $q \in Q$.

We will most often work with verifiers who treat all the players symmetrically. The next lemma shows that in that case we can always assume that the optimal players' strategy has the same symmetry.

Lemma 2.6. *Let $G = G(r, \pi, V)$ be a game such that $\pi(q_1, \ldots, q_r)$ is symmetric in $q_1, \ldots, q_r$ and V is symmetric under simultaneous permutation of the questions $(q_1, \ldots, q_r)$ and of the answers $(a_1, \ldots, a_r)$. Then given any strategy $P_1, \ldots, P_r$ with entangled state $|\Psi\rangle$ that succeeds with probability p in G, there exists a strategy $P'_1, \ldots, P'_r$ with entangled state $|\Psi'\rangle$ and success probability p such that $P'_1 = \ldots = P'_r$ and $|\Psi'\rangle$ is invariant with respect to any permutation of its r registers.*

Proof. Let $\mathfrak{S}_r$ be the set of permutations of $\{1, \ldots, r\}$ and assume, by appropriately padding with extra qubits, that all registers of $|\Psi\rangle$ have the same dimension. Define strategies $P'_1, \ldots, P'_r$ as follows: the players share the entangled state $|\Psi'\rangle = \sum_{\sigma \in \mathfrak{S}_r} |\sigma(1)\rangle \ldots |\sigma(r)\rangle \otimes |\Psi^\sigma\rangle$, where the register containing $|\sigma(i)\rangle$ is given to player i and $|\Psi^\sigma\rangle$ is obtained from $|\Psi\rangle$ by swapping the r registers according to σ. For $1 \le i \le r$ player i measures the register containing $|\sigma(i)\rangle$ and applies $P_{\sigma(i)}$. By symmetry of π and V this new strategy achieves the same winning probability p, and $|\Psi'\rangle$ has the required symmetry properties. □

3 Protocols

In this section we introduce different games (or "tests") played between the referee and r players. All tests treat the r players symmetrically, and as a consequence of Lema 2.6 we may assume players use a

[8] We write $V(\cdot, \cdot)$ as $V(\cdot|\cdot)$ to clarify the role of the inputs.

[9] This measure does not explicitly take into account the description size of π, which we always assume to be at most polynomial in $|G|$.

$(d, m, r, \mathbb{F})$ **low-degree test**

1. Let $d, m, \mathbb{F}$ be parameters given as input.
2. Choose a random $\boldsymbol{x} \in \mathbb{F}^m$ and two random directions $\vec{y}_1, \vec{y}_2 \in \mathbb{F}^m$. Automatically accept if the two vectors are not linearly independent. Otherwise, let s be the plane $(\boldsymbol{x}; \vec{y}_1, \vec{y}_2)$.
3. Select two players among r at random. Send s to the first, and $\boldsymbol{x}$ to the second.
4. Receive a bivariate degree-d polynomial g defined on s from the first player, and a value $a \in \mathbb{F}$ from the second.
5. Accept if and only if $g(\boldsymbol{x}) = a$.

Figure 1: The plane-vs-point low-degree test attempts to verify that the r players answer consistently with a degree-d polynomial defined over $\mathbb{F}^m$.

symmetric strategy; in particular their respective state can be represented using the same Hilbert space $\mathcal{H}$ for each player. In Section 3.1 we first introduce a variant of the *low-degree test*, a test that plays a key role in the construction of efficient PCPs. In Sections 3.2 and 3.4 we give standard tests respectively for the verification of the satisfiability of a 3-SAT formula and a system of quadratic equations in boolean variables. The latter uses a linearity test for functions $\mathbb{F}_2^n \to \mathbb{F}_2$ given in Section 3.3. We note that none of the tests we define is new and all have appeared previously in the PCP literature.

3.1 The low-degree test

3.1.1 A first protocol

The line-vs-point low-degree test was introduced in [RS96]. Here we analyze a variant from [RS97]. The test is called the "plane-vs-point" low-degree test because it calls for two players to send back the restriction of a low-degree polynomial to a plane and a point chosen randomly in that plane respectively. The test is described in Figure 1. We summarize its main properties.

Complexity. The longest question is the description of the affine plane s, which requires $3m \log |\mathbb{F}|$ bits. The longest answer is the degree-d bivariate polynomial g, which can be specified using at most $(d+1)^2 \log |\mathbb{F}|$ bits.

Strategies. A strategy for the players in the $(d, m, r, \mathbb{F})$ low-degree test is a triple $(|\Psi\rangle, A, C)$ where

- $|\Psi\rangle$ is a permutation-invariant state on $\mathcal{H}^{\otimes r}$,
- $A = \{A_{\boldsymbol{x}}^a\}$ is a set of "points" measurements $\{A_{\boldsymbol{x}}^a\}_{a \in \mathbb{F}}$ defined for every $\boldsymbol{x} \in \mathbb{F}^m$,
- $C = \{C_s^g\}$ is a set of "planes" measurements $\{C_s^g\}_{g \in \mathcal{P}_d(s)}$ defined for every $s \in \mathcal{S}_2(\mathbb{F}^m)$.

Analysis. We state the soundness of the test as a theorem. The proof is given in Section 6. Note that although the test is defined for any $r \geq 2$, the theorem requires $r \geq 3$.

Theorem 3.1. *Let $0 < \varepsilon \leq 1/2$, $d \geq 1, m \geq 2, r \geq 3$ integers, and $\mathbb{F}$ a finite field of size $|\mathbb{F}| = q$ such that $q \geq (dm/\varepsilon)^{d_1}$, where $d_1 \geq 1$ is a universal constant. Let $(|\Psi\rangle, A, C)$ be a strategy with success $1-\varepsilon$ in the $(d, m, r, \mathbb{F})$-low-degree test. Then there exists a measurement $\{M^g\}$ with outcomes $g \in \mathcal{P}_d(\mathbb{F}^m)$ such that*

$$\mathrm{E}_{\boldsymbol{x}\in\mathbb{F}^m} \sum_{g\in\mathcal{P}_d(\mathbb{F}^m)} \sum_{a\in\mathbb{F}:\, g(\boldsymbol{x})\neq a} \langle A^a_{\boldsymbol{x}}, M^g\rangle_\Psi \;\leq\; C_1\varepsilon^{c_1}, \tag{6}$$

where $c_1 \leq 1, C_1 > 0$ are universal constants.

Eq. (6) serves as a measure of distance between the provers' original strategy, defined by the measurements $A_{\boldsymbol{x}}$, and the new strategy defined by the single measurement M. The equation states that the two measurements are consistent in the sense that, if two players are simultaneously sent the same question $\boldsymbol{x}$, and the first determines his answer by applying the measurement $\{A^a_{\boldsymbol{x}}\}$ while the second first measures using $\{M^g\}$ and then returns $g(\boldsymbol{x})$, then the players will provide identical answers except with probability at most $C_1\varepsilon^{c_1}$. Hence provers succeeding in the low-degree test are in a sense "equivalent" to provers applying the measurement M to determine a low-degree polynomial g even *before* having looked at their question. We also note that using Claim 2.2 Eq. (6) is easily seen to imply the distance bound

$$\mathrm{E}_{\boldsymbol{x}\in\mathbb{F}^m} \sum_{a\in\mathbb{F}} \Big\| A^a_{\boldsymbol{x}} - \sum_{g\in\mathcal{P}_d(\mathbb{F}^m):\, g(\boldsymbol{x})=a} M^g \Big\|^2_\Psi \;=\; O\big(\varepsilon^{c_1/2}\big).$$

3.1.2 A test with reduced answer size

When the low-degree test is used the degree d will typically be poly-logarithmic in the input size, so that the answer length of the test described in Section 3.1.1 is poly-logarithmic as well. In this section we show how the previous test can be composed with itself to obtain a test with reduced answer length. The idea of composition was instrumental in the proof of the PCP theorem [AS98].

Let m, d, q be integers and $\mathbb{F}$ a field of size $|\mathbb{F}| = q$. We first describe how variable substitution (see e.g. [DFK$^+$11, Section 4.4]) can be used to map a degree-d polynomial g over $\mathbb{F}^2$ to a degree-d' polynomial g' over $\mathbb{F}^{m'}$, where $m' = d' := 2\lceil \log(d+1)\rceil$. For $i = 0, \ldots, \lceil \log(d+1)\rceil - 1$ introduce new variables $\tilde{x}_i := x^{2^i}, \tilde{y}_i := y^{2^i}$. Using the base-2 decomposition of k and ℓ, any monomial $x^k y^\ell$ can be written as a product of the $\tilde{x}_i$ and $\tilde{y}_j$, each appearing at most once. Let $g' \in \mathbb{F}[\tilde{x}_i, \tilde{y}_i]$ be such that $g' \to g$ (formally) when $\tilde{x}_i \to x^{b^i}, \tilde{y}_i \to y^{b^i}$. Let

$$\# : \begin{cases} \mathbb{F}^2 & \to & \mathbb{F}^{m'} \\ (x,y) & \mapsto & (x, x^2, \ldots, x^d, y, y^2 \ldots, y^d), \end{cases}$$

and note that for any $\boldsymbol{x} \in \mathbb{F}^2$, $g(\boldsymbol{x}) = g'(\#\boldsymbol{x})$.

For any number $r \geq 2$ of players, the $(d, m, r, \mathbb{F})$ two-level low-degree test is described in Figure 2. We summarize its main properties.

Complexity. The longest question is the pair (s, s'), which is $3m \log|\mathbb{F}| + 3m' \log|\mathbb{F}| \leq 6m \log|\mathbb{F}|$ bits. The longest answer is the polynomial g', which can be specified using at most $(d')^2 \log|\mathbb{F}| = O((\log d)^2 \log|\mathbb{F}|)$ bits.

$(d, m, r, \mathbb{F})$ **two-level low-degree test**

1. Let $d, m, \mathbb{F}$ be parameters given as input. Set $d' = m' := 2\lceil \log(d+1) \rceil$.
2. The referee chooses a random $\boldsymbol{x} \in \mathbb{F}^m$ and two random directions $\vec{y}_1, \vec{y}_2 \in \mathbb{F}^m$. He automatically accepts if $\vec{y}_1, \vec{y}_2$ are not linearly independent. Let $s := (\boldsymbol{x}; \vec{y}_1, \vec{y}_2)$ be the corresponding affine plane.
3. The referee chooses a random $\boldsymbol{x}' \in \mathbb{F}^{m'}$ and two random directions $\vec{y}'_1, \vec{y}'_2 \in \mathbb{F}^{m'}$. He automatically accepts if $\vec{y}'_1, \vec{y}'_2$ are not linearly independent. Let $s' := (\boldsymbol{x}'; \vec{y}'_1, \vec{y}'_2)$ be the corresponding affine plane.
4. The referee selects two players at random, and performs one of the following two tests, with probability $1/2$ each.
   - 4.1 The referee sends $\boldsymbol{x}$ to the first player and and $(s, \#\boldsymbol{x})$ to the second. He receives answers $a \in \mathbb{F}$ and $a' \in \mathbb{F}$ respectively, and rejects if $a \neq a'$.
   - 4.2 The referee sends the pair (s, s') to the first player and $(s, \boldsymbol{x}')$ to the second. The first player answers with a degree-d' bivariate polynomial g' over s' and the second with a value $a' \in \mathbb{F}$. The referee rejects if $g'(\boldsymbol{x}') \neq a'$.
5. If the referee has not rejected then he accepts.

Figure 2: The $(d, m, r, \mathbb{F})$ two-level low-degree test attempts to verify that the r players answer consistently with a degree-d polynomial defined over $\mathbb{F}^m$. Note that queries to the second player in steps 4.1 and 4.2 are identically distributed, so that the players cannot distinguish which test is being performed.

Strategies. The players have the following measurements. For every $\boldsymbol{x} \in \mathbb{F}^m$, a "points" measurement $\{A^a_{\boldsymbol{x}}\}_{a\in\mathbb{F}}$. For every plane $s \in \mathcal{S}_2(\mathbb{F}^m)$ and every $\boldsymbol{x}' \in s$ (where $\boldsymbol{x}'$ is represented as $\#\boldsymbol{x}$ for some $\boldsymbol{x} \in s$), another points measurement $\{B^a_{s,\boldsymbol{x}}\}_{a\in\mathbb{F}}$. For every plane $s \in \mathcal{S}_2(\mathbb{F}^m)$ and every plane $s' \in \mathcal{S}_2(\mathbb{F}^{m'})$, a "planes" measurement $\{C^g_{s,s'}\}$. where g is a degree-d' bivariate polynomial defined on s'.

Analysis. We state the soundness of the test as a theorem. The proof is given in Section 6.6.

Theorem 3.2. *Let $0 < \varepsilon \leq 1/2$, $d \geq 1, m \geq 2, r \geq 3$ integers, and $\mathbb{F}$ a finite field of size $|\mathbb{F}| = q$ such that $q \geq (dm/\varepsilon)^{d_2}$, where $d_2 \geq 1$ is a universal constant. Let $(|\Psi\rangle, A, B, C)$ be an r-player strategy with success $1-\varepsilon$ in the $(d, m, r, \mathbb{F})$ two-level low-degree test. Then there exists a measurement $\{M^g\}$ with outcomes $g \in \mathcal{P}_{dd'}(\mathbb{F}^m)$ such that*

$$\mathrm{E}_{\boldsymbol{x}\in\mathbb{F}^m} \sum_{g\in\mathcal{P}_{dd'}(\mathbb{F}^m)} \sum_{a\in\mathbb{F}:\, g(\boldsymbol{x})\neq a} \langle A^a_{\boldsymbol{x}}, M^g\rangle_\Psi \leq C_2\varepsilon^{c_2},$$

where $c_2 \leq 1, C_2 > 0$ are universal constants.

3.2 The 3-SAT test

Let φ be a 3-SAT formula with n variables and $\mathrm{poly}(n)$ clauses. Let $h = \lceil \log n \rceil$ and $m = \lceil \log n / \log\log n \rceil$, so that $(h+1)^m \geq n$. Let $\mathbb{F}$ be a field of size $|\mathbb{F}| = q \geq h+1$, and identify $[n]$ with the subset $\{0,\ldots,h\}^m \subseteq \mathbb{F}^m$. Let $d := mh$. In the test, the players are supposed to hold a degree-d polynomial g over $\mathbb{F}^m$ obtained as the low-degree extension of a satisfying assignment to the variables of φ: g is the unique m-variate polynomial of degree at most h in each variable such that $g(\boldsymbol{x}) = x$ for every $\boldsymbol{x} \in \{0,\ldots,h\}^m$ associated to the variable x (see e.g. [BFLS91, Proposition 4.1] for a proof of existence and unicity).

A degree-4 curve c in $\mathbb{F}^m$ is specified by m univariate polynomials of degree at most 4 over $\mathbb{F}$, $(c_1,\ldots,c_m)$. The restriction of g to c is a univariate polynomial $g_{|c}(t) = g(c_1(t),\ldots,c_m(t))$ of degree at most $4d$. Using variable substitution as in Section 3.1.2, $g_{|c}$ can also be thought of as a polynomial of degree d' in $\mathbb{F}^{m'}$, where $d' = m' = \lceil \log(4d+1) \rceil$. Let $\# : \mathbb{F} \to \mathbb{F}^{m'}$ be the map which performs the variable substitution. The $(\varphi, n, r, \mathbb{F})$ 3-SAT test is described in Figure 3. We note that the use of curves to aggregate the values of a polynomial at different points is standard in the PCP litterature; see e.g. [MR10].

Complexity. The maximum question length is $O(m \log |\mathbb{F}|)$: it is $O(m \log |\mathbb{F}|)$ in the two-level low-degree test, and in step 2.2 the longest question is the curve c which takes at most $m \cdot 4 \log |\mathbb{F}|$ bits to specify. The two-level low-degree test has answer length $O((\log d)^3 \log |\mathbb{F}|)$. The polynomial $g \in \mathcal{P}_{4d'}(c')$ in step 2(b)ii requires $4d' \log |\mathbb{F}|$ bits. Overall, the answer length is $O((\log\log n)^3 \log |\mathbb{F}|)$.

Strategies. The players have a state $|\Psi\rangle$, measurements (A, B, C) corresponding to a strategy in the $(d, m, r, \mathbb{F})$ two-level low-degree test, for every degree-4 curve c in $\mathbb{F}^m$ and $\boldsymbol{w} \in c$ (specified as a point in $\mathbb{F}^{m'}$) a measurement $\{D^a_{c,\boldsymbol{w}}\}_{a\in\mathbb{F}}$, and finally for every degree-4 curve c' in $\mathbb{F}^{m'}$, a "curve" measurement $\{F^g_{c,c'}\}$, where $g \in \mathcal{P}_{4d'}(c')$.

Analysis. It is clear that if φ is satisfiable then the players have a perfect strategy that does not use any entanglement. They can simply define a polynomial g as the degree-d extension of a satisfying assignment to φ, and answer the two-level low-degree test according to g. If a player is asked a query of the form $(c, \#w)$ he answers with $g(w)$. If he is asked for (c, c') he answers with the restriction of g to the curve c',

$(\varphi, n, r, \mathbb{F})$ 3-**SAT test**

1. Let $h = \lceil \log n \rceil$, $m = \lceil \log n / \log\log n \rceil$, $d = mh$, and $d' = m' = \lceil \log(4d+1) \rceil$.
2. Do each of the following with probability $1/2$ each:
   - 2.1 Perform the $(d, m, r, \mathbb{F})$ two-level low-degree test.
   - 2.2 Pick a clause $C \in \varphi$ at random. Let $x, y, z \in [n]$ be the three variables in φ, and $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ the associated points in $\mathbb{F}^m$. Let $\boldsymbol{w}$ be a random point in $\mathbb{F}^m$ and c the degree-4 curve through $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w})$. Do each of the following with probability $1/2$ each:
     - 2.2.1 Select two players at random. Send $\boldsymbol{w}$ to the first, receiving $a \in \mathbb{F}$ as answer, and $(c, \#\boldsymbol{w})$ to the second, receiving $a' \in \mathbb{F}$ as answer. Reject if $a \neq a'$.
     - 2.2.2 Pick a random $\boldsymbol{w}' \in \mathbb{F}^{m'}$, and select two players at random. Send $(c, \boldsymbol{w}')$ to the first, receiving $a \in \mathbb{F}$, and (c, c') to the second, where $c' \subseteq \mathbb{F}^{m'}$ is the degree-4 curve going through $(\#\boldsymbol{x}, \#\boldsymbol{y}, \#\boldsymbol{z}, \boldsymbol{w}')$, receiving $g \in \mathcal{P}_{4d'}(c')$ as answer. Reject if $(g(\#\boldsymbol{x}), g(\#\boldsymbol{y}), g(\#\boldsymbol{z}))$ is not a satisfying assignment to the variables in clause C, or if $g(\boldsymbol{w}') \neq a$.

Figure 3: The $(\varphi, n, r, \mathbb{F})$ 3-SAT test attempts to verify that the r players answer consistently with a degree-d polynomial over $\mathbb{F}^m$ that is the low-degree extension of a satisfying assignment for φ (encoded in the values of g on $\{0, 1, \ldots, h\}^m$).

seen as a univariate polynomial of degree at most $4d'$ defined on $c' \subset c \approx \mathbb{F}^{m'}$. We state the soundness of the test as the following theorem. The theorem is proved in Section 7.1.

Theorem 3.3. *Let $0 < \varepsilon \leq K_3$, where $K_3 > 0$ is a universal constant, φ a 3-SAT formula on $n \geq 3$ variables, $r \geq 3$ and $\mathbb{F}$ a field of size $|\mathbb{F}| = q$ such that $q \geq (\log n/\varepsilon)^{d_3}$, where d_3 is a universal constant. Let $(|\Psi\rangle, A, B, C, D, F)$ be an r-player strategy with success $1-\varepsilon$ in the $(\varphi, n, r, \mathbb{F})$ SAT test. Then there is an assignment to the variables in φ that satisfies all but a fraction at most $C_3\varepsilon^{c_3}$ of the clauses, where $C_3 > 0, 0 < c_3 \leq 1$ are universal constants.*

3.3 The linearity test

Let n be an integer and $\mathbb{F}_2$ the field with two elements. The (n, r) linearity test uses $r \geq 3$ players and is described in Figure 4.

Complexity. Questions have length n and answers are a single bit.

Strategies. A strategy for the players in the (n, r) linearity test is given by a state $|\Psi\rangle$ and a family of measurements $\{A_x^a\}$ with outcomes $a \in \mathbb{F}_2$.

Analysis. The linearity test was first introduced in [BLR93] in the classical setting. The analysis with entangled players is joint work of the author and Tsuyoshi Ito [Vid11].

(n, r) **linearity test**

1. The referee chooses $x, y \in \mathbb{F}_2^n$ uniformly at random. He selects three players at random and sends them $x, y, x + y$ respectively.
2. The players answer with $a, b, c \in \mathbb{F}_2$ respectively. The referee accepts if and only if $c = a + b$.

Figure 4: The linearity test attempts to verify that the r players answer consistently with a linear function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

Theorem 3.4. *Let n be an integer, $r \geq 3$, $\varepsilon > 0$ and $(|\Psi\rangle, A)$ a strategy for the players in the (n, r) linearity test. There exists a measurement $\{M^u\}$ with outcomes $u \in \mathbb{F}_2^n$ such that*

$$\mathrm{E}_{x \in \mathbb{F}_2^n} \sum_{\substack{u \in \mathbb{F}_2^n, a \in \mathbb{F}_2 \\ a \neq u \cdot x}} \langle M^u, A_x^a \rangle_\Psi \;=\; O(\sqrt{\varepsilon}).$$

3.4 The QUADEQ test

Let QUADEQ be the language consisting of all systems of quadratic equations over $\mathbb{F}_2$ that are satisfiable. An instance of QUADEQ over n variables x_i is thus a set of $K = \mathrm{poly}(n)$ quadratic equations of the form

$$\sum_{i,j \in [n]} a_{ij}^{(k)} x_i x_j \;=\; c^{(k)} \qquad (\mathrm{mod}\, 2),$$

for $k = 1, \ldots, K$, that are simultaneously satisfiable. QUADEQ is well-known to be NP-complete. Here we recall a standard test for verifying membership in QUADEQ (see e.g. [AB09, Theorem 11.19]). Let φ be an instance of QUADEQ on n variables and $r \geq 3$. Looking ahead, we assume that the variables of φ are partitioned into two chunks of $n' = n/2$ variables each, labeled ℓ_1 and ℓ_2 (the labels will be used to identify the chunks among a larger universe of variables). The (φ, n, r) QUADEQ test is described in Figure 5.

Complexity. The maximal question length is n^2 plus the length of the labels. The answer length is one bit.

Strategies. The players have a state $|\Psi\rangle$, for each label ℓ_i measurements $A_i \equiv A_{\ell_i}$ corresponding to a strategy in the $(n/2, r)$ linearity test, and for each pair of labels (ℓ_1, ℓ_2) measurements $B \equiv B_{\ell_1,\ell_2}$ and $C \equiv C_{\ell_1,\ell_2}$ corresponding to strategies in the (n, r) and (n^2, r) linearity tests respectively.

Analysis. Suppose φ is satisfiable, and let $x = (x_1, x_2)$, where $x_i \in \mathbb{F}_2^{n/2}$ contains the assignment to variables from chunk ℓ_i, be a satisfying assignment. Then the players have a perfect strategy that does not use any entanglement. For this, they answer a query of the form (ℓ_i, u) with $u \cdot x_i$; a query of the form (ℓ_1, ℓ_2, v), where $v \in \mathbb{F}_2^n$, with $v \cdot (x_1, x_2)$; a query of the form (ℓ_1, ℓ_2, w), where $w \in \mathbb{F}_2^{n^2}$, with $w \cdot ((x_1, x_2) \otimes (x_1, x_2))$. We state the soundness of the test as the following lemma. The lemma is proved in Section 7.2.

(φ, n, r) **QUADEQ test**

1. The referee performs each of the following with probability $1/4$ each:

   1.1 With probability $1/4$ each, do the following:

      1.1.1 Send label ℓ_1 to three players chosen at random and perform the $(n/2, r)$ linearity test.

      1.1.2 Same with label ℓ_2.

      1.1.3 Send labels (ℓ_1, ℓ_2) to three players chosen at random and perform the (n, r) linearity test.

      1.1.4 Same but perform the (n^2, r) linearity test.

   1.2 Select random $u, v \in \mathbb{F}_2^{n/2}$ and send $(\ell_1, u), (\ell_2, v), (\ell_1, \ell_2, (u, v))$ to three players chosen at random. Receive a, b, c respectively and reject if $a + b \neq c$.

   1.3 Select two random vectors $u, v \in \mathbb{F}_2^n$. Send $(\ell_1, \ell_2, u), (\ell_1, \ell_2, v), (\ell_1, \ell_2, u \otimes v)$ to three players chosen at random. Verify that their answers (a, b, c) satisfy $a \cdot b = c$.

   1.4 Select a random vector $v \in \mathbb{F}_2^K$ and let $w = \sum_k w_k a^{(k)} \in \mathbb{F}_2^{n^2}$. Send (ℓ_1, ℓ_2, w) to a randomly chosen player, and check that the answer $a = \sum_k w_k c^{(k)}$.

Figure 5: The QUADEQ test attempts to verify that the r players answer consistently with functions $f_{\ell_1}, f_{\ell_2} : \mathbb{F}_2^{n/2} \to \mathbb{F}_2$ and $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $g : \mathbb{F}_2^{n^2} \to \mathbb{F}_2$ such that $f(x_1, x_2) = f_{\ell_1}(x_1) + f_{\ell_2}(x_2)$ and $g = f \otimes f$.

Lemma 3.5. *Let $0 < \varepsilon \leq K_4$, where $K_4 > 0$ is a universal constant, φ a QUADEQ instance on $n \geq 2$ variables and $r \geq 3$. Let $(|\Psi\rangle, A, B, C)$ be an r-player strategy with success $1 - \varepsilon$ in the (φ, n, r) QUADEQ test. Then φ is satisfiable. Moreover, suppose given a collection of QUADEQ instances $\varphi_1, \ldots, \varphi_T$, each acting on a pair of chunks of variables chosen from a common universe $\{x_1, \ldots, x_S\}$, where $x_i \in \mathbb{F}_2^{n/2}$. Let $(|\Psi\rangle, (A_i), (B_{i,j}), (C_{i,j}))$ be such that for every $t \in \{1, \ldots, T\}$ the strategy $(|\Psi\rangle, A_i, B_{i,j}, C_{i,j})$, where φ_t is over chunks x_i and x_j, has success $1 - \varepsilon$ in the (φ_t, n, r) QUADEQ test. Then there exists measurements $\{M_i^{x_i}\}_{x_i \in \mathbb{F}_2^{n/2}}$, for every $i \in \{1, \ldots, S\}$, such that for every φ_t on (x_i, x_j) it holds that*

$$\sum_{(x_i, x_j) \vdash \varphi_t} \langle M_i^{x_i}, M_j^{x_j} \rangle_\Psi \geq 1 - C_4 \varepsilon^{c_4},$$

where $(x_i, x_j) \vdash \varphi_t$ means that the assignment (x_i, x_j) satisfies φ_t and $0 < c_4 \leq 1$, $C_4 > 0$ are universal constants.

Note that the "furthermore" part of the lemma does not claim that the system $\{\varphi_t\}_{t=1,\ldots,T}$ is simultaneously satisfiable.

4 Hardness results

In this section we prove our main theorem, Theorem 1, which is restated as Corollary 4.4 below. In Section 4.1 we state a first hardness result that follows almost directly from the 3-SAT test from Section 3.2, whose analysis depends on the (composed) low-degree test from Section 3.1.2. In Section 4.2 we use the QUADEQ test from Section 3.4 to obtain a hardness result for games with constant answer size. In

Section 4.3 we apply the parallel repetition theorem from [KV11] to amplify the resulting hardness of approximation factor. Finally, our main theorem is proven in Section 4.4.

4.1 The basic hardness result

Our first hardness result is the following.

Theorem 4.1. *There is an $\varepsilon > 0$ such that the following holds. Given a 3-player game G in explicit form, it is NP-hard to distinguish between $\omega(G) = 1$ and $\omega^*(G) \leq 1 - \varepsilon$. Furthermore, the problem is still NP-hard when restricting to games G of size n such that the following hold:*

- *Questions have length $O(\log n)$ and answers length $\mathrm{poly}(\log \log n)$,*
- *The referee treats all players symmetrically and only sends questions to two out of the three players,*
- *The referee's test is a projection test: among the two players who receive a question, there is one whose answer determines a unique correct answer for the other.*

Proof. The proof of the theorem follows from the analysis of the 3-SAT test given in Theorem 3.3. First recall that the PCP theorem shows that there exists an $\varepsilon_1 > 0$ such that it is NP-hard to distinguish between a 3-SAT formula being satisfiable or the formula having at most a fraction $1 - \varepsilon_1$ of its clauses simultaneously satisfied (see e.g. [ALM+98, BGLR93, Hås01]). Let n be an integer, $\varepsilon_2 = \min(K_3, (\varepsilon_1/C_3)^{1/c_3})$ and $\mathbb{F}$ a finite field of size $q \in [(\log n/\varepsilon_1)^{d_3}, 2(\log n/\varepsilon_1)^{d_3}]$. Given a 3-SAT formula φ, let G_φ be the 3-player game corresponding to the $(\varphi, n, 3, \mathbb{F})$ 3-SAT test. With our choice of q the question length in G_φ is $O(\log n)$ and the answer length $O((\log \log n)^4)$; in particular the size of G_φ is polynomial in n. Furthermore it is clear that an explicit description of G_φ can be computed in polynomial time from φ.

If φ is satisfiable then $\omega(G_\varphi) = 1$. Furthermore, Theorem 3.3 implies that if $\omega^*(G_\varphi) > 1 - \varepsilon_2$ then (by definition of ε_2) there is an assignment satisfying more than a fraction $1 - \varepsilon_1$ of the clauses of φ. Hence deciding between $\omega(G_\varphi) = 1$ and $\omega^*(G_\varphi) \leq 1 - \varepsilon_2$ is at least as hard as deciding between φ being satisfiable and φ having at most a fraction $1 - \varepsilon_1$ of its clauses satisfiable. □

4.2 Hardness for games with constant answer size

In this section we combine Theorem 4.1 with the QUADEQ test from Section 3.4 to obtain a hardness result for games with binary answers.

Corollary 4.2. *There is an $\varepsilon > 0$ such that the following holds. Given a 3-player game G in explicit form in which answers from the players are restricted to a single bit each, it is NP-hard to distinguish between $\omega(G) = 1$ and $\omega^*(G) \leq 1 - \varepsilon$.*

Proof. Let φ be a 3-SAT formula on n variables, and $G_1 = G_\varphi$ and $\varepsilon_1 > 0$ the 3-player game whose existence follows from Theorem 4.1: if φ is satisfiable then $\omega(G_1) = 1$ whether if φ is not satisfiable then $\omega^*(G_1) \leq 1 - \varepsilon_1$. We show the existence of a 3-player game G_2 with binary answers and an $\varepsilon_2 > 0$ such that if φ is satisfiable then $\omega(G_2) = 1$ whether if φ is not satisfiable then $\omega^*(G_2) \leq 1 - \varepsilon_2$. Furthermore, G_2 can be computed in polynomial time from G_1.

Let Q be the set of all questions that can be asked in the game G_1, and π the distribution on $Q \times Q$ with which pairs of questions are chosen (recall that even though the game involves three players, only two questions are asked simultaneously). Let $m = \mathrm{poly}(\log \log n)$ be the maximal length of an answer in G_1, and write $A = \{0,1\}^m$ for the set of all possible answers. For every $(q_1, q_2) \in Q \times Q$ the referee in G_1

expects a pair of answers $(a_1, a_2) \in A \times A$. He then verifies a certain condition $V(a_1, a_2|q_1, q_2) \in \{0, 1\}$. Using NP-completeness of QUADEQ, this condition can be expressed as an instance ψ_{q_1,q_2} of QUADEQ over $2m + m'$ variables. Here the first $2m$ variables correspond to the bits of a_1 and a_2. The additional m' variables are auxiliary variables used in the reduction transforming $V(\cdot, \cdot|q_1, q_2)$ in an instance of QUADEQ. Technically the QUADEQ test should be modified to take into account these auxiliary variables. However, the way to do this is quite standard (see e.g. [AB09, Corollary 22.13] for details) and for simplicity in this outline we ignore the role played by the auxiliary variables and assume $m' = 0$. The $2m$ variables can then be split into two chunks of variables, such that the first chunk is associated to a_1 and the second to a_2. Hence we may think of each QUADEQ instance ψ_{q_1,q_2} obtained from $(q_1, q_2) \in Q \times Q$ as acting on two chunks of variables taken from a universe of chunks of m binary variables, each labelled using a unique label $\ell(q)$ associated to a single question $q \in Q$. From a classical deterministic strategy in G_1 one can construct an assignment to the variables in all chunks satisfying a fraction of instances ψ_{q_1,q_2} equal to the success probability of the strategy in G_1.

Consider the following game G_2:

1. The verifier samples questions (q_1, q_2) as in G_1.
2. The verifier runs the $(\psi_{q_1,q_2}, m, 3)$ QUADEQ test, where the labels are $\ell_1 = \ell(q_1)$ and $\ell_2 = \ell(q_2)$.
3. The verifier accepts if and only if the QUADEQ test accepts.

First we note that the length of questions in G_2 is at most twice that of G_1 (for the labels) plus the square of the answer lengths in G_1, so it is $O(\log n)$. The answer length is a single bit. Hence the size of G_2 is polynomial in the size of G_1.

The discussion above shows that if $\omega(G_1) = 1$ then $\omega(G_2) = 1$ as well; in fact it more generally holds that $\omega(G_2) \geq \omega(G_1)$. Conversely, suppose that $\omega^*(G_2) \geq 1 - \varepsilon_2$ where $\varepsilon_2 > 0$ is to be specified later. Using Markov's inequality, for a fraction at least $1 - \sqrt{\varepsilon_2}$ of pairs (q_1, q_2) (chosen according to π) the players have success at least $1 - \sqrt{\varepsilon_2}$ in the $(\psi_{q_1,q_2}, m, 3)$ QUADEQ test. Provided ε_2 is small enough, the "furthermore" part of Lemma 3.5 shows the existence of a family of measurements $\{M_q^a\}_{a \in A}$ such that for each of the "good" pairs (q_1, q_2) it holds that

$$\sum_{(a_1,a_2):\, V(a_1,a_2|q_1,q_2)=1} \langle M_{q_1}^{a_1}, M_{q_2}^{a_2} \rangle_\Psi \;=\; 1 - O\big(\varepsilon_2^{c_4/2}\big).$$

It is then immediate that the strategy $(|\Psi\rangle, \{M_q^a\})$ is a strategy for the players in game G_1 with success probability at least $1 - O\big(\varepsilon_2^{c_4/2}\big)$, which can be made larger than $1 - \varepsilon_1$ provided ε_2 is chosen small enough. □

4.3 Amplifying the gap

The constant ε for which we established NP-hardness in Corollary 4.2 can be very small. In this section we show that the entangled-player parallel repetition theorem from [KV11] can be applied to obtain the following.

Corollary 4.3. *Let $\delta > 0$ be an arbitrary constant. Then the following is NP-hard. Given a 3-player game G in explicit form, distinguish between $\omega(G) = 1$ and $\omega^*(G) \leq \delta$. Furthermore, the problem is still NP-hard when restricting to games G of size n such that the following hold:*

- *Questions in G have length $O(\log n)$ and answers have length $\mathrm{poly}(\delta^{-1})$,*
- *The referee treats all players symmetrically and only sends questions to two out of the three players.*

Proof. Let φ be a 3-SAT formula on n variables, and $G_1 = G_\varphi$ and $\varepsilon > 0$ the 3-player binary game whose existence follows from Corollary 4.2: if φ is satisfiable then $\omega(G_1) = 1$ whether if φ is not satisfiable then $\omega^*(G_1) \leq 1 - \varepsilon$. We show the existence of a 3-player game G_2 having the properties described in the theorem and such that if φ is satisfiable then $\omega(G_2) = 1$ whether if φ is not satisfiable then $\omega^*(G_2) \leq \delta$. Furthermore, an explicit description of G_2 can be computed from G_1 in time polynomial in $|G_1|$ and exponential in $\varepsilon^{-1}, \delta^{-1}$.

First consider the following 3-player game G_1':

- The referee samples a triple of questions (q, q', q'') as in G_1.
- He chooses two players at random, sends (q, q', q'') to the first and one of q, q', q'', chosen at random among the three possibilities, to the second.
- The referee receives answers (a, a', a'') from the first player and b from the second. He accepts if and only if (a, a', a'') would have been accepted as answers to (q, q', q'') in G_1, and b equals the answer from the first player matching the question sent to the second player.

It is clear that $\omega(G_1) = 1 \implies \omega(G_1') = 1$. Suppose $\omega(G_1') \geq 1 - \varepsilon'$, where $\varepsilon' > 0$ is a small constant to be specified later. Let $(|\Psi\rangle, A_{q,q',q''}, B_q)$ be a strategy for the players with success $1 - \varepsilon'$ in G_1'. We argue that, provided ε' is chosen small enough, $(|\Psi\rangle, B_q)$ has success at least $1 - \varepsilon$ in G_1. For every question q and answer a let

$$A_q^a := \mathrm{E}_{(q',q'')} \sum_{a',a'':V(a,a',a''|q,q',q'')=1} A_{q,q',q''}^{a,a',a''},$$

where the expectation is taken according to the marginal distribution on questions (q', q'') when q is fixed (note that the position in which q is placed does not matter as the distribution π on questions in G_1 is symmetric). The test performed by the referee in game G_1' enforces that $\{A_q^a\}$ is a sub-measurement such that both[10]

$$\mathrm{E}_q \sum_a \langle A_{q'}^a, \mathrm{Id} \rangle_\Psi \geq 1 - \varepsilon' \qquad \text{and} \qquad \mathrm{E}_q \sum_a \langle A_{q'}^a, B_q^a \rangle_\Psi \geq 1 - \varepsilon'. \tag{7}$$

In particular, applying Claim 2.2 we have that

$$\mathrm{E}_q \sum_a \left\| A_q^a - B_q^a \right\|_\Psi^2 = O\left(\sqrt{\varepsilon'}\right). \tag{8}$$

[10] We refer to Section 2 for an introduction to the notation used here.

As a consequence, we can write the following

$$\begin{aligned}
\omega^*(G_1) &\geq \mathrm{E}_{(q,q',q'')} \sum_{\substack{(a,a',a'')\\ V(a,a',a''|q,q',q'')=1}} \mathrm{Tr}_\rho\big(B_q^a \otimes B_{q'}^{a'} \otimes B_{q''}^{a''}\big) \\
&\approx_{\varepsilon'^{1/4}} \mathrm{E}_{(q,q',q'')} \sum_{\substack{(a,a',a'')\\ V(a,a',a''|q,q',q'')=1}} \sum_{\substack{(a,b',b'')\\ V(a,b',b''|q,q',q'')=1}} \mathrm{Tr}_\rho\big(A_{q,q',q''}^{a,b',b''} \otimes B_{q'}^{a'} \otimes B_{q''}^{a''}\big) \\
&\approx_{\varepsilon'} \mathrm{E}_{(q,q',q'')} \sum_{\substack{(a,a',a'')\\ V(a,a',a''|q,q',q'')=1}} \mathrm{Tr}_\rho\big(A_{q,q',q''}^{a,a',a''} \otimes B_{q'}^{a'} \otimes B_{q''}^{a''}\big) \\
&\approx_{\varepsilon'} \mathrm{E}_{(q,q',q'')} \sum_{\substack{(a,a',a'')\\ V(a,a',a''|q,q',q'')=1}} \big\langle A_{q,q',q''}^{a,a',a''}, B_{q'}^{a'} \big\rangle_\Psi \\
&\geq 1-\varepsilon',
\end{aligned}$$

where the second line uses (8), the third and fourth use (7) together with the Cauchy-Schwarz inequality and the last is by definition of ε' and G_1'. Hence $\omega^*(G_1) \geq 1 - O((\varepsilon')^{1/4}) \geq 1-\varepsilon$ provided ε' is chosen small enough.

To conclude the proof of the corollary we define the game G_2 as a special type of parallel repetition of the game G_1'. Let K, K' be parameters to be chosen later.

- The referee picks K pairs of questions $(q_1^j, q_2^j)_{j=1,\ldots,K}$ according to the same distribution as in G_1'. In addition, he picks K' pairs $(r_1^j, r_2^j)_{j=1,\ldots,K'}$ where each r_1^j is chosen independently according to the marginal distribution on the first player and r_2^j independently according to the marginal on the second player,
- He picks two players at random and sends a random permutation of the questions $(q_1^j)_{j=1,\ldots,K}$ and $(r_1^j)_{j=1,\ldots,K'}$ to the first and $(q_2^j)_{j=1,\ldots,K}$ and $(r_2^j)_{j=1,\ldots,K'}$ to the second.
- Upon receiving answers $(a_1^j)_{j=1,\ldots,K+K'}$ and $(a_2^j)_{j=1,\ldots,K+K'}$ respectively he accepts if and only if for every j among the indices of the "q" questions (he undoes his random permutation of the questions) the pair (a_1^j, a_2^j) is a valid pair of answers to (q_1^j, q_2^j). (Answers to the "r" questions are ignored.)

It is clear that $\omega(G_1') = 1 \implies \omega(G_2) = 1$. Furthermore, using that G_1' is a projection game Theorem 7 from [KV11] shows that there is an appropriate choice of the parameters $K, K' = \mathrm{poly}(\delta^{-1}, (\varepsilon')^{-1})$ such that if $\omega^*(G_2) \geq \delta$ then $\omega^*(G_1') \geq 1-\varepsilon'$. (Theorem 7 from [KV11] as stated applies to two-player games. However, since here the referee only plays with two players anyways it is not hard to verify that the theorem extends to the present setting. In particular, the reduction performed in [KV11] is oblivious to the choice of entangled state.) □

4.4 Hardness for three-player XOR games

Håstad [Hås01, Theorem 5.5] showed that for any $\varepsilon > 0$ it is NP-hard to approximate the classical value of a 3-player XOR game within a multiplicative factor $2-\varepsilon$. Starting from Corollary 4.2 and adapting Håstad's proof to the case of entangled players we arrive at the following, which is a restatement of Theorem 1.

Corollary 4.4. *Let $\varepsilon, \delta > 0$ be arbitrary constants. Then the following is NP-hard. Given a 3-player XOR game G, distinguish between $\omega(G) \geq 1 - \varepsilon$ and $\omega^*(G) \leq (1+\delta)/2$.*

Proof. The proof follows the analysis of the test $L_2^{\varepsilon}(u)$ in [Hås01, Lemma 5.2], but we need to slightly modify the test to account for the fact that we do not know that direct parallel repetition of projection games works in the case of entangled players, so we need to accommodate the use of "confuse" questions in [KV11]. The proof, however, still follows closely Håstad's proof, to which we refer for more details than given here.

We first introduce some notation. Let φ be a 3-SAT formula and $G_1 = G_\varphi$ be the 3-player binary game associated to φ as the game G_2 in the proof of Corollary 4.2. Let $X = \{x_1, \ldots, x_n\}$ be the set of all possible questions in G. We think of the answers as taking values in $\{\pm 1\}$, where here -1 corresponds to "true", i.e. a value of 1, and 1 to "false", i.e. 0. For every triple of questions (x, y, z), let $\psi_{x,y,z} : \{\pm 1\}^3 \to \{\pm 1\}$ be the function determining whether the referee accepts or rejects any given answer triple to those questions.

For any subset $U \subseteq X$, let $\mathcal{F}_U = \{f : \{\pm 1\}^U \to \{\pm 1\}\}$. For every pair of functions $f, -f \in \mathcal{F}_U$ we select a unique representative and let $R_U \subset \mathcal{F}_U$ be the resulting set.[11] For $\alpha \subseteq \{\pm 1\}^U$, let $\chi_\alpha : \mathcal{F}_U \to \{\pm 1\}$ be defined by $\chi_\alpha(f) = \prod_{x \in \alpha} f(x)$. For any set of operators $\{A_f\}_{f \in \mathcal{F}_U}$ and α define

$$\hat{A}_\alpha := \mathrm{E}_{f \in \mathcal{F}_U} \chi_\alpha(f) A_f, \qquad \text{so that} \qquad A_f = \sum_\alpha \chi_\alpha(f) \hat{A}_\alpha. \tag{9}$$

Let K, K' be parameters to be chosen later. Consider the following 3-player XOR game G_2.

1. The referee independently samples $K + K'$ triples of questions (x_k, y_k, z_k) as in game G_1. For $1 \leq k \leq K$ let $w_k \in \{x_k, y_k, z_k\}$ be chosen uniformly at random. For $K+1 \leq k \leq K+K'$ let $w_k \in X$ be chosen according to the single-player marginal in G. Let $U = \{w_k,\ 1 \leq k \leq K + K'\}$ and $W = \{x_k, y_k, z_k,\ 1 \leq k \leq K + K'\}$. Note that the sets U and W are unordered. Let $Z = U \cup W$. Let $\psi = \wedge_{1 \leq k \leq K+K'} \psi_{x_k, y_k, z_k} \in \mathcal{F}_W$.

2. The referee chooses a function $\mu \in \mathcal{F}_Z$ by setting $\mu(y) = 1$ with probability $1 - \varepsilon$ and $\mu(y) = -1$ with probability ε, independently for every $y \in \{-1, 1\}^Z$. He chooses $f \in \mathcal{F}_U$, $g_1 \in \mathcal{F}_W$ uniformly and sets $g_2 = f g_1 \mu \in \mathcal{F}_Z$ by defining $g_2(y) = f(y_{|U}) g_1(y_{|W}) \mu(y)$ for every $y \in \{\pm 1\}^Z$.

3. The referee chooses a random permutation of the three players and sends $-1_{f \in R_U} f$ to the first player, $-1_{(g_1 \wedge \psi) \in R_W}(g_1 \wedge \psi)$ to the second, $-1_{(g_2 \wedge \psi) \in R_Z}(g_2 \wedge \psi)$ to the third.[12]

4. He receives answers $a, b, c \in \{\pm 1\}$ and accepts if and only if

$$abc = (-1_{f \in R_U})(-1_{(g_1 \wedge \psi) \in R_W})(-1_{(g_2 \wedge \psi) \in R_Z}).$$

First we show that if $\omega(G_1) = 1$ then $\omega(G_2) \geq 1 - \varepsilon$. Indeed, let $x \in \{\pm 1\}^X$ be a perfect strategy for the players in G_1. Then in G_2 the players can answer their queries f', g_1', g_2' by $f'(x_{|U})$, $g_1'(x_{|W})$, $g_2'(x_{|Z})$ respectively. Given $\psi(x) = 1$ since x came from a perfect strategy in G_1, $g_1 = g_1 \wedge \psi$ and $g_2 = g_2 \wedge \psi$, so the players will be accepted if and only if $f g_1 g_2(x_{|Z}) = \mu(x_{|Z}) = 1$, which happens with probability exactly $1 - \varepsilon$ by definition of μ. To establish soundness, we first introduce the following game G_1'.

1. The referee chooses U, W as in game G_1.

[11] The role of R_U is to enable an operation known as "folding over true".

[12] Here the $\wedge$ is computed by interpreting -1 as "true" and 1 as "false". This operation of "folding over ψ" is also used in [Hås01] and is convenient for the analysis.

2. The referee chooses two players at random, sends U to the first and W to the second.

3. Each player returns an assignment to all variables in the set he was asked. The referee checks that the assignments are consistent on the variables in $U \cap W$, and that they satisfy ψ.

The following claim states the soundness property of G_1'.

Claim 4.5. *For any $\delta', \varepsilon > 0$ there exists K, K' (depending only on δ' and ε) such that if $\omega^*(G_1') \geq \delta'$ then $\omega^*(G_1) \geq 1 - \varepsilon$.*

Proof. The game G_1' is obtained from G_1 exactly as G_2 is obtained from G_1' in the proof of Corollary 4.3, and the soundness follows from [KV11, Theorem 7] using the same steps as in the analysis done in the proof of the corollary. □

We are now ready to establish soundness of the game G_2.

Claim 4.6. *Suppose that $\omega^*(G_2) \geq (1+\delta)/2$. Then $\omega^*(G_1') \geq 4\varepsilon\delta^2$, where G_1' is the "parallel repeated" game obtained from G_1 as above.*

Proof. We follow almost textually the proof of [Hås01, Lemma 5.2]. Let $(|\Psi\rangle, A_{U,f}, B_{W,g_1}, C_{Z,g_2})$ be a strategy for the players in G_2 with success at least $(1+\delta)/2$, where for every U, W, Z and f, g_1, g_2, $A_{U,f}$, B_{W,g_1} and C_{Z,g_2} are observables.

First fix a choice of U and W and let ψ be defined as in the game. For convenience we rename $A_f := r_f A_{U,r_f f}$, where $r_f = -1_{f \in R_U}$, and similarly $B_{g_1} := r_{g_1} B_{W,r_{g_1} g_1}$, where $r_{g_1} = -1_{(g_1 \wedge \psi) \in R_W}$ and $C_{g_2} := r_{g_2} C_{Z,r_{g_2} g_2}$, where $r_{g_2} = -1_{(g_2 \wedge \psi) \in R_Z}$. Conditioned on the referee making these choices, the players' success probability in the game is

$$\delta_{U,W,\psi} := \mathrm{E}_{f,g_1,g_2} \mathrm{Tr}_\rho \big(A_f \otimes B_{g_1} \otimes C_{g_2} \big).$$

Expanding the observables as per (9) and proceeding as in [Hås01, Proof of Lemma 5.2] we arrive at the following:

$$\delta_{U,W,\psi} = \sum_\gamma (1-2\varepsilon)^{|\gamma|} \mathrm{Tr}_\rho \big(\hat{A}_{\pi_U(\gamma)} \otimes \hat{B}_{\pi_W(\gamma)} \otimes \hat{C}_\gamma \big), \tag{10}$$

where here the summation ranges over all those $\gamma \in \{\pm 1\}^Z$ that are such that $\psi(x) = 1$ for every assignment $x \in \gamma$, and $\pi_U(\gamma)$ (resp. $\pi_W(\gamma)$) is defined as the set of assignments $x \in \{\pm 1\}^U$ (resp. $y \in \{\pm 1\}^W$) for which there is an odd number of $z \in \gamma$ whose restriction to U (resp. W) is x (resp. y).

We define a strategy for the players in G_1'. The player who receives the set U measures according to the measurement $\{\hat{A}_\alpha^2\}_{\alpha \subseteq \{\pm 1\}^U}$ and answers with a random $x \in \alpha$. The player who receives the set W measures according to the measurement $\{\hat{B}_\beta^2\}_{\beta \subseteq \{\pm 1\}^W}$ and answers with a random $y \in \beta$. (The fact that these are well-defined POVM follows from (9) and Parseval's formula.)

By definition of A_f using the folding operation, any assignment y returned by the second player automatically satisfies ψ (see Lemma 2.34 in [Hås01]). So the probability that the players' answers are accepted is simply the probability that they are consistent, i.e. x and y agree on the variables in $U \cap W$. For any $(\alpha, \beta) \subseteq \{\pm 1\}^U \times \{\pm 1\}^W$ let

$$S(\alpha, \beta) := \big\{ \gamma \subseteq \{\pm 1\}^Z : \pi_U(\gamma) = \alpha \wedge \pi_W(\gamma) = \beta \big\}.$$

Let $r_{\alpha,\beta} = \min_{\gamma \in S(\alpha,\beta)} |\gamma|$; if $S_{\alpha,\beta}$ is empty we let $r_{\alpha,\beta} = \infty$. Then we claim that conditioned on having obtained a pair (α, β) the probability of the players being consistent is at least $r_{\alpha,\beta}^{-1}$. Indeed, let $\gamma \in S(\alpha, \beta)$

be such that $|\gamma| = r_{\alpha,\beta}$. For any $z \in \gamma$ there is at least one pair of answers, $(x = \pi_U(z), y = \pi_W(z))$, that is consistent, and by definition of α, β from γ there are at most $|\gamma|^2$ pairs of possible answers $(x \in \pi_U(\gamma), y \in \pi_W(\gamma))$ in total. Hence the overall success of the above-defined strategy for this U, W is at least

$$\sum_{\alpha,\beta} r_{\alpha,\beta}^{-1} \operatorname{Tr}_\rho\big(\hat{A}_\alpha^2 \otimes \hat{B}_\beta^2 \otimes \mathrm{Id}\big).$$

Starting from (10) and applying the Cauchy-Schwarz inequality,

$$\begin{aligned}\delta_{U,W,\psi} &\leq \Big(\sum_{\alpha,\beta} (1-2\varepsilon)^{2r_{\alpha,\beta}} \operatorname{Tr}_\rho\big(\hat{A}_\alpha^2 \otimes \hat{B}_\beta^2 \otimes \mathrm{Id}\big)\Big)^{1/2} \Big(\sum_{\alpha,\beta}\Big(\sum_{\gamma \in S(\alpha,\beta)} \operatorname{Tr}_\rho\big(\mathrm{Id}\otimes\mathrm{Id}\otimes\hat{C}_\gamma\big)\Big)^2\Big)^{1/2} \\ &\leq \Big(\sum_{\alpha,\beta} \frac{1}{4\varepsilon r_{\alpha,\beta}} \operatorname{Tr}_\rho\big(\hat{A}_\alpha^2 \otimes \hat{B}_\beta^2 \otimes \mathrm{Id}\big)\Big)^{1/2}, \qquad (11)\end{aligned}$$

where for the second line we used $(1-2\varepsilon)^t \leq (4\varepsilon t)^{-1/2}$ for any $t > 0$ and $0 < \varepsilon < 1/2$, and we bounded the term inside the second square root by 1 by observing that

$$\sum_{\alpha,\beta}\Big(\sum_{\gamma \in S(\alpha,\beta)} \operatorname{Tr}_\rho\big(\mathrm{Id}\otimes\mathrm{Id}\otimes\hat{C}_\gamma\big)\Big)^2 \;=\; \mathrm{E}_{f_1 \in \mathcal{F}_U,\, f_2 \in \mathcal{F}_W} \operatorname{Tr}_\rho\big(\mathrm{Id}\otimes\mathrm{Id}\otimes C_{f_1 f_2}^2\big) \;=\; 1,$$

where the first equality follows by expanding out the right-hand side in the Fourier basis. Taking the expectation over U, W and applying Jensen's inequality, from (11) we arrive at $\delta \leq \sqrt{\tau/(4\varepsilon)}$, where τ is the success probability of the above-defined strategy in G_1'. Hence $\omega^*(G_1') \geq 4\varepsilon\delta^2$, as claimed. □

Let K and K' be as in Claim 4.5 for $\delta' = 4\varepsilon\delta^2$. The claim together with Claim 4.6 shows that if $\omega^*(G_2) \geq (1+\delta)/2$ then $\omega^*(G_1) \geq 1-\varepsilon$, as required. □

5 The consolidation procedure

The proof of Theorem 3.1, which states the soundness of the low-degree point-vs-plane test against entangled players, relies on an induction procedure: the measurement $\{M^g\}$ is constructed, starting from the $\{A_x^a\}$, by removing the dependence of A_x on the m coordinates of $x \in \mathbb{F}^m$ one at a time. As the induction proceeds the error (as measured by an expression similar to (6)) blows up exponentially. To keep it bounded it is necessary to "improve" the quality of the measurements constructed at each step of the induction. The main result of this section, stated in Proposition 5.8, shows that this is possible as long as the measurements constructed remain mildly consistent with an underlying "robust" structure (which will eventually be obtained directly from measurements A_x passing the low-degree test with high probability). The "robustness" of the structure is used to argue that any measurement mildly consistent with it can be improved to one that is highly consistent.

We first define precisely the three properties of a measurement $\{M^g\}$ that we wish to improve. In Section 5.2 we introduce the notion of a (δ, μ)-robust triple, the underlying structure that will enable the improvement. In Section 5.3 we show how two of the three properties can be improved. Finally, the main result, Proposition 5.8, is proved in Section 5.4.

5.1 Consistency parameters

The measurements $\{M^g\}$ constructed throughout the induction will not always be complete measurements, i.e. they will satisfy $0 \leq M^g \leq \mathrm{Id}$ and $\sum^g M^g \leq \mathrm{Id}$, but not necessarily with equality. Whenever these conditions hold we call $\{M^g\}$ a *sub-measurement*. For convenience we restate Definition 2.3.

Definition 5.1. *Let S be a finite set, $A = \{A^g\}_{g\in S}$ such that $0 \leq A^g \leq \mathrm{Id}$ for every g, and $M = \{M^g\}_{g\in S}$ a sub-measurement. For any $\delta, \gamma, \eta > 0$, we say that M is*

- *δ-consistent with A if $\sum_g \langle \mathrm{Id} - A^g, M^g\rangle_\Psi \leq \delta$,*
- *γ-projective if $\langle M, \mathrm{Id} - M\rangle_\Psi \leq \gamma$, where $M := \sum_g M^g$,*
- *η-complete if $\mathrm{Tr}_\rho(M) = \langle M, \mathrm{Id}\rangle_\Psi \geq (1-\eta)$.*

If M satisfies the first item with $A = M$ we also say that M is δ-self-consistent.

The first property in the definition, consistency, can be understood as a measure of distance: measurements that are consistent are "close" in a precise sense (see the discussion following the statement of Theorem 3.1 for more on this). The second property, projectivity, intuitively measures how far an operator M is from being self-consistent, or "orthogonal" (if $|\Psi\rangle$ was the maximally entangled state on two subsystems, $\langle M, \mathrm{Id} - M\rangle_\Psi$ would be 0 if and only if M is the orthogonal projection on a subspace). The last property, completeness, measures how far a measurement is from being complete. Note that complete measurements are automatically 0-projective.

5.2 Robust triples

In this section we define the notion of (δ, μ)-robust triple, and prove some useful properties.

Definition 5.2. *Let $G = (V, E)$ be a graph, S a finite set, $\mathcal{G} \subseteq \{g : V \to S\}$ a set of functions and for every $v \in V$, $A_v = \{A_v^a\}_{a\in S}$ a measurement with outcomes in S. Given $\delta > 0$ and $0 < \mu \leq 1$, we say that $(G, A, \mathcal{G})$ is a (δ, μ)-robust triple if:*

1. *(self-consistency) The measurements A are δ-self-consistent, on average over $v \in V$:*

$$\mathrm{E}_{v\in V} \sum_{a\in S} \langle A_v^a, \mathrm{Id} - A_v^a\rangle_\Psi \leq \delta,$$

2. *(small intersection) For any $g \neq g' \in \mathcal{G}$, $\Pr_{v\in V}\left(g(v) = g'(v)\right) \leq \delta$,*
3. *(stability) For any sub-measurement $\{R^g\}_{g\in\mathcal{G}}$ it holds that*

$$\mathrm{E}_{v\in V}\mathrm{E}_{v'\in N(v)} \sum_g \langle R^g, (A_v^{g(v)} - A_{v'}^{g(v')})^2\rangle_\Psi \leq \delta,$$

   where $N(v)$ is the set of neighbors of v in G,

4. *(expansion) G has mixing time $O(\mu^{-1})$. Precisely, if for any $v \in V$ we let $p_k(v)$ denote the distribution on V that results from starting a k-step random walk at v, then for any $\delta > 0$ and some $k = O(\log(1/\delta)\log(1/\mu))$ it holds that $\mathrm{E}_{v\in V}\|p_k(v) - u\|_1 \leq \delta$, where u is the uniform distribution on V.*

We will sometimes make the underlying state $|\Psi\rangle$ explicit by writing the triple as $(G, A, \mathcal{G})_\Psi$.

We note a useful property that follows from the definition.

Claim 5.3. *Suppose $(G, A, \mathcal{G})_\Psi$ is a (δ, μ)-robust triple. Then the measurements A_v are almost-projective, in the sense that*

$$\mathrm{E}_v \sum_a \langle A_v^a - (A_v^a)^2, \mathrm{Id}\rangle_\Psi \;=\; O\big(\sqrt{\delta}\big). \tag{12}$$

Furthermore, there exists a $\delta' = O\big(\delta^{1/2}\log^2(1/\delta)\log^2(1/\mu)\big)$ such that for any sub-measurement $\{R^g\}_{g\in\mathcal{G}}$,

$$\sum_g \big\langle R^g, A^g - (A^g)^2\big\rangle_\Psi \;\le\; \delta',$$

where $A^g := \mathrm{E}_{v\in V} A_v^{g(v)}$.

Proof. The first property in the claim follows from the self-consistency condition. Indeed,

$$\begin{aligned}
\mathrm{E}_v \sum_a \langle A_v^a - (A_v^a)^2, \mathrm{Id}\rangle_\Psi &= \mathrm{E}_v \sum_a \langle A_v^a(\mathrm{Id} - A_v^a), \mathrm{Id}\rangle_\Psi \\
&= \mathrm{E}_v \sum_{a,b} \langle A_v^a(\mathrm{Id} - A_v^a), A_v^b\rangle_\Psi \\
&\approx_{\sqrt{\delta}} \mathrm{E}_v \sum_a \langle A_v^a(\mathrm{Id} - A_v^a), A_v^a\rangle_\Psi \\
&\approx_{\sqrt{\delta}} \mathrm{E}_v \sum_a \langle \mathrm{Id} - A_v^a, A_v^a\rangle_\Psi \\
&\le \delta,
\end{aligned}$$

where the third and fourth lines follow from the Cauchy-Schwarz inequality and the self-consistency condition.

To show the second property, first recall from Definition 5.2 that the robustness condition implies the stability property

$$\mathrm{E}_{v,v'\in N(v)} \sum_g \big\langle R^g, (A_v^{g(v)} - A_{v'}^{g(v')})^2\big\rangle_\Psi \;\le\; \delta. \tag{13}$$

We first observe that this condition implies that for any $k \ge 1$,

$$\mathrm{E}_{v,v'\in N^k(v)} \sum_g \big\langle R^g, (A_v^{g(v)} - A_{v'}^{g(v')})^2\big\rangle_\Psi \;\le\; k^2\,\delta, \tag{14}$$

where $N^k(v)$ is the set of all $v' \in V$ that are at distance at most k from v in G, and the distribution on $N^k(v)$ is the one that results from starting a k-step random walk at v. Indeed, (14) simply follows from (13) and successive applications of the triangle inequality.

The expansion condition in the definition of a (δ, μ)-robust triple implies that for some $k = O(\log(1/\delta)\log(1/\mu))$ the distribution on $N^k(v)$ is δ-close in statistical distance to uniform on V. Applying (14) for this k, we get

$$\mathrm{E}_{v,v'} \sum_g \big\langle R^g, (A_v^{g(v)} - A_{v'}^{g(v')})^2\big\rangle_\Psi \;\le\; (k^2+2)\delta,$$

since for any v, v', $\sum_g \big\langle R^g, (A_v^{g(v)} - A_{v'}^{g(v')})^2\big\rangle_\Psi \le 2$. Expanding the square and using (12), we see that

$$\sum_g \big\langle R^g, (A^g)^2\big\rangle_\Psi \;\ge\; \sum_g \big\langle R^g, A^g\big\rangle_\Psi - \frac{k^2+2}{2}\,\delta - O\big(\sqrt{\delta}\big),$$

which proves the claim. □

5.3 Consistency consolidation

In this section we prove the following lemma, which establishes consolidation for the consistency and projectivity properties (see Definition 5.1). Intuitively, the lemma shows that if a sub-measurement Q is mildly consistent with a family of measurements $\{A_v\}$ that underlie a robust triple, then Q can be modified into a sub-measurement S that is highly consistent with A and projective.

Lemma 5.4. *Let $\delta, \eta > 0$ be such that $\delta \leq \eta \leq 1/2$, $\mu > 0$, and $|\Psi\rangle$ a permutation-invariant state over $r \geq 3$ registers. Let $(G, A, \mathcal{G})_\Psi$ be a (δ, μ)-robust triple and $\{Q^g\}_{g\in\mathcal{G}}$ a sub-measurement that is η-consistent with A. Then there exists a sub-measurement $\{S^g\}_{g\in\mathcal{G}}$ such that S is η'-consistent with A and projective, for some $\eta' = O(\delta^{1/4}\log^2(1/\delta)\log^2(1/\mu))$ that is independent of η. Moreover, S also satisfies $\langle S, \mathrm{Id}\rangle_\Psi \geq \langle Q, \mathrm{Id}\rangle_\Psi - \eta - \eta'$.*

The remainder of the section is devoted to the proof of the lemma. For any $g \in \mathcal{G}$, let $A^g := \mathrm{E}_{v\in V} A_v^{g(v)}$. We first give the following useful claim.

Claim 5.5. *Let $r \geq 2$, $|\Psi\rangle$ an r-register permutation-invariant state and ρ the reduced density of $|\Psi\rangle\langle\Psi|$ on any one register. Suppose that $\{A_v^a\}$ is a family of measurements that is δ-self-consistent, i.e.*

$$\mathrm{E}_v \sum_a \langle A_v^a, \mathrm{Id} - A_v^a\rangle_\Psi \;=\; \mathrm{E}_v \sum_a \langle\Psi| A_v^a \otimes (\mathrm{Id} - A_v^a) \otimes \mathrm{Id}^{\otimes(r-2)} |\Psi\rangle \;\leq\; \delta.$$

Then the following holds.

$$\mathrm{E}_v \sum_a \mathrm{Tr}\big(A_v^a \rho^{1/2} (\mathrm{Id} - \overline{A_v^a}) \rho^{1/2}\big) \;\leq\; 2\delta.$$

Proof. Let $|\Psi\rangle = \sum_i \sqrt{\lambda_i}|u_i\rangle|v_i\rangle$ be the Schmidt decomposition, where the $|u_i\rangle$ are orthonormal vectors on the first register, and $|v_i\rangle$ are on the remaining $(r-1)$ registers. By definition, $\rho = \sum_i \lambda_i |u_i\rangle\langle u_i|$. By self-consistency of A it holds that

$$\mathrm{E}_v \sum_a \langle\Psi| A_v^a \otimes A_v^a \otimes \mathrm{Id} |\Psi\rangle \;=\; \mathrm{E}_v \sum_a \sum_{i,j} \sqrt{\lambda_i}\sqrt{\lambda_j} \langle u_i| A_v^a |u_j\rangle \langle v_i| A_v^a \otimes \mathrm{Id} |v_j\rangle \;\geq\; 1 - \delta,$$

where here the Id acts on all but the first two players. Applying the Cauchy-Schwarz inequality, we get

$$\mathrm{E}_v \sum_a \sum_{i,j} \sqrt{\lambda_i}\sqrt{\lambda_j} \big|\langle u_i| A_v^a |u_j\rangle\big|^2 \;\geq\; (1-\delta)^2 \;\geq\; 1 - 2\delta.$$

To conclude, observe that the left-hand side is exactly $1 - \mathrm{E}_v \sum_a \mathrm{Tr}(A_v^a \rho^{1/2}(\mathrm{Id} - \overline{A_v^a})\rho^{1/2})$. □

The proof of Lemma 5.4 relies on the use of the following semidefinite program. Recall that $\rho = \mathrm{Tr}_{\mathcal{H}^{\otimes(r-1)}} |\Psi\rangle\langle\Psi|$ is the reduced density of $|\Psi\rangle$ on either players' subspace, which we may always assume is invertible (if not, simply restrict all measurements to the support of ρ).

Primal SDP

$$\begin{aligned} \omega \;:=\; \max & \sum_g \mathrm{Tr}\big(T^g \rho^{1/2} \overline{A^g} \rho^{1/2}\big) \qquad (15) \\ s.t.\quad & \forall g,\ T^g \geq 0, \quad \sum_g T^g \leq \mathrm{Id}\,. \end{aligned}$$

Dual SDP

$$\begin{aligned} & \min \mathrm{Tr}(X) \qquad (16) \\ s.t.\quad & \forall g,\ X \geq \rho^{1/2} \overline{A^g} \rho^{1/2}, \\ & X \geq 0. \end{aligned}$$

We make a few preliminary observations about the SDP.

Claim 5.6. *Strong duality holds for* (15) *and* (16)*. Let* $\{T^g\}$ *be an optimal solution to the primal,* X *a matching dual solution, and* $Z := \rho^{-1/2} X \rho^{-1/2}$*. Then the following hold.*

1. $\omega = \sum_g \mathrm{Tr}\big(T^g \rho^{1/2} \overline{A^g} \rho^{1/2}\big) \geq \mathrm{Tr}_\rho(Q) - \eta - O(\sqrt{\delta})$,
2. $T := \sum_g T^g = \mathrm{Id}$,
3. $\forall g, \quad T^g \rho^{1/2} Z = T^g \rho^{1/2} \overline{A^g}$ *and* $Z \rho^{1/2} T^g = \overline{A^g} \rho^{1/2} T^g$.

Proof. It is easy to verify that both primal and dual SDPs are strictly feasible, and hence strong duality holds. By choosing $T^g := Q^g$ in (15) we get

$$\begin{aligned}
\omega &\geq \sum_g \mathrm{Tr}\big(Q^g \rho^{1/2} \overline{A^g} \rho^{1/2}\big) \\
&\approx_{\sqrt{\delta}} \sum_g \mathrm{Tr}\big(\rho^{1/2} Q^g A^g \rho^{1/2}\big) \\
&= \sum_g \mathrm{Tr}\big(Q^g A^g \otimes \mathrm{Id}\big) \\
&\approx_{\sqrt{\delta}} \sum_g \mathrm{Tr}_\rho\big(Q^g \otimes A^g\big) \\
&\geq \mathrm{Tr}_\rho(Q) - \eta,
\end{aligned}$$

where the second line uses the Cauchy-Schwarz inequality and Claim 5.5, the fourth line self-consistency of A and the fifth follows from η-consistency of Q and A. This proves the first item in the claim.

Let $(\{T^g\}, X)$ be an optimal primal-dual solution pair. Clearly, we may without loss of generality assume that $T = \sum_g T^g = \mathrm{Id}$, as imposing this can only improve the primal objective function. Finally, the last conditions stated in the claim follow from the complementary slackness conditions

$$\forall g, \quad T^g X = T^g \rho^{1/2} \overline{A^g} \rho^{1/2} \quad \text{and} \quad X T^g = \rho^{1/2} \overline{A^g} \rho^{1/2} T^g, \tag{17}$$

the definition of Z and the fact that ρ is invertible. □

Let $(\{T^g\}, X)$ be an optimal primal-dual solution pair to (15)-(16), and for every $g \in \mathcal{G}$ define

$$S^g := \mathrm{E}_v A_v^{g(v)} T^g A_v^{g(v)}. \tag{18}$$

For every g, we have $0 \leq S^g \leq A^g$ and $S := \sum_g S^g \leq \mathrm{Id}$. We first prove the following about $\{S^g\}$.

Claim 5.7. *Let* $(G, A, \mathcal{G})_\Psi$ *be a* (δ, μ)*-robust triple,* $\{S^g\}$ *as defined in* (18)*, and* δ' *as in Claim 5.3. Then* $\{S^g\}$ *is a sub-measurement such that*

1. $\mathrm{Tr}_\rho(S) = \sum_g \mathrm{Tr}_\rho(S^g) \geq \omega - O(\sqrt{\delta})$,
2. S *is* $O(\delta')$*-consistent with* A.

Proof. We have

$$\begin{aligned}\mathrm{Tr}_\rho(S) &= \mathrm{E}_v \sum_g \mathrm{Tr}\big(A_v^{g(v)} T^g A_v^{g(v)} \rho^{1/2} \,\mathrm{Id}\, \rho^{1/2}\big) \\ &\approx_{\sqrt{\delta}} \mathrm{E}_v \sum_g \mathrm{Tr}\big(T^g \rho^{1/2} \overline{A_v^{g(v)}} \rho^{1/2}\big) \\ &\geq \omega,\end{aligned}$$

where the second line follows from Claim 5.5 and the third is by definition of ω. This proves the first item in the claim. To show the second, note that

$$\sum_g \big\langle S^g, \mathrm{Id} - A^g \big\rangle_\Psi \approx_{\sqrt{\delta}} \sum_g \big\langle T^g, A^g(\mathrm{Id} - A^g)A^g \big\rangle_\Psi = O(\delta' + \sqrt{\delta}),$$

where the first approximate equality uses self-consistency of A and the last equality follows from Claim 5.3. □

The condition on consistency of S and A in Lemma 5.4 now follows from the second item in Claim 5.7 provided $\eta' = \Omega(\delta')$, and the completeness condition follows from the first item in Claim 5.7 together with the first item in Claim 5.6, provided $\eta' = \Omega(\sqrt{\delta})$. To complete the proof of the lemma it only remains to verify the projectivity condition. Recall that $Z = \rho^{-1/2} X \rho^{-1/2}$. We have

$$\begin{aligned}\langle S, \mathrm{Id} - S\rangle_\Psi &= \mathrm{Tr}_\rho\big(S \otimes (\mathrm{Id} - S) \otimes \mathrm{Id}^{\otimes(r-2)}\big) \\ &\approx_{\sqrt{\delta}} \sum_g \mathrm{Tr}_\rho\big(T^g \otimes (\mathrm{Id} - S) \otimes A^g\big) \\ &\leq \sum_g \mathrm{Tr}_\rho\big(T^g \otimes (\mathrm{Id} - S) \otimes \overline{Z}\big) \\ &= \mathrm{Tr}_\rho\big((\mathrm{Id} - S) \otimes \overline{Z}\big) \\ &\leq \mathrm{Tr}_\rho\big(\overline{Z}\big) - \sum_g \mathrm{Tr}_\rho\big(S^g \otimes A^g\big) \\ &= \sum_g \mathrm{Tr}\big(T^g \rho^{1/2} \overline{A^g} \rho^{1/2}\big) - \mathrm{E}_v \sum_g \mathrm{Tr}_\rho\big(A_v^{g(v)} T^g A_v^{g(v)} \otimes A^g\big) \\ &\approx_{\sqrt{\delta}+\delta'} \sum_g \mathrm{Tr}_\rho\big(A_v^{g(v)} T^g A_v^{g(v)}\big) - \mathrm{E}_v \sum_g \mathrm{Tr}_\rho\big(A_v^{g(v)} T^g A_v^{g(v)}\big) \\ &= O\big(\delta' + \sqrt{\delta}\big),\end{aligned}$$

where the second line uses the definition of S and self-consistency of A; the third uses the dual constraint and the definition of Z; the fourth item 2 from Claim 5.6; the fifth again uses the dual constraint; the sixth uses strong duality and the fact that $\mathrm{Tr}_\rho\big(\overline{Z}\big)$ is real (since Z is Hermitian) for the first term, and the definition of S for the second; the seventh uses Claim 5.5 for the first term and Claim 5.3 for the second. This establishes the projectivity condition on S provided $\eta' = \Omega(\delta' + \sqrt{\delta})$

5.4 Self-consolidation

The following proposition states our main "consolidation" result.

Proposition 5.8 (Self-consolidation)**.** *There exists a constant $K > 0$ such that the following holds. Let $r \geq 3$, H a symmetric r-player game, X a finite set, and for every $\boldsymbol{x} \in X$, $G_{\boldsymbol{x}} = (V_{\boldsymbol{x}}, E_{\boldsymbol{x}})$ a graph, $S_{\boldsymbol{x}}$ a set, and $\mathcal{G}_{\boldsymbol{x}} \subseteq \{g : V_{\boldsymbol{x}} \to S_{\boldsymbol{x}}\}$.*

Suppose that for any $0 < \varepsilon < K$ and strategy $(P, |\Psi\rangle)$ for the players that has success $1-\varepsilon$ in the game H and is ε-self-consistent there exists a collection $A_{\boldsymbol{x}} = \{A^a_{\boldsymbol{x},v}\}_{a \in S}$ of projective measurements defined for every $v \in V_{\boldsymbol{x}}$, possibly depending on P but independent of $|\Psi\rangle$, such that that for all $\boldsymbol{x} \in X$, $(G_{\boldsymbol{x}}, A_{\boldsymbol{x}}, \mathcal{G}_{\boldsymbol{x}})_\Psi$ is a (δ, μ)-robust triple for some $\delta, \mu > 0$ such that $\eta'(\delta, \mu) < 1/4$, where η' is as defined in Lemma 5.4.

Suppose further that for any $\varepsilon' > 0$ there exists $\eta = \eta(\varepsilon')$ such that $\eta \to 0$ as $\varepsilon' \to 0$, and whenever $(P', |\Psi'\rangle)$ is a strategy with success $1-\varepsilon'$ in H, there exists a family of sub-measurements $\{Q^g_{\boldsymbol{x}}\}_{g \in \mathcal{G}}$ that is η-consistent with $A'_{\boldsymbol{x}}$ (obtained from P') and η-complete, on average over $\boldsymbol{x} \in X$.

Then for any small enough $0 < \varepsilon < K$ and strategy $(P, |\Psi\rangle)$ for the players that has success $1-\varepsilon$ in the game H and is ε-self-consistent there exists a family of (complete) measurements $\{R^g_{\boldsymbol{x}}\}_{g \in \mathcal{G}}$ that is η_c-consistent with $A_{\boldsymbol{x}}$ for some $\eta_c = O(r(\eta')^{1/4})$, on average over $\boldsymbol{x} \in X$.

The significance of the proposition is that the parameter η_c is independent of the parameter η associated with the family $\{Q^g_{\boldsymbol{x}}\}$. It only depends on the robustness parameters δ, μ (which themselves implicitly depend on ε). Before proving the proposition we establish two general claims about symmetric r-player games.

Claim 5.9. *Let $r \geq 2$, H a symmetric r-player game, and $\{P^a_q\}$ a set of projective measurements for the players in H (here $q \in Q$ and $a \in A$, respectively the sets of possible questions and answers in the game). Then there exists an operator $X = X(H, P)$ such that $0 \leq X \leq \mathrm{Id}$ and for any permutation-invariant state $|\Psi\rangle$, the success probability p_s of the strategy $(P, |\Psi\rangle)$ in H satisfies*

$$\left| p_s - \langle \Psi | X \otimes \mathrm{Id}^{\otimes(r-1)} | \Psi \rangle \right| \leq 2(r-1)\sqrt{2\delta},$$

where δ is the self-consistency parameter

$$\delta = \mathrm{E}_q \sum_a \langle \Psi | P^a_q \otimes (\mathrm{Id} - P^a_q) \otimes \mathrm{Id}^{\otimes(r-2)} | \Psi \rangle,$$

and here the expectation is taken according to the marginal distribution of questions on a single player.

Proof. We do the proof for the case $r = 2$; the general case is similar. The players' success probability in H can be expressed as

$$p_s = \mathrm{E}_{(q,q')} \sum_{(a,a')} V(a, a'|q, q') \langle \Psi | P^a_q \otimes P^{a'}_{q'} | \Psi \rangle,$$

where $V(a, a'|q, q') \in \{0, 1\}$ are coefficients representing the referee's decision to accept or reject the pair of answers (a, a') to the questions (q, q'). Let

$$X := \mathrm{E}_{(q,q')} \sum_{(a,a')} V(a, a'|q, q') \sqrt{P^a_q} P^{a'}_{q'} \sqrt{P^a_q}.$$

Then $0 \leq X \leq \mathrm{Id}$. Let $Y := \mathrm{E}_{(q,q')} \sum_{(a,a')} V(a,a'|q,q') \sqrt{P_q^a} \otimes P_{q'}^{a'} \sqrt{P_q^a}$. We have

$$\begin{aligned}
\left| p_s - \langle \Psi | Y | \Psi \rangle \right| &= \left| \mathrm{E}_{(q,q')} \sum_{(a,a')} V(a,a'|q,q') \langle \Psi | \left(\sqrt{P_q^a} \otimes P_{q'}^{a'} \, \mathrm{Id} \right) \left(\sqrt{P_q^a} \otimes \mathrm{Id} - \mathrm{Id} \otimes \sqrt{P_q^a} \right) | \Psi \rangle \right| \\
&\leq \left(\mathrm{E}_{(q,q')} \sum_{a,a'} \langle \Psi | P_q^a \otimes P_{q'}^{a'} | \Psi \rangle \right)^{1/2} \\
&\quad \cdot \left(\mathrm{E}_{(q,q')} \sum_{a,a'} \langle \Psi | \left(\sqrt{P_q^a} \otimes \mathrm{Id} - \mathrm{Id} \otimes \sqrt{P_q^a} \right) \left(\mathrm{Id} \otimes P_{q'}^{a'} \right) \left(\sqrt{P_q^a} \otimes \mathrm{Id} - \mathrm{Id} \otimes \sqrt{P_q^a} \right) | \Psi \rangle \right)^{1/2} \\
&\leq \left(2 - 2 \mathrm{E}_q \sum_a \langle \Psi | \sqrt{P_q^a} \otimes \sqrt{P_q^a} | \Psi \rangle \right)^{1/2} \\
&\leq \sqrt{2\delta},
\end{aligned}$$

where the second line follows from the Cauchy-Schwarz inequality and $V(a,a'|q,q') \leq 1$ and the last uses the definition of δ and $\sqrt{P_q^a} \geq P_q^a$ since $0 \leq P_q^a \leq \mathrm{Id}$ for every q, a. A similar sequence of inequalities results in the bound

$$\left| \langle \Psi | Y | \Psi \rangle - \langle \Psi | X \otimes \mathrm{Id} \, | \Psi \rangle \right| \leq \sqrt{2\delta},$$

and combining the two proves the lemma for $r = 2$. For general r the proof is the same but the operators corresponding to players $2, \ldots, r$ need to be brought to the first register one at a time, so that the error is $(r-1)$ times what it is for $r = 2$. □

Claim 5.10. *Let $\varepsilon > 0$, $r \geq 2$, $0 \leq R \leq \mathrm{Id}$ be such that $\langle R, \mathrm{Id} \rangle_\Psi \geq 1/2$, $\delta := \langle R, \mathrm{Id} - R \rangle_\Psi$, and $|\Phi\rangle := (\mathrm{Id} - R)^{\otimes r} |\Psi\rangle / z$, where $z = \| (\mathrm{Id} - R)^{\otimes r} |\Psi\rangle \|$. Then*

$$\left\| (\mathrm{Id} - R)^{\otimes r} |\Psi\rangle - \left(\mathrm{Id}^{\otimes (r-1)} \otimes (\mathrm{Id} - R) \right) |\Psi\rangle \right\|^2 \leq r^2 \delta, \tag{19}$$

and it holds that

$$z^2 \geq 1 - \langle R, \mathrm{Id} \rangle_\Psi - 3r\sqrt{\delta}. \tag{20}$$

Moreover, there is an $\varepsilon' = O(r(\varepsilon^{1/4} + \delta^{1/4}) \langle \mathrm{Id} - R, \mathrm{Id} \rangle_\Psi^{-1/2})$ such that for any symmetric r-player game H and projective symmetric strategy $(P, |\Psi\rangle)$ for the players that has success $1 - \varepsilon$ in H and is ε-self-consistent the strategy $(P, |\Phi\rangle)$ has success at least $1 - \varepsilon'$ in H.

Proof. Let $|\tilde{\Phi}\rangle := (\mathrm{Id} - R)^{\otimes r} |\Psi\rangle$. We first evaluate

$$\begin{aligned}
\left\| |\tilde{\Phi}\rangle - \left(\mathrm{Id} \otimes (\mathrm{Id} - R)^{\otimes (r-1)} \right) |\Psi\rangle \right\|^2 &= \left\| R \otimes (\mathrm{Id} - R)^{\otimes (r-1)} |\Psi\rangle \right\|^2 \\
&\leq \langle R, \mathrm{Id} - R \rangle_\Psi \\
&= \delta.
\end{aligned}$$

Repeating a similar inequality r times and using the triangle inequality shows (19). Let X be the operator whose existence is guaranteed by Claim 5.9. Since by assumption the strategy $(P, |\Psi\rangle)$ is ε-self-consistent, the claim shows that

$$\langle \Psi | X \otimes \mathrm{Id}^{\otimes (r-1)} \, | \Psi \rangle \geq 1 - \varepsilon - 2(r-1)\sqrt{2\varepsilon}. \tag{21}$$

Let $|\tilde{\Psi}\rangle = |\Psi\rangle - |\tilde{\Phi}\rangle$. By (19) it holds that

$$\left\| |\tilde{\Psi}\rangle - \left(\mathrm{Id}^{\otimes (r-1)} \otimes R \right) |\Psi\rangle \right\|^2 \leq r^2 \delta, \tag{22}$$

so that

$$\||\tilde{\Psi}\rangle\|^2 \leq \left(\langle R^2, \mathrm{Id}\rangle_\Psi^{1/2} + r\sqrt{\delta}\right)^2 \tag{23}$$

$$\leq \langle R, \mathrm{Id}\rangle_\Psi + 2r\sqrt{\delta} + r^2\delta, \tag{24}$$

where we used $R^2 \leq R$ since $R \leq \mathrm{Id}$. Using that $|\Psi\rangle$ is a unit vector, (19) also implies

$$\begin{aligned} z^2 &= \||\tilde{\Phi}\rangle\|^2 \\ &\leq \left\|\left(\mathrm{Id}^{\otimes(r-1)} \otimes (\mathrm{Id} - R)\right)|\Psi\rangle\right\|^2 + 2r\sqrt{\delta} + r^2\delta \\ &\leq \langle\Psi|\,\mathrm{Id}^{\otimes(r-1)} \otimes (\mathrm{Id} - R)|\Psi\rangle + 2r\sqrt{\delta} + r^2\delta \\ &= 1 - \langle R, \mathrm{Id}\rangle_\Psi + 3r^2\sqrt{\delta}, \end{aligned} \tag{25}$$

where for the third line we used $(\mathrm{Id} - R)^2 \leq (\mathrm{Id} - R)$ since $0 \leq R \leq \mathrm{Id}$. We may also obtain a bound in the other direction as

$$\begin{aligned} z^2 &\geq \left\|\left(\mathrm{Id}^{\otimes(r-1)} \otimes (\mathrm{Id} - R)\right)|\Psi\rangle\right\|^2 - 2r\sqrt{\delta} \\ &\geq \langle\Psi|\,\mathrm{Id}^{\otimes(r-2)} \otimes (\mathrm{Id} - R) \otimes (\mathrm{Id} - R)|\Psi\rangle - 2r\sqrt{\delta} \\ &\geq 1 - \langle R, \mathrm{Id}\rangle_\Psi - \delta - 2r\sqrt{\delta}, \end{aligned}$$

where here the second line follows from the Cauchy-Schwarz inequality and the third uses the definition of δ. This proves (20). Combining (24) and (25) we obtain that

$$z^{-2}(1 - \||\tilde{\Psi}\rangle\|^2) \;\geq\; 1 - 6r^2\sqrt{\delta}/\langle R, \mathrm{Id}\rangle_\Psi. \tag{26}$$

From (21) we get

$$\begin{aligned} 1 - \varepsilon - 2(r-1)\sqrt{2\varepsilon} &\leq \langle\Psi|X|\Psi\rangle \\ &= \langle\tilde{\Psi}|X|\tilde{\Psi}\rangle + \langle\tilde{\Phi}|X|\tilde{\Phi}\rangle + 2\Re\langle\tilde{\Psi}|X|\tilde{\Phi}\rangle \\ &\leq \||\tilde{\Psi}\rangle\|^2 + z^2\langle\Phi|X|\Phi\rangle \\ &\quad + 2|\langle\Psi|X(\mathrm{Id} - R) \otimes (\mathrm{Id} - R)^{\otimes(r-2)} \otimes R(\mathrm{Id} - R)|\Psi\rangle| + 2r\sqrt{\delta}, \end{aligned}$$

where for the last inequality we used (22). Using the Cauchy-Schwarz inequality and consistency of R, the third term above is at most $2\sqrt{\delta}$. Re-arranging terms we see that

$$\langle\Phi|X|\Phi\rangle \;\geq\; z^{-2}\big(1 - \||\tilde{\Psi}\rangle\|^2 - (\varepsilon + 2(r-1)\sqrt{2\varepsilon} + 2(r+1)\sqrt{\delta}\big),$$

which using (26) and the assumption on $\langle R, \mathrm{Id}\rangle_\Psi$ shows $\langle\Phi|X|\Phi\rangle \geq 1 - \Omega(r^2(\sqrt{\varepsilon} + \sqrt{\delta})(\langle \mathrm{Id} - R, \mathrm{Id}\rangle_\Psi^{-1})$. The same calculation can be done replacing X by the operator $Y = \mathrm{E}_q \sum_a P_q^a \otimes P_q^a$ that represents the player's consistency, showing that $(P, |\Phi\rangle)$ is $O(r^2(\sqrt{\varepsilon} + \sqrt{\delta})\langle \mathrm{Id} - R, \mathrm{Id}\rangle_\Psi^{-1})$-self-consistent. We may thus apply Claim 5.9 to finish the proof. □

We end this section with the proof of Proposition 5.8.

Proof of Proposition 5.8. Let ε, r, H, P, $|\Psi\rangle$, X and $(G_x, A_x, \mathcal{G}_x)$ be as in the statement of the proposition. Let K be such that for any $\varepsilon' < K$ it holds that $\eta(\varepsilon') \leq 1/4$. This is possible since $\eta(\varepsilon') \to 0$ as $\varepsilon' \to 0$.

By assumption, $(G_x, A_x, \mathcal{G}_x)_\Psi$ is a (δ, μ)-robust triple, and there is a family of sub-measurements $\{Q_x^g\}$ that is η_1-consistent with A_x and η_1-complete, where $\eta_1 = \eta(\varepsilon)$. Given our choice of ε, $\eta_1 < 1/2$, hence we may apply Lemma 5.4 (for every x) to deduce the existence of sub-measurements $\{\tilde{Q}_x^g\}$ that are (on average over $x \in X$) η_2-consistent with A_x, η_2 projective and $(\eta_1 + \eta_2)$-complete, where $\eta_2 = \eta'(\varepsilon)$. Among all sub-measurements that are η_2-consistent with A_x and η_2-projective, let $\{R_x^g\}$ be the one that has the smallest completeness parameter. Note that the existence of $\tilde{Q}_x$ implies that necessarily $\langle R, \mathrm{Id}\rangle_\Psi \geq 1 - (\eta_1 + \eta_2) \geq 1/2$, where as usual $R = \mathrm{E}_{x\in X} \sum_g R_x^g$.

If $\langle \mathrm{Id} - R, \mathrm{Id}\rangle_\Psi \leq \eta_2^{1/4}$ then we are done. Otherwise, let $\varepsilon_2 := \varepsilon'(\varepsilon, \eta_2, R) = O(\eta_2^{1/8})$, where ε' is as defined in Claim 5.10. Let $|\tilde{\Phi}\rangle := (\mathrm{Id} - R)^{\otimes r}|\Psi\rangle$, $z = \||\tilde{\Phi}\rangle\|$ and $|\Phi\rangle := |\tilde{\Phi}\rangle/z$. By Claim 5.10, the strategy $(P, |\Phi\rangle)$ has success $1 - \varepsilon_2$ in H. The assumption made in the proposition thus guarantees the existence of another family of sub-measurements $\{S_x^g\}$ that is η_3-consistent with A_x and η_3-complete for some $\eta_3 = \eta(\varepsilon_2)$. Provided K is chosen small enough, using $\eta(\varepsilon') \to 0$ as $\varepsilon' \to 0$ it holds that $\eta_3 < 1/4$. Consider a new family of sub-measurements $T_x = \{T_x^g\}$, where for every $g \in \mathcal{G}$,

$$T_x^g := RR_x^gR + (\mathrm{Id} - R)S_x^g(\mathrm{Id} - R).$$

The $\{T_x^g\}$ are clearly non-negative, and sum to at most Id since both $\{R_x^g\}$ and $\{S_x^g\}$ do. Moreover,

$$\begin{aligned}
\mathrm{E}_x \sum_g \langle T_x^g, \mathrm{Id} - A_x^g\rangle_\Psi &= \mathrm{E}_x \sum_g \langle RR_x^gR, \mathrm{Id} - A_x^g\rangle_\Psi + \mathrm{E}_x \sum_g \langle \Psi|(\mathrm{Id} - R)S_x^g(\mathrm{Id} - R) \otimes (\mathrm{Id} - A_x^g)|\Psi\rangle \\
&\leq \mathrm{E}_x \sum_g \langle \Psi|R_x^g \otimes \mathrm{Id} - A_x^g \otimes R|\Psi\rangle + 3\sqrt{\eta_2} \\
&\quad + z^2 \mathrm{E}_x \sum_g \langle \Phi|S^g \otimes (\mathrm{Id} - A^g)|\Phi\rangle + 2\Big\||\tilde{\Phi}\rangle - \big((\mathrm{Id} - R) \otimes \mathrm{Id}^{(r-1)}\big)|\Psi\rangle\Big\| \\
&\leq \eta_2 + z^2\eta_3 + 6r\sqrt{\eta_2}, \qquad (27)
\end{aligned}$$

where the second line uses projectivity of R for the first term, and the last inequality uses consistency of S with A for the second term and (19) for the third. Moreover, we can evaluate

$$\begin{aligned}
\langle T, \mathrm{Id}\rangle_\Psi &= \langle R^3, \mathrm{Id}\rangle_\Psi + \langle (\mathrm{Id} - R)S(\mathrm{Id} - R), \mathrm{Id}\rangle_\Psi \\
&\geq \langle R, \mathrm{Id}\rangle_\Psi - 3\sqrt{\eta_2} + z^2\langle \Phi|S \otimes \mathrm{Id}\,|\Phi\rangle - 2\Big\||\tilde{\Phi}\rangle - \big((\mathrm{Id} - R) \otimes \mathrm{Id}^{(r-1)}\big)|\Psi\rangle\Big\| \\
&\geq \langle R, \mathrm{Id}\rangle_\Psi + z^2(1 - \eta_3) - 6r\sqrt{\eta_2}, \qquad (28)
\end{aligned}$$

where in the second line we used projectivity of R, and for the last we used (19) as well as the completeness condition on S. Applying Lemma 5.4 to the T_x, we deduce the existence of a family of sub-measurements V_x that is η_2-consistent with A_x and projective, and such that

$$\begin{aligned}
\langle V, \mathrm{Id}\rangle_\Psi &\geq \langle T, \mathrm{Id}\rangle_\Psi - \big(\eta_2 + z^2\eta_3 + 3r\sqrt{\eta_2}\big) - \eta_2 \\
&\geq \langle R, \mathrm{Id}\rangle_\Psi + z^2(1 - 2\eta_3) - O\big(r\sqrt{\eta_2}\big),
\end{aligned}$$

where the first line uses (27) and the second (28). Comparing with our assumption that among all sub-measurements that are η_2-consistent with A and projective R had the smallest completeness parameter, and using $\eta_3 \leq 1/4$, from (28) we get that $z^2 = O(r\sqrt{\eta_2})$. Using the bound $z^2 \geq 1 - \langle R, \mathrm{Id}\rangle_\Psi - 3r\sqrt{\eta_2}$ which follows from (20) we see that necessarily $1 - \langle R, \mathrm{Id}\rangle_\Psi = O(r\sqrt{\eta_2})$. Finally, to conclude we make R into a complete family of measurements by adding $\mathrm{Id} - R_x$ to an arbitrary term R_x^g, for every x. □

6 Analysis of the low-degree test

In this section we prove Theorems 3.1 and 3.2. We first prove Theorem 3.1 in Sections 6.1 to 6.5; the proof of Theorem 3.2 is given in Section 6.6.

Fix $0 < \varepsilon \leq 1/2$, $d \geq 1$, $m \geq 2$ and $r \geq 3$. Let $(|\Psi\rangle, A, C)$ be a strategy with success $1-\varepsilon$ in the $(d, m, r, \mathbb{F})$ low-degree-test described in Figure 1. The test accepts in two cases. First, the referee automatically accepts if the two directions $\vec{y}_1, \vec{y}_2$ are not independent, which happens with probability at most $(1+|\mathbb{F}|)/|\mathbb{F}|^m \leq 2/|\mathbb{F}| \leq \varepsilon$ given the assumption on $q = |\mathbb{F}|$ made in the theorem. Second, the referee accepts provided the players are consistent. Thus an overall acceptance probability of $1-\varepsilon$ implies that the following must hold:

$$\mathrm{E}_{p \in \mathcal{S}_2(\mathbb{F}^m)} \mathrm{E}_{\boldsymbol{x} \in p} \sum_{h, a:\, a \neq h(\boldsymbol{x})} \langle A^a_{\boldsymbol{x}}, C^h_p \rangle_\Psi \leq 2\varepsilon, \tag{29}$$

where $\langle \cdot, \cdot \rangle_\Psi$ is defined in Section 2 (to which we refer for an introduction to the notation used in this section), the first expectation is taken over the choice of a uniformly random 2-dimensional affine subspace p of $\mathbb{F}^m$, and the second over a uniformly random point $x \in p$.

The proof of Theorem 3.1 is by induction on $m \geq 2$. For $m = 2$ there is a unique plane s in $\mathbb{F}^2$, hence the players have a unique "planes" measurement $\{C^g\}_{g \in \mathcal{P}_d(\mathbb{F}^2)}$. By setting $M^g := C^g$ for every g, Eq. (29) implies the conclusion of the theorem, provided C_1 is chosen to be at least 2.

We now assume that Theorem 3.1 is true for some dimension $(m-1) \geq 2$ and for every $\varepsilon, d, r, \mathbb{F}$ satisfying the assumptions of the theorem. We will prove the theorem for dimension m (and every $\varepsilon, d, r, \mathbb{F}$ satisfying the assumptions). The proof is divided in three steps. In the first step, carried out in Section 6.3, we show that the induction hypothesis implies the existence of a family of measurements $\{Q^g_s\}$, defined for every $s \in \mathcal{S}_{m-1}(\mathbb{F}^m)$ and with outcomes $g \in \mathcal{P}_d(s)$ that are consistent with $\{A^a_{\boldsymbol{x}}\}$ (Lemma 6.8). In Section 6.4 we show how the measurements Q_s can be combined together in a sequence of measurements $\{Q^{(h_i)}_{(s_i)}\}$, where $k \geq 1$ and $(s_i)_{1 \leq i \leq k}$ are parallel $(m-1)$ dimensional subspaces, with outcomes $h_i \in \mathcal{P}_d(s_i)$ (Lemma 6.11). Finally, in Section 6.5 we show that if k is large enough these measurements can be transformed into a single measurement $\{M^h\}$ with outcomes $h \in \mathcal{P}_d(\mathbb{F}^m)$ that satisfies the conclusion of Theorem 3.1 (Claim 6.15). We begin by stating some useful direct consequences of (29).

6.1 The lines measurements

In this section we define a "lines" family of projective measurements $\{B^g_\ell\}_{g \in \mathcal{P}_d(\ell)}$, defined for every $\ell \in \mathcal{S}_1(\mathbb{F}^m)$, and we show that these measurements, together with the "points" and "planes" measurements, A and C, that form the players' strategy all enjoy good joint consistency properties.

Lemma 6.1. *There exists a constant d_c such that the following holds. Let $(d+1)/|\mathbb{F}| < \varepsilon \leq 1/2$ and suppose that $\{A^a_{\boldsymbol{x}}\}$ and $\{C^h_p\}$ are projective measurements such that* (29) *holds. Then for every line $\ell \in \mathcal{S}_1(\mathbb{F}^m)$ there exists a projective measurement $\{B^g_\ell\}_{g \in \mathcal{P}_d(\ell)}$ such that, if for every $\boldsymbol{x} \in \mathbb{F}^m$ and $a \in \mathbb{F}$ we define*

$$B^a_{\boldsymbol{x}} := \mathrm{E}_{\ell \in \mathcal{S}_1(\mathbb{F}^m),\, \ell \ni \boldsymbol{x}} \sum_{g \in \mathcal{P}_d(\ell):\, g(\boldsymbol{x}) = a} B^g_\ell \qquad \text{and} \qquad C^a_{\boldsymbol{x}} := \mathrm{E}_{p \in \mathcal{S}_2(\mathbb{F}^m),\, p \ni \boldsymbol{x}} \sum_{h \in \mathcal{P}_d(p):\, h(\boldsymbol{x}) = a} C^h_p,$$

and for $\ell \in \mathcal{S}_1(\mathbb{F}^m)$ and $g \in \mathcal{P}_d(\ell)$,

$$C^g_\ell := \mathrm{E}_{p \in \mathcal{S}_2(\mathbb{F}^m),\, p \supset \ell} \sum_{h:\, h_{|\ell} = g} C^h_p,$$

then the following hold

$$\max\Big\{\mathrm{E}_{x\in\mathbb{F}^m}\sum_{a\in\mathbb{F}}\big\|B_x^a-A_x^a\big\|_\Psi^2,\ \mathrm{E}_{x\in\mathbb{F}^m}\sum_{a\in\mathbb{F}}\big\|C_x^a-A_x^a\big\|_\Psi^2,\ \mathrm{E}_{\ell\in\mathcal{S}_1(\mathbb{F}^m)}\sum_{g\in\mathcal{P}_d(\ell)}\big\|B_\ell^g-C_\ell^g\big\|_\Psi^2\Big\}\ =\ O\big(\varepsilon^{d_c}\big), \tag{30}$$

and

$$\max\Big\{\mathrm{E}_{x\in\mathbb{F}^m}\sum_{\substack{a,b\in\mathbb{F}\\ a\neq b}}\langle A_x^a,A_x^b\rangle_\Psi,\ \mathrm{E}_{\ell\in\mathcal{S}_1(\mathbb{F}^m)}\sum_{\substack{g,g'\in\mathcal{P}_d(\ell)\\ g\neq g'}}\langle B_\ell^g,B_\ell^{g'}\rangle_\Psi,\ \mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)}\sum_{\substack{h,h'\in\mathcal{P}_d(p)\\ h\neq h'}}\langle C_p^h,C_p^{h'}\rangle_\Psi\Big\}\ =\ O\big(\varepsilon^{d_c}\big). \tag{31}$$

We note that although all properties stated in the lemma follow from (29), we could have obtained them directly, and with a somewhat better dependence on ε, by assuming the existence of a strategy $(A,B,C,|\Psi\rangle)$ with success $1-\varepsilon$ in the following slight variant of the low-degree test from Figure 1. Let as usual $(d,m,\mathbb{F})$ be input parameters, and perform the following:

1. Choose a random $x\in\mathbb{F}^m$ and two random directions $\vec{y}_1,\vec{y}_2\in\mathbb{F}^m$. Accept if the two vectors are not linearly independent. Otherwise, let p be the plane $(x;\vec{y}_1,\vec{y}_2)$ and ℓ the line $(x;\vec{y}_1)$.
2. Select two players at random and send them one out of the nine possible pairs of questions $(u,v)\in\{x,\ell,p\}\times\{x,\ell,p\}$, chosen uniformly at random.
3. Receive $g\in\mathcal{P}_d(u)$ from the first player and $h\in\mathcal{P}_d(v)$ from the second. Accept if and only if g and h are consistent on the intersection of their respective domains.

Nevertheless, we opt to work with the standard low-degree test as described in Figure 1, which is somewhat more concise. We first show the following claim, which establishes the part of the lemma that has to do with the measurements A and C only.

Claim 6.2. *Suppose that $\{A_x^a\}$ and $\{C_p^h\}$ are projective measurements satisfying* (29)*. Then the following holds:*

$$\mathrm{E}_{x\in\mathbb{F}^m}\sum_a\big\|A_x^a-C_x^a\big\|_\Psi^2\ =\ O\big(\sqrt{\varepsilon}\big). \tag{32}$$

Moreover, the families of measurements A and C are both self-consistent:

$$\mathrm{E}_{x\in\mathbb{F}^m}\sum_{a\neq b}\langle A_x^a,A_x^b\rangle_\Psi=O\big(\varepsilon^{1/4}\big), \tag{33}$$

$$\mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)}\sum_{h\neq h'}\langle C_p^h,C_p^{h'}\rangle_\Psi=O\big(\varepsilon^{1/4}\big). \tag{34}$$

Proof. We first evaluate

$$\begin{aligned}\mathrm{E}_{x\in\mathbb{F}^m}\sum_a\big\|A_x^a\otimes\mathrm{Id}-\mathrm{Id}\otimes C_x^a\big\|_\Psi^2&=2-2\,\mathrm{E}_{x\in\mathbb{F}^m}\sum_a\langle A_x^a,C_x^a\rangle_\Psi\\&=2-2\,\mathrm{E}_x\mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m):\,p\ni x}\sum_{h,a:\,a=h(x)}\langle A_x^a,C_p^h\rangle_\Psi\\&\leq 4\,\varepsilon,\end{aligned} \tag{35}$$

where for the first equality we used the assumption that A and C are projective, for the second the definition of C^a_x and the last inequality follows from (29). Thus

$$\begin{aligned}
\mathrm{E}_{x\in\mathbb{F}^m}\sum_a \left\|A^a_x - C^a_x\right\|^2_\Psi &= 2 - 2\,\mathrm{E}_x\sum_a \Re\big(\mathrm{Tr}_\rho(A^a_x C^a_x)\big)\\
&= 2 - 2\,\mathrm{E}_x\sum_a \langle A^a_x, A^a_x\rangle_\Psi + 2\,\mathrm{E}_x\sum_a \Re\big(\mathrm{Tr}_\rho\big((A^a_x\otimes \mathrm{Id})(C^a_x\otimes\mathrm{Id} - \mathrm{Id}\otimes A^a_x)\big)\big)\\
&\leq 2 - 2\,\mathrm{E}_x\sum_a \langle A^a_x, A^a_x\rangle_\Psi + 2\sqrt{4\varepsilon}\\
&= 2 - 2\,\mathrm{E}_x\sum_a \langle A^a_x, C^a_x\rangle_\Psi + 2\,\mathrm{E}_x\sum_a \Re\big(\mathrm{Tr}_\rho\big((A^a_x\otimes \mathrm{Id})(A^a_x\otimes\mathrm{Id} - \mathrm{Id}\otimes C^a_x)\big)\big)\\
&\quad + 2\sqrt{4\varepsilon}\\
&\leq 4\varepsilon + 8\sqrt{\varepsilon},
\end{aligned}$$

where for the third and last lines we used the Cauchy-Schwarz inequality and (35), and in the fourth line we used that the number of players $r \geq 3$ and the permutation-invariance of $|\Psi\rangle$. This proves (32). Consistency for A can be verified as

$$\begin{aligned}
\mathrm{E}_{x\in\mathbb{F}^m}\sum_{a\neq b}\langle A^a_x, A^b_x\rangle_\Psi &= \mathrm{E}_{x\in\mathbb{F}^m}\sum_{a\neq b}\langle A^a_x, C^b_x\rangle_\Psi + \mathrm{E}_{x\in\mathbb{F}^m}\sum_a\langle A^a_x, A^a_x - C^a_x\rangle_\Psi\\
&\leq 2\,\varepsilon + \Big(\mathrm{E}_{x\in\mathbb{F}^m}\sum_a \left\|A^a_x\right\|^2_\Psi\Big)^{1/2}\Big(\mathrm{E}_{x\in\mathbb{F}^m}\sum_a \left\|A^a_x - C^a_x\right\|^2_\Psi\Big)^{1/2}\\
&= O\big(\varepsilon^{1/4}\big),
\end{aligned}$$

and a similar chain of inequalities proves consistency for C as well. □

We turn to the proof of the lemma.

Proof of Lemma 6.1. For every line $\ell \in \mathcal{S}_1(\mathbb{F}^m)$ and $g \in \mathcal{P}_d(\ell)$, define

$$\tilde{B}^g_\ell := C^g_\ell = \mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m),\, p\supset\ell}\sum_{h:h_{|\ell}=g} C^h_p. \tag{36}$$

We verify that the $\tilde{B}$ are self-consistent:

$$\begin{aligned}
\mathrm{E}_\ell\sum_{g\neq g'}\langle \tilde{B}^g_\ell, \tilde{B}^{g'}_\ell\rangle_\Psi &= \mathrm{E}_\ell\mathrm{E}_{p,p'\supset\ell}\sum_{h,h':h_{|\ell}\neq h'_{|\ell}}\langle C^h_p, C^{h'}_{p'}\rangle_\Psi\\
&= \mathrm{E}_\ell\mathrm{E}_{p,p'\supset\ell}\mathrm{E}_{x\in\ell}\sum_{h,h':h_{|\ell}\neq h'_{|\ell}}\sum_{a,b}\langle C^h_p A^a_x, C^{h'}_{p'}A^b_x\rangle_\Psi\\
&= \mathrm{E}_\ell\mathrm{E}_{p,p'\supset\ell}\mathrm{E}_{x\in\ell}\sum_{h,h':h_{|\ell}\neq h'_{|\ell}}\langle C^h_p A^{h(x)}_x, C^{h'}_{p'}A^{h'(x)}_x\rangle_\Psi + O\big(\varepsilon^{1/4}\big)\\
&= \mathrm{E}_\ell\mathrm{E}_{p,p'\supset\ell}\mathrm{E}_{x\in\ell}\sum_{\substack{h,h':h_{|\ell}\neq h'_{|\ell}\\ h(x)=h'(x)}}\langle C^h_p A^{h(x)}_x, C^{h'}_{p'}A^{h'(x)}_x\rangle_\Psi + O\big(\varepsilon^{1/8}\big)\\
&= O\big(\varepsilon^{1/8}\big),
\end{aligned} \tag{37}$$

where the third line uses (29) and the fact that C is projective, the fourth (33) and the Cauchy-Shwarz inequality, and the last that two distinct degree-d polynomials on ℓ intersect in a fraction at most $(1+d)/|\mathbb{F}| \leq \varepsilon$ of points given our assumption on $q = |\mathbb{F}|$. Applying Markov's inequality, we deduce from (37) that for all but a fraction at most $O(\varepsilon^{1/16})$ of lines ℓ, the measurement $\{B_\ell^g\}$ is self-consistent. For these ℓ we can apply the *orthogonalization lemma* from [KV11], which for convenience is restated as Lemma 6.4 below. The lemma guarantees the existence of a universal constant $c_p > 0$ and a family of projective measurements $\{\tilde{B}_\ell^g\}$ such that

$$\sum_g \left\| B_\ell^g - \tilde{B}_\ell^g \right\|_\Psi^2 = O\big(\varepsilon^{c_p/16}\big). \tag{38}$$

For the remaining ℓ we define $\{\tilde{B}_\ell^g\}$ arbitrarily (one of them is identity, the others 0). Together with (32), the definition of $\tilde{B}$ and the triangle inequality, (38) proves (30) provided d_c is chosen small enough. Given that self-consistency of A and C have already been proven in Claim 6.2, to conclude the proof of the lemma it remains to establish consistency of B, which follows immediately from (37), (38) and the Cauchy-Schwarz inequality. □

We also state the following useful consequence of Lemma 6.1.

Claim 6.3. *Under the same assumptions as in Lemma 6.1, for any family of sub-measurements $\{T_p^g\}_{g\in\mathcal{P}_d(p)}$, defined for every plane $p \in \mathcal{S}_2(\mathbb{F}^m)$, it holds that*

$$\mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)} \sum_{h\in\mathcal{P}_d(p)} \left\langle T_p^h, \left(\mathrm{E}_{x\in p} A_x^{h(x)} - C_p^h\right)^2 \right\rangle_\Psi = O\big(\varepsilon^{d_c}\big), \tag{39}$$

and

$$\mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)} \sum_{h\in\mathcal{P}_d(p)} \left\langle T_p^h, \left(\mathrm{E}_{\ell\subset p} B_\ell^{h_{|\ell}} - C_p^h\right)^2 \right\rangle_\Psi = O\big(\varepsilon^{d_c/2}\big). \tag{40}$$

Proof. To show (39), expand the square and use

$$\begin{aligned}
\mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)} \sum_{h\in\mathcal{P}_d(p)} \mathrm{E}_{x\in p} \big\langle T_p^h, A_x^{h(x)} C_p^h \big\rangle_\Psi &\approx_{\varepsilon^{d_c}} \mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)} \sum_{h\in\mathcal{P}_d(p)} \mathrm{E}_{x\in p} \big\langle T_p^h C_p^h, A_x^{h(x)} C_p^h \big\rangle_\Psi \\
&\approx_{\varepsilon^{d_c}} \mathrm{E}_{p\in\mathcal{S}_2(\mathbb{F}^m)} \sum_{h\in\mathcal{P}_d(p)} \mathrm{E}_{x\in p} \big\langle T_p^h C_p^h, A_x^{h(x)} \big\rangle_\Psi \\
&\approx_{\varepsilon} \mathrm{E}_{\substack{p\in\mathcal{S}_2(\mathbb{F}^m) \\ x\in p}} \sum_{h\in\mathcal{P}_d(p)} \big\langle T_p^h, A_x^{h(x)} \big\rangle_\Psi,
\end{aligned}$$

where the first and second lines follow from (31) and the third from (29). Similar bounds for the other terms appearing in the expansion of the square suffice to prove (39). To show (40) one proceeds in the same way, using the Cauchy-Schwarz inequality and (30) and then (31) in lieu of (39) to perform the third step above. □

We end with a statement of the orthogonalization lemma, a slightly simplified version of [KV10, Lemma 23].

Lemma 6.4 (Orthogonalization lemma)**.** *Let $\{A_i\}$ be a measurement and $|\Psi\rangle$ a permutation-invariant state such that*

$$\sum_i \langle A_i, A_i \rangle_\Psi \geq 1 - \varepsilon.$$

Then there exists a projective measurement $\{B_i\}$ such that

$$\sum_i \|A_i - B_i\|_\Psi^2 = O(\varepsilon^{c_p}),$$

where $c_p > 0$ is a universal constant.

6.2 Robust triples

The proof of the induction step $(m-1) \to m$ requires successive applications of the "consolidation" proposition, Proposition 5.8. For this we will use different "robust triples" (see Definition 5.2), which are defined in this section.

Let $1 \le k \le m$, $s \in \mathcal{S}_k(\mathbb{F}^m)$, G_s the complete graph on the vertex set defined by the points in s, and $\mathcal{G}_s = \mathcal{P}_d(s)$. Let $\mathcal{T}_s = (G_s, \{B_z^a\}, \mathcal{G}_s)$, where the measurements $\{B_z^a\}$ are as defined in Lemma 6.1.

Claim 6.5. *The triple $\mathcal{T}_s$ is $(O(\varepsilon^{d_c/4}), 1/2)$-robust for all but a fraction at most $O(\varepsilon^{d_c/4})$ of $s \in \mathcal{S}_k(\mathbb{F}^m)$, where $d_c > 0$ is the constant from Lemma 6.1.*

Proof. Using (30) and (31) we have

$$\mathrm{E}_{s\in\mathcal{S}_k(\mathbb{F}^m)}\mathrm{E}_{z\in s}\sum_{a\in\mathbb{F}}\big\langle B_z^a, \mathrm{Id} - B_z^a\big\rangle_\Psi \approx_{\varepsilon^{d_c/2}} \mathrm{E}_{s\in\mathcal{S}_k(\mathbb{F}^m)}\mathrm{E}_{z\in s}\sum_{a\in\mathbb{F}}\big\langle A_z^a, \mathrm{Id} - A_z^a\big\rangle_\Psi = O\big(\varepsilon^{d_c}\big).$$

Applying Markov's inequality, the measurements B are $O(\varepsilon^{d_c/4})$ self-consistent for all but a fraction at most $O(\varepsilon^{d_c/4})$ of subspaces s. For any $s \in \mathcal{S}_k(\mathbb{F}^m)$ let $\{R_s^g\}$ be an arbitrary sub-measurement. We have

$$\begin{aligned}
&\mathrm{E}_{s\in\mathcal{S}_k(\mathbb{F}^m)}\mathrm{E}_{z,z'\in s}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, \big(B_z^{g(z)} - B_{z'}^{g(z')}\big)^2\big\rangle_\Psi \\
&\approx_{q^{-1}} 2\,\mathrm{E}_{s\in\mathcal{S}_k(\mathbb{F}^m)}\mathrm{E}_{z\in s}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, \big(B_z^{g(z)}\big)^2\big\rangle_\Psi - 2\Re\Big(\mathrm{E}_{\substack{s\in\mathcal{S}_k(\mathbb{F}^m)\\ p\in\mathcal{S}_2(s),\, z,z'\in p}}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, B_z^{g(z)}B_{z'}^{g(z')}\big\rangle_\Psi\Big), \quad (41)
\end{aligned}$$

where we used that two uniformly distributed $z, z' \in s$ can equivalently (up to an error in statistical distance of $O(1/|\mathbb{F}|)$) be sampled by first choosing a uniformly random plane $p \subset s$ and then two uniform points $z, z' \in p$. To estimate the second term above, write

$$\begin{aligned}
\mathrm{E}_{\substack{s\in\mathcal{S}_k(\mathbb{F}^m)\\ p\in\mathcal{S}_2(s),\, z,z'\in p}}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, B_z^{g(z)}B_{z'}^{g(z')}\big\rangle_\Psi &\approx_{\varepsilon^{d_c/2}} \mathrm{E}_{\substack{s\in\mathcal{S}_k(\mathbb{F}^m)\\ p\in\mathcal{S}_2(s),\, z,z'\in p}}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, A_z^{g(z)}A_{z'}^{g(z')}\big\rangle_\Psi \\
&\approx_{\varepsilon^{d_c/2}} \mathrm{E}_{\substack{s\in\mathcal{S}_k(\mathbb{F}^m)\\ p\in\mathcal{S}_2(s)}}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, C_p^g C_p^g\big\rangle_\Psi \\
&\approx_{\varepsilon^{d_c/2}} \mathrm{E}_{\substack{s\in\mathcal{S}_k(\mathbb{F}^m)\\ p\in\mathcal{S}_2(s),\, z\in p}}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, B_z^{g(z)}\big\rangle_\Psi,
\end{aligned}$$

where the first line follows from the Cauchy-Schwarz inequality and (30), the second from (39) and the last uses pojectivity of the $\{C_p^g\}$ and (30). Together with (41), we obtain

$$\mathrm{E}_{s\in\mathcal{S}_k(\mathbb{F}^m)}\mathrm{E}_{z,z'\in s}\sum_{g\in\mathcal{P}_d(s)}\big\langle R_s^g, \big(B_z^{g(z)} - B_{z'}^{g(z')}\big)^2\big\rangle_\Psi = O\big(\varepsilon^{d_c/2} + q^{-1}\big).$$

Applying Markov's inequality and assuming the constant d_1 from Theorem 3.1 is chosen small enough that $dq^{-1} \leq \varepsilon^{d_c/2}$, we have thus shown that the measurements B are $O(\varepsilon^{d_c/4})$-stable for all but a fraction at most $O(\varepsilon^{d_c/4})$ of subspaces s. Finally, the small intersection property required in the definition of a robust triple follows from the Schwarz-Zippel lemma, and the expansion property trivially holds for the complete graph G_s. □

We generalize the previous construction to tuples of k parallel subspaces $s_i \in \mathcal{S}_{m-1}(\mathbb{F}^m)$. For any $z \in \mathbb{F}^m$ and $a \in \mathbb{F}$ let $X^a_z := B^a_z$, and for any $k \geq 2$, k-tuple of aligned points $z_1, \ldots, z_k \in \mathbb{F}^m$ and any $a_1, \ldots, a_k \in \mathbb{F}$ let

$$X^{(a_i)}_{(z_i)} := \sum_{\substack{g \in \mathcal{P}_d(\ell(z_i)) \\ \forall i, g(z_i) = a_i}} B^g_{\ell(z_i)}, \tag{42}$$

where $\ell(z_i)$ is the line going through the z_i. Let $V_{(s_i)}$ be the set of all k-tuples of aligned points $(z_1, \ldots, z_k)$, where $z_i \in s_i$, and $G_{(s_i)}$ the complete graph on V. Let $\mathcal{G}_{(s_i)} \subseteq \{g : V_{(s_i)} \to \mathbb{F}^k\}$ be the set of all k-tuples of degree-d $(m-1)$-variate polynomials (g_i), where $g_i \in \mathcal{P}_d(s_i)$. Finally, let $\mathcal{T}_{(s_i)} = (G_{(s_i)}, \{X^{(a_i)}_{(z_i)}\}, \mathcal{G}_{(s_i)})$.

Lemma 6.6. *Let $2 \leq k \leq 2d$. The triple $\mathcal{T}_{(s_i)}$ is $(O(\varepsilon^{d_c/4}), 1/2)$-robust for all but a fraction at most $O(\varepsilon^{d_c/4})$ of k-tuples $(s_i) \in (\mathcal{S}_{m-1}(\mathbb{F}^m))^k$.*

Proof. We verify the four properties needed of a robust triple. Expansion is clear, since the graph is complete. The property of small intersection follows from the Schwartz-Zippel lemma. Next we verify self-consistency.

$$\begin{aligned}
\mathrm{E}_{(s_i),(z_i)\in(s_i)} \sum_{(a_i)\neq(a'_i)} \big\langle X^{(a_i)}_{(z_i)}, X^{(a'_i)}_{(z_i)} \big\rangle_\Psi &= \mathrm{E}_{(s_i),(z_i)\in(s_i)} \sum_{(a_i)\neq(a'_i)} \sum_{g,g' : \forall i, g(z_i)=a_i, g'(z_i)=a'_i} \big\langle B^g_{\ell(z_i)}, B^{g'}_{\ell(z_i)} \big\rangle_\Psi \\
&\leq \mathrm{E}_{(s_i),(z_i)\in(s_i)} \sum_{g\neq g'} \big\langle B^g_{\ell(z_i)}, B^{g'}_{\ell(z_i)} \big\rangle_\Psi \\
&= O(\varepsilon^{d_c}),
\end{aligned} \tag{43}$$

where the last equality follows from (31). It remains to prove stability. For any k-tuple (s_i), let $\{R^g_{(s_i)}\}$ be an arbitrary sub-measurement with outcomes $g = (g_i) \in \mathcal{G}_{(s_i)}$. We abuse notation and also use g to designate the unique polynomial of degree $(d+k-1)$ defined on the whole of $\mathbb{F}^m$ that has degree at most d when restricted to each s_i, and at most $(k-1)$ when restricted to any line $\ell(z_i)$, where $z_i \in s_i$. Such a polynomial can be obtained by interpolation from the g_i. (Uniqueness follows since equality on every line $\ell(z_i)$ implies equality on $\mathbb{F}^m$.) For simplicity of notation, we also write R^g and omit the expectation over (s_i). We have

$$\begin{aligned}
&\mathrm{E}_{(z_i),(z'_i)\in(s_i)} \sum_g \big\langle R^g, \big(X^{(g(z_i))}_{(z_i)} - X^{(g(z'_i))}_{(z'_i)}\big)^2 \big\rangle_\Psi \\
&\quad\leq \mathrm{E}_{(z_i),(z'_i)\in(s_i)} \sum_g \big\langle R^g, \big(B^{g_{|\ell(z_i)}}_{\ell(z_i)} - B^{g_{|\ell(z'_i)}}_{\ell(z'_i)}\big)^2 \big\rangle_\Psi + 2\,\mathrm{E}_{(z_i)} \sum_g \sum_{\substack{h\in\mathcal{P}_d(\ell(z_i)), h\neq g_{|\ell} \\ h(z_i)=g(z_i)}} \big\langle R^g, B^h_{\ell(z_i)} \big\rangle_\Psi \\
&\quad\leq \mathrm{E}_{\ell,\ell'} \sum_g \big\langle R^g, \big(B^{g_{|\ell}}_\ell - B^{g_{|\ell'}}_{\ell'}\big)^2 \big\rangle_\Psi + 2\,\mathrm{E}_\ell \sum_{g,h:\, h\neq g_{|\ell}} \Pr_{(z_i)\in\ell} \big(\forall i, h(z_i) = g(z_i)\big) \big\langle R^g_{(s_i)}, B^h_\ell \big\rangle_\Psi \\
&\quad\leq \mathrm{E}_{\ell,\ell'} \sum_g \big\langle R^g, \big(B^{g_{|\ell}}_\ell - B^{g_{|\ell'}}_{\ell'}\big)^2 \big\rangle_\Psi + O\big(dkq^{-1}\big),
\end{aligned} \tag{44}$$

where for the first inequality we used the definition of X and orthogonality of the B_ℓ^h to separate out those terms for which $h = g_{|\ell}$ and $h \neq g_{|\ell}$ (but still $h(z_i) = g(z_i)$ for every i), and for the last we used the Schwartz-Zippel lemma. This last term can then be bounded exactly as the analogue term was bounded to establish the stability property in the proof of Claim 6.5, using (40) instead of (39). This establishes the stability property for the X measurements, on average over the choice of the k-tuple (s_i). Applying Markov's inequality proves the lemma (provided the constant d_1 from Theorem 3.1 is chosen small enough that $2d^2q^{-1} \leq \varepsilon^{c_d/2}$). □

The following claim establishes consistency of X with A.

Claim 6.7. *For any $k \geq 1$ and $(z_1, \ldots, z_k) \in (\mathbb{F}^m)^k$ the $\{X^{(a_i)}_{(z_i)}\}_{(a_i)\in\mathbb{F}^k}$ form a projective measurement. Moreover, for any $1 \leq j \leq k$ we have*

$$\mathrm{E}_{(z_i)\in(\mathbb{F}^m)^k} \sum_{(a_i)\in\mathbb{F}^k} \sum_{a:\, a\neq a_j} \langle X^{(a_i)}_{(z_i)}, A^a_{z_j}\rangle_\Psi \;=\; O\big(\varepsilon^{d_c/2}\big).$$

Proof. If $k = 1$ the claim is immediate by definition of $X^{a_1}_{z_1}$ and (30), (31). If $k \geq 2$,

$$\begin{aligned}
\mathrm{E}_{(z_i)} \sum_{(a_i)} \sum_{a\neq a_j} \big\langle X^{(a_i)}_{(z_i)}, A^a_{z_j}\big\rangle_\Psi &= \mathrm{E}_{(z_i)} \sum_{(a_i)} \sum_{a\neq a_j} \sum_{g:\forall i,\, g(z_i)=a_i} \big\langle B^g_{\ell(z_i)}, A^a_{z_j}\big\rangle_\Psi \\
&\leq \mathrm{E}_\ell \mathrm{E}_{z_j\in\ell} \sum_{g,a:\, a\neq g(z_j)} \big\langle B^g_\ell, A^a_{z_j}\big\rangle_\Psi \\
&= O\big(\varepsilon^{d_c/2}\big).
\end{aligned}$$

Here the inequality follows simply by ignoring the constraint that $g(z_i) = a_i$ for all indices but $i = j$, and the last follows from the case $k = 1$. □

6.3 The measurements Q_s

Recall that we set to prove Theorem 3.1 by induction on m. Our first step is to prove that the induction hypothesis can be used to deduce the existence of a family of measurements $\{Q_s\}$ parameterized by $(m-1)$-dimensional subspaces s of $\mathbb{F}^m$ that are consistent with the measurements $\{A_z\}$ coming from the players' strategy.

Lemma 6.8. *There exists a universal constant $0 < c_\ell \leq d_c/400$ such that the following holds. Under the assumptions of Theorem 3.1, for every $s \in \mathcal{S}_{m-1}(\mathbb{F}^m)$ there exists a measurement $\{Q^g_s\}_{g\in\mathcal{P}_d(s)}$ such that*

$$\mathrm{E}_{s\in\mathcal{S}_{m-1}(\mathbb{F}^m)} \mathrm{E}_{x\in s} \sum_{g,a:\, a\neq g(x)} \langle Q^g_s, A^a_x\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big).$$

Fix an $s \in \mathcal{S}_{m-1}(\mathbb{F}^m)$. We call s-restricted $(d, m-1, \mathbb{F})$ low-degree test the variant of the low-degree test in which the referee chooses $(z, \vec{y}_1, \vec{y}_2)$ uniformly in s, and then proceeds as in the usual test. We claim the following.

Claim 6.9. *For a fraction at least $1 - O(\varepsilon^{-2}q^{-1})$ of $(m-1)$-dimensional subspaces s, the strategy $(|\Psi\rangle, A, C)$ has success at least $1 - 3\varepsilon$ in the s-restricted $(d, m-1, \mathbb{F})$-low-degree test.*

Proof. In the $(d, m, \mathbb{F})$ low-degree test over $\mathbb{F}^m$, the referee picks a triple $(z, \vec{y}_1, \vec{y}_2)$ uniformly at random in $\mathbb{F}^m$, automatically accepts if $(\vec{y}_1, \vec{y}_2)$ are not linearly independent, and proceeds if they are; conditioned on not accepting immediately the resulting plane $p = (z; \vec{y}_1, \vec{y}_2)$ is uniformly distributed in $\mathcal{S}_2(\mathbb{F}^m)$.

Consider now a referee who selects random $(z, \vec{y}_1, \ldots, \vec{y}_{m-1})$ in $\mathbb{F}^m$, automatically accepts if they are not linearly independent, and proceeds with the plane $p = (z; \vec{y}_1, \vec{y}_2)$ if they are. Conditioned on the referee not accepting immediately, the subspace $s = (z; \vec{y}_1, \ldots, \vec{y}_{m-1})$ is uniformly distributed in $\mathcal{S}_{m-1}(\mathbb{F}^m)$, and p is uniformly distributed in $\mathcal{S}_2(s)$. Hence the only difference between the two scenarios is in the probability of accepting immediately. In both cases, it follows from [AS97, Lemma 10] that this probability is upper bounded by $2/q$ (but it is higher in the second scenario). In particular, the players' success probability in the second scenario, conditioned on not having accepted immediately, is at least $1 - \varepsilon - 2/q$, so that

$$\mathrm{E}_s\left[1 - \varepsilon_s\right] \geq 1 - \varepsilon - \frac{2}{q},$$

where ε_s is the players' success in the s-restricted $(d, m-1, \mathbb{F})$-low-degree test. To conclude it suffices to perform a variance analysis exactly as in [AS97, Lemma 12]. One then obtains that, for any $\alpha > 0$,

$$\Pr_s\left(1 - \varepsilon_s \leq (1-\alpha)(1-\varepsilon-2/q)\right) \leq O\left(\alpha^{-2} q^{-1}\right).$$

Choosing $\alpha = \varepsilon$, provided q is large enough with respect to ε^{-1} the claim is proved. □

We turn to the proof of the lemma.

Proof of Lemma 6.8. Let $s \in \mathcal{S}_{m-1}(\mathbb{F}^m)$. If the strategy $(|\Psi\rangle, A, C)$ has success at least $1 - 3\varepsilon$ in the s-restricted $(d, m-1, \mathbb{F})$-low-degree test, by applying the induction hypothesis Theorem 3.1 implies the existence of a measurement $\{Q_s^g\}$ which satisfies

$$\mathrm{E}_{x \in s} \sum_{a \in \mathbb{F}} \sum_{g:\, g(x) \neq a} \left\langle A_x^a, Q_s^g \right\rangle_\Psi \leq C_1 (3\varepsilon)^{c_1}.$$

Using (30) and the Cauchy-Schwarz inequality we also obtain that $\{Q_s^g\}$ is δ-consistent with $\{B_z^a\}$ for some $\delta = O(\varepsilon^{c_1} + \varepsilon^{d_c/2})$. Define the Q_s arbitrarily for the remaining subspaces s. Let $\mathcal{S}$ be the set of all s for which the triple $\mathcal{T}_s$ defined in Claim 6.5 is $(O(\varepsilon^{d_c/4}), 1/2)$-robust. Claim 6.5 shows that a fraction at least $1 - O(\varepsilon^{d_c/4})$ of s (assuming $d_c \leq 1$) are in $\mathcal{S}$. Using Claim 6.9, we thus get

$$\mathrm{E}_{s \in \mathcal{S}} \sum_{a \in \mathbb{F}} \sum_{g:\, g(x) \neq a} \left\langle B_x^a, Q_s^g \right\rangle_\Psi \leq 2\delta,$$

provided the constant d_1 from Theorem 3.1 is chosen large enough.

We are in a position to apply Proposition 5.8, with the set X there being $\mathcal{S}$ here. The proposition shows that, provided ε is small enough, for every $s \in \mathcal{S}$ there exists an "improved" measurement, such that on average over $s \in \mathcal{S}$ the $\{Q_s^g\}$ are $O((\eta'(\varepsilon^{d_c/4}, 1/2))^{1/2})$-consistent with the $\{B_x^a\}$, where η' is as in Lemma 5.4. For the remaining subspaces s we define $\{Q_s^g\}$ arbitrarily. Using (31) to relate consistency with B to consistency with A, the lemma is proved provided c_ℓ is chosen small enough ($c_\ell = d_c/40$ suffices). □

As a corollary of Lemma 6.8, the following claim shows that the measurements $\{Q_s\}$ are self-consistent.

Claim 6.10. *The measurements* $\{Q_s^g\}_{g\in\mathcal{P}_d(s)}$ *satisfy*

$$\mathrm{E}_{s\in\mathcal{S}_{m-1}(\mathbb{F}^m)}\sum_{g\in\mathcal{P}_d(s)}\langle Q_s^g,(\mathrm{Id}-Q_s^g)\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big),$$

where c_ℓ *is as defined in Lemma 6.8.*

Proof. We can write

$$\begin{aligned}\mathrm{E}_{s\in\mathcal{S}_{m-1}(\mathbb{F}^m)}\sum_{g,g'\in\mathcal{P}_d(s),g\neq g'}\langle Q_s^g,Q_s^{g'}\rangle_\Psi &\approx_{\varepsilon^{c_\ell}} \mathrm{E}_{s\in\mathcal{S}_{m-1}(\mathbb{F}^m)}\mathrm{E}_{\boldsymbol{x}\in s}\sum_{g,g'\in\mathcal{P}_d(s),g\neq g'}\mathrm{Tr}_\rho\big(Q_s^g\otimes Q_s^{g'}\otimes A_{\boldsymbol{x}}^{g(\boldsymbol{x})}\big)\\ &= O\big(\varepsilon^{c_\ell}\big),\end{aligned}$$

where both lines follow from consistency of Q with A. □

6.4 Pasting the Q_s

In this section we combine the k measurements $\{Q_{s_i}^h\}_{h\in\mathcal{P}_d(s_i)}$, $1\le i\le k$, obtained from Lemma 6.8 for any k-tuples of parallel subspaces $s_i\in\mathcal{S}_{m-1}(\mathbb{F}^m)$ into a single measurement $\{Q_{(s_i)}^{(h_i)}\}_{h_i\in\mathcal{P}_d(s_i)}$. Let $\{X_{(z_i)}^{(a_i)}\}_{a_i\in\mathbb{F}}$ be the measurements defined in (42) for every k-tuple of aligned points $\boldsymbol{z}_i\in\mathbb{F}^m$.

Lemma 6.11. *For any* $k\ge 1$, $(m-1)$*-tuple of linearly independent directions* $\vec{y}_1,\dots,\vec{y}_{m-1}\in\mathbb{F}^m$ *and* k*-tuple of aligned points* $\boldsymbol{z}_1,\dots,\boldsymbol{z}_k\in\mathbb{F}^m$*, letting* $s_i=(z_i;\vec{y}_1,\dots,\vec{y}_{m-1})$ *there exists a family of measurements* $\{Q_{(s_i)}^{(h_i)}\}_{(h_i)\in(\mathcal{P}_d(s_i))}$ *such that*

$$\mathrm{E}_{\vec{y}_i,\boldsymbol{z}_i}\sum_{\substack{h_i\in\mathcal{P}_d(s_i),a_i\in\mathbb{F}\\ \exists i,a_i\neq h_i(\boldsymbol{z}_i)}}\big\langle Q_{(s_i)}^{(h_i)},X_{(z_i)}^{(a_i)}\big\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big), \tag{45}$$

where c_ℓ *is the constant defined in Lemma 6.8.*

We first prove the case $k=1$, which follows almost immediately from Lemma 6.8.

Claim 6.12. *The following holds:*

$$\mathrm{E}_{s\in\mathcal{S}_{m-1}(\mathbb{F}^m)}\mathrm{E}_{\boldsymbol{z}\in s}\sum_{h,a:\,a\neq h(\boldsymbol{z})}\big\langle Q_s^h,X_{\boldsymbol{z}}^a\big\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big).$$

Proof. By definition,

$$\begin{aligned}\mathrm{E}_{s\in\mathcal{S}_{m-1}(\mathbb{F}^m)}\mathrm{E}_{\boldsymbol{z}\in s}\sum_{h,a:\,a\neq h(\boldsymbol{z})}\big\langle Q_s^h,X_{\boldsymbol{z}}^a\big\rangle_\Psi &= \mathrm{E}_{s,\boldsymbol{z}}\sum_{h,a:\,a\neq h(\boldsymbol{z})}\big\langle Q_s^h,A_{\boldsymbol{z}}^a\big\rangle_\Psi+\mathrm{E}_{s,\boldsymbol{z}}\sum_{h,a:\,a\neq h(\boldsymbol{z})}\big\langle Q_s^h,(B_{\boldsymbol{z}}^a-A_{\boldsymbol{z}}^a)\big\rangle_\Psi\\ &\le O(\varepsilon^{c_\ell})+\Big(\mathrm{E}_{\boldsymbol{z}}\sum_a\big\|B_{\boldsymbol{z}}^a-A_{\boldsymbol{z}}^a\big\|_\Psi^2\Big)^{1/2}\\ &= O(\varepsilon^{c_\ell}),\end{aligned}$$

where the inequality uses Lemma 6.8 to bound the first term and Cauchy-Schwarz for the second, and the last follows from (30) and $c_\ell\le d_c/2$. □

We will use the following general "pasting" lemma.

Lemma 6.13. *Let S_1, S_2 be two disjoint sets and $\{Q^g\}$ and $\{R^h\}$ measurements with outcomes in $\mathcal{G} \subseteq \{g : S_1 \to \mathbb{F}\}$ and $\mathcal{H} \subseteq \{h : S_2 \to \mathbb{F}\}$ respectively. Suppose that Q and R are each consistent with a family of measurements $\{A_v^a\}_{a\in\mathbb{F}}$ defined for every $v \in S_1 \cup S_2$:*

$$\max\Big\{\mathrm{E}_{v\in S_1}\sum_{g,a:\, a\neq g(v)}\big\langle Q^g, A_v^a\big\rangle_\Psi,\ \mathrm{E}_{v\in S_2}\sum_{h,a:\, a\neq h(v)}\big\langle R^h, A_v^a\big\rangle_\Psi\Big\} \leq \delta,$$

for some $\delta > 0$, and that Q is δ-self-consistent. Then there exists a "pasted" measurement $\{T^f\}$, where $f = (f_1, f_2)$ and $f_1 : S_1 \to \mathbb{F}$, $f_2 : S_2 \to \mathbb{F}$, such that T is consistent with A:

$$\mathrm{E}_{v\in S_1\cup S_2}\sum_{f,a:\, a\neq f_1(v)}\big\langle T^f, A_v^a\big\rangle_\Psi \;=\; O\big(\sqrt{\delta}\big).$$

Proof. For any $f = (f_1, f_2)$ let $T^f := \sqrt{Q^{f_1}}R^{f_2}\sqrt{Q^{f_1}}$. Then $\{T^f\}$ is a measurement, and

$$\begin{aligned}
\mathrm{E}_{v\in S_1\cup S_2}\sum_{f,a:\, a\neq f(v)}\big\langle T^f, A_v^a\big\rangle_\Psi &= \frac{1}{|S_1|+|S_2|}\sum_{v\in S_1\cup S_2}\sum_{f,a:\, a\neq f(v)}\big\langle\sqrt{Q^{f_1}}R^{f_2}\sqrt{Q^{f_1}}, A_v^a\big\rangle_\Psi \\
&\leq \frac{1}{|S_1|+|S_2|}\sum_{v\in S_2}\sum_{f,a:\, a\neq f_2(v)}\big\langle\sqrt{Q^{f_1}}R^{f_2}\sqrt{Q^{f_1}}, A_v^a\big\rangle_\Psi + \frac{\delta|S_1|}{|S_1|+|S_2|} \\
&\approx_{\sqrt{\delta}} \frac{1}{|S_1|+|S_2|}\sum_{v\in S_2}\sum_{f,a:\, a\neq f_2(v)}\big\langle R^{f_2}, A_v^a Q^{f_1}\big\rangle_\Psi + \frac{\delta|S_1|}{|S_1|+|S_2|} \\
&= O\big(\sqrt{\delta}\big),
\end{aligned}$$

where the first inequality uses consistency of Q with A, the second uses self-consistency of Q, and the last consistency of R with A. □

We turn to the proof of Lemma 6.11.

Proof of Lemma 6.11. The proof of the lemma is by induction on k. The case $k = 1$ was proved in Claim 6.12. Assume the lemma true for $k-1$, and for any $(k-1)$-tuple $(s_i) \in (\mathcal{S}_{m-1}(\mathbb{F}^m))^{k-1}$ of parallel subspaces let $\{Q^g_{s_1\cup\cdots\cup s_{k-1}}\}_g$ be the resulting family of measurements: it holds that

$$\mathrm{E}_{(s_i),\, z_i\in s_i}\sum_{(h_i),(a_i):\, \exists i, a_i\neq h_i(z_i)}\big\langle Q^{(h_i)}_{(s_i)}, X^{(a_i)}_{(z_i)}\big\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big). \tag{46}$$

Moreover, from the case $k = 1$ the measurements $\{Q^g_s\}$ satisfy

$$\mathrm{E}_{s,\, z\in s}\sum_{h,a:\, a\neq h(z)}\big\langle Q^h_s, X^a_z\big\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big). \tag{47}$$

Let $(s_i) \in (\mathcal{S}_{m-1}(\mathbb{F}^m))^k$ be a k-tuple of parallel subspaces. By (46), (47), Claim 6.10, Markov's inequality and a union bound we see that for all but a fraction at most $O(\varepsilon^{c_\ell/2})$ of such tuples, it holds that both measurements $\{Q^{(h_1,\ldots,h_{k-1})}_{(s_1,\ldots,s_{k-1})}\}$ and $\{Q^h_{s_k}\}$ are $O(\varepsilon^{c_\ell/2})$-consistent with the corresponding X measurements, and moreover $\{Q^h_{s_k}\}$ is $O(\varepsilon^{c_\ell/2})$-self-consistent. We are thus in a position to apply Lemma 6.13, with the

set S_1 being the set of points in s_k and the set S_2 the set of points in $s_1 \cup \cdots \cup s_{i-1}$ (the measurements A being the corresponding X measurements). As a result, the lemma promises the existence of a measurement $\{Q^{(h_1,\ldots,h_k)}_{(s_1,\ldots,s_k)}\}$ for which we can write

$$\begin{aligned}
&\mathrm{E}_{z_i \in s_i} \sum_{\substack{(h_i),(a_i)\\ \exists i, a_i \neq h_i(z_i)}} \big\langle Q^{(h_i)}_{(s_i)}, X^{(a_i)}_{(z_i)} \big\rangle_\Psi \qquad (48)\\
&\quad = \mathrm{E}_{z_i \in s_i} \sum_{(h_i)} \sum_{\substack{g \in \mathcal{P}_d(\ell(z_i))\\ \exists i, g(z_i) \neq h_i(z_i)}} \big\langle Q^{(h_i)}_{(s_i)}, B^{g_{|\ell(z_i)}}_{\ell(z_i)} \big\rangle_\Psi\\
&\quad \leq \mathrm{E}_{z_i \in s_i} \sum_{(h_i)} \sum_{\substack{g \in \mathcal{P}_d(\ell(z_i))\\ \exists i \leq k-1, g(z_i) \neq h_i(z_i)}} \big\langle Q^{(h_i)}_{(s_i)}, B^{g_{|\ell(z_i)}}_{\ell(z_i)} \big\rangle_\Psi + \mathrm{E}_{z_k \in s_k, \ell \ni z_k} \sum_{(h_i)} \sum_{\substack{g \in \mathcal{P}_d(\ell)\\ g(z_k) \neq h_k(z_k)}} \big\langle Q^{(h_i)}_{(s_i)}, B^{g_{|\ell}}_{\ell} \big\rangle_\Psi\\
&\quad = \mathrm{E}_{z_i \in s_i} \sum_{(h_i)} \sum_{(a_i):\, \exists i \leq k-1, a_i \neq h_i(z_i)} \big\langle Q^{(h_i)}_{(s_i)}, X^{(a_i)}_{(z_i)} \big\rangle_\Psi + \mathrm{E}_{z_k \in s_k} \sum_{(h_i)} \sum_{a \neq h_k(z_k)} \big\langle Q^{(h_i)}_{(s_i)}, X^{a}_{z_k} \big\rangle_\Psi\\
&\quad = O\big(\varepsilon^{c_\ell/4}\big), \qquad (49)
\end{aligned}$$

where for the first and third lines we used the definition of X, and for the last we used the consistency properties of the Q measurements with the corresponding X promised by Lemma 6.13. For those k-tuples (s_i) for which we could not apply Lemma 6.13 we define $\{Q^{(h_i)}_{(s_i)}\}$ arbitrarily, obtaining as a result that (49) holds on average over the choice of a k-tuple (s_i).

To conclude the proof of the lemma we apply Proposition 5.8, with the set X there being the set $\mathcal{S}$ of k-tuples of subspaces for which the triple $\mathcal{T}_{(s_i)}$ introduced in Claim 6.6 is $(O(\varepsilon^{d_c/4}), 1/2)$-robust. The proposition shows that, provided ε is small enough, for every $(s_i) \in \mathcal{S}$ there exists an "improved" measurement $Q_{(s_i)}$ such that on average over $(s_i) \in \mathcal{S}$ the $\{Q^{(g_i)}_{(s_i)}\}$ are $O((\eta'(\varepsilon^{d_c/4}, 1/2))^{1/2})$-consistent with the $\{X^{(a_i)}_{(z_i)}\}$, where η' is as in Lemma 5.4. For the remaining subspaces (s_i) we keep the $Q_{(s_i)}$ as previously defined. Using the definition of η' and the fact that $c_\ell \leq d_c/40$, the lemma is proved. □

6.5 The measurements M^g

In this section we take the family of measurements $\{Q^{(g_i)}_{(s_i)}\}$ constructed in Lemma 6.11 and show that they can be transformed in a single measurement $\{M^g\}_{g \in \mathcal{P}_d(\mathbb{F}^m)}$ that satisfies the conclusion of Theorem 3.1.

Let $\{Q^{(g_1,\ldots,g_{d+1})}_{(s_1,\ldots,s_{d+1})}\}$ be the family of measurements obtained in Lemma 6.11 for $k = d+1$. By interpolation, from any tuple $g = (g_i)$ we may recover a single polynomial g of degree at most $2d$ defined on $\mathbb{F}^m$ and such that $g_{|s_i} = g_i$ for every $i = 1, \ldots, d+1$. This results in a family of measurements $\{R^g_{(s_1,\ldots,s_{d+1})}\}_{g \in \mathcal{P}_{2d}(\mathbb{F}^m)}$, where here we implicitly select one "representative" outcome $g \in \mathcal{P}_{2d}(\mathbb{F}^m)$ for every tuple (g_i) (as different degree-$2d$ polynomials may interpolate the same tuple). The following claim shows that we can in fact restrict our attention to interpolating polynomials of degree at most d.

Claim 6.14. *For every $(d+1)$-tuple of aligned subspaces (s_i) there exists a measurement $\{S^g_{(s_i)}\}_{g \in \mathcal{P}_d(\mathbb{F}^m)}$ such that*

$$\mathrm{E}_{(s_i)} \sum_{h \neq g_{|\ell}} \langle S^g_{(s_i)}, B^h_\ell \rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big).$$

Proof. First note that Lemma 6.11 and the definition of the measurements X implies the following:

$$\mathrm{E}_{(s_i),z_i\in s_i} \sum_{g\in\mathcal{P}_{2d}(\mathbb{F}^m)} \langle R^g_{(s_i)}, (\mathrm{Id} - B^{g_{|\ell}}_{\ell(z_i)})\rangle_\Psi \;=\; O\big(\varepsilon^{c_\ell}\big). \tag{50}$$

Note that B^h_ℓ is only defined for $h \in \mathcal{P}_d(\ell)$, but in general a degree-$(2d)$ polynomial will also have degree $2d$ when restricted to a line. Here though the definition of the X measurements shows that $g_{|\ell}$ should be interpreted as the degree-d polynomial obtained by interpolation from the values $(g(z_i))$.

Next we argue that the contribution of measurement outcomes corresponding to polynomials of degree strictly larger than d must be small.

$$\begin{aligned}\mathrm{E}_{(s_i)} \sum_{g,\,\deg(g)>d} \langle R^g_{(s_i)}, \mathrm{Id}\rangle_\Psi &\approx_{\varepsilon^{c_\ell}} \mathrm{E}_{(s_i),z,\ell,\ell'\ni z} \sum_{g,\,\deg(g)>d} \sum_{\substack{h(\ell\cap s_i)=g(\ell\cap s_i)\\ h'(\ell'\cap s_i)=g(\ell'\cap s_i)}} \mathrm{Tr}_\rho\big(R^g_{(s_i)}\otimes B^h_\ell \otimes B^{h'}_{\ell'}\big)\\ &= O\big(\varepsilon^{d_c/2}\big),\end{aligned}$$

where for the first line we applied (50) twice, and the second follows from the following argument. If g has degree $> d$, its restriction to all but a fraction at most $O(q^{-1})$ of lines ℓ also has degree $> d$ (see e.g. [MR08, Lemma 6.4]). Hence the degree-d polynomial recovered by interpolation from $(d+1)$ values of g at random aligned points $z_i \in \ell$ is unlikely to agree with $g_{|\ell}$ (since they have different degrees). Thus on the right-hand side of the first line above, the polynomial h (resp. h') will almost certainly disagree with g on a random point in ℓ (resp. ℓ') that is not in $\cup s_i$. The point z of intersection of ℓ and ℓ' is such a point, which gives the conclusion using (31) and (30). The measurements S can thus be defined as R when $\deg(g) \le d$, and made into a complete measurement by adding all $R^g_{(s_i)}$ for $\deg(g) > d$ to a single outcome of degree less than d for S (e.g. the $g \equiv 0$ outcome). Using $c_\ell \le d_c/2$, the claim is proved. □

Let $g \in \mathcal{P}_d(\mathbb{F}^m)$, and define

$$M^g \;:=\; \mathrm{E}_{(s_1,\ldots,s_{d+1})} S^g_{(s_i)}, \tag{51}$$

where the expectation is taken over all tuples of parallel $(m-1)$-dimensional subspaces s_i. Clearly $M^g \ge 0$ for every g. It also holds that $\sum_g M^g = \mathrm{Id}$. Indeed, for any $g \in \mathcal{P}_d(\mathbb{F}^m)$ and any tuple (s_i), $g_{|s_i}$ has degree at most d; moreover for any tuple $(g_i \in \mathcal{P}_d(s_i))$ there is at most one $g \in \mathcal{P}_d(\mathbb{F}^m)$ that interpolates all the g_i (indeed, any two such g should be 0 on each of $d+1$ parallel $(m-1)$-dimensional subspaces, hence should be 0 on all of $\mathbb{F}^m$). We conclude the proof of Theorem 3.1 by showing the following.

Claim 6.15. *Under the assumptions of Theorem 3.1 the measurement $\{M^g\}_{g\in\mathcal{P}_d(\mathbb{F}^m)}$ defined in* (51) *satisfies*

$$\mathrm{E}_x \sum_{g,a:\,a\neq g(x)} \big\langle M^g, A^a_x\big\rangle_\Psi \;=\; O\big(\varepsilon^{c_1}\big),$$

where $c_1 \le 1$ is a universal constant.

Proof. We have

$$\begin{aligned}\mathrm{E}_x \sum_{g,a:\,a\neq g(x)} \big\langle M^g, A^a_x\big\rangle_\Psi &= \mathrm{E}_{(s_i),x} \sum_{g,a:\,a\neq g(x)} \big\langle S^g_{(s_i)}, A^a_x\big\rangle_\Psi\\ &\approx_{\varepsilon^{d_c/2}} \mathrm{E}_{(s_i),x} \sum_{g,a:\,a\neq g(x)} \big\langle S^g_{(s_i)}, B^a_x\big\rangle_\Psi\\ &= \mathrm{E}_{(s_i),x,\ell\ni x} \sum_{g,h:\,h(x)\neq g(x)} \big\langle S^g_{(s_i)}, B^h_\ell\big\rangle_\Psi\\ &= O\big(\varepsilon^{c_\ell}\big)\end{aligned}$$

where for the second line we used (30) and the last follows from Claim 6.14. □

6.6 Analysis of the two-level low-degree test

In this section we prove Theorem 3.2. Let $(|\Psi\rangle, A, B, C)$ be a strategy for the players with success probability at least $1-\varepsilon$ in the $(d, m, r, \mathbb{F})$ two-level low-degree test, as described in Figure 2. The probability that the referee accepts in steps 2. or 3. is at most $(1+|\mathbb{F}|)/|\mathbb{F}|^m \leq 2/|\mathbb{F}| \leq \varepsilon$ (given the assumption on $q = |\mathbb{F}|$ made in the theorem) for each step. Hence the strategy's success probability in steps 4.1 and 4.2 must be at least $1-6\varepsilon$ each, which immplies the following:

$$\mathrm{E}_{s\in\mathcal{S}_2(\mathbb{F}^m)}\mathrm{E}_{\boldsymbol{x}\in s}\sum_{a,b\in\mathbb{F},\,a\neq b}\left\langle A^a_{\boldsymbol{x}}, B^b_{s,\boldsymbol{x}}\right\rangle_\Psi \leq 6\varepsilon \tag{52}$$

$$\mathrm{E}_{\substack{s\in\mathcal{S}_2(\mathbb{F}^m)\\ s'\in\mathcal{S}_2(\mathbb{F}^{m'})}}\mathrm{E}_{\boldsymbol{x}'\in s'}\sum_{g'\in\mathcal{P}_{d'}(s')}\sum_{a'\in\mathbb{F},\,a'\neq g'(\boldsymbol{x}')}\left\langle C^{g'}_{s,s'}, B^{a'}_{s,\boldsymbol{x}'}\right\rangle_\Psi \leq 6\varepsilon \tag{53}$$

The following claim applies the analysis of the low-degree test to measurements B and C, separately for each $s\in\mathcal{S}_2(\mathbb{F}^m)$.

Claim 6.16. *For any $s\in\mathcal{S}_2(\mathbb{F}^m)$ there exists a measurement $\{M^g_s\}$ with outcomes $g\in\mathcal{P}_{dd'}(s)$ such that*

$$\mathrm{E}_{s\in\mathcal{S}_2(\mathbb{F}^m)}\mathrm{E}_{\boldsymbol{x}\in s}\sum_{g,a:\,a\neq g(\boldsymbol{x})}\left\langle A^a_{\boldsymbol{x}}, M^g_s\right\rangle_\Psi = O\big(\varepsilon^{c_1}\big), \tag{54}$$

where $c_1>0$ is the constant from Theorem 3.1.

Proof. Given a plane $s\in\mathcal{S}_2(\mathbb{F}^m)$ let ε_s be the value of the left-hand-side of (53) (for that s), so that $\mathrm{E}_s[\varepsilon_s]\leq 6\varepsilon$. By definition of ε_s, the strategy $(|\Psi\rangle, B_s, C_s)$ has success at least $1-\varepsilon_s$ in the $(d', m', r, \mathbb{F})$ low-degree test. Choosing the constant d_2 large enough, Markov's inequality implies that a fraction at least $1-\varepsilon$ of subspaces s are such that ε_s satisfies the assumptions of Theorem 3.1. For those s, applying the theorem we obtain a measurement $\{M^g_s\}_{g\in\mathcal{P}_{d'}(\mathbb{F}^{m'})}$ such that

$$\mathrm{E}_{\boldsymbol{x}\in s}\sum_{g,a:\,g(\boldsymbol{x})\neq a}\left\langle M^g_s, B^a_{s,\boldsymbol{x}}\right\rangle_\Psi = O\big(\varepsilon_s^{c_1}\big). \tag{55}$$

Translating g back to a function on $s\subseteq\mathbb{F}^m$, we may also thing of g as a bivariate polynomial with degree at most dd'. Using concavity of $z\to z^{c_1}$ (since $c_1\leq 1$) and the fact that (55) holds for all but an ε fraction of s we obtain

$$\mathrm{E}_{s\in\mathcal{S}_2(\mathbb{F}^m),\boldsymbol{x}\in s}\sum_{g\in\mathcal{P}_{dd'}(s)}\sum_{a:\,a\neq g(\boldsymbol{x})}\left\langle M^g_s, B^a_{s,\boldsymbol{x}}\right\rangle_\Psi = O\big(\varepsilon^{c_1}\big),$$

where for those s such that (55) we defined $\{M^g_s\}$ arbitrarily. Finally, using (52) it is not hard to see that this implies the claim. □

We turn to the proof of Theorem 3.2.

Proof of Theorem 3.2. For every $s\in\mathcal{S}_2(\mathbb{F}^m)$ let $\{M^g_s\}_{g\in\mathcal{P}_{dd'}(s)}$ be the measurement promised by Claim 6.16. The consistency relation (54) precisely states that the strategy $(|\Psi\rangle, A, M)$ has success probability at least $1-O(\varepsilon^{c_1})$ in the $(dd', m, r, \mathbb{F})$-low degree test. Provided the constant d_2 is chosen large enough, we may

apply Theorem 3.1 to that strategy to obtain a single measurement $\{\tilde{M}^h\}$ with outcomes $h \in \mathcal{P}_{dd'}(\mathbb{F}^m)$ satisfying

$$\mathrm{E}_{\boldsymbol{x}\in\mathbb{F}^m} \sum_{h\in\mathcal{P}_{dd'}(\mathbb{F}^m)} \sum_{a:\, a\neq h(\boldsymbol{x})} \big\langle \tilde{M}^h, A^a_{\boldsymbol{x}} \big\rangle_\Psi \;=\; O\big(\varepsilon^{c_1^2}\big),$$

which proves the theorem by choosing $c_2 = c_1^2$ and C_2 large enough. □

7 Analysis of additional tests

7.1 The 3-SAT test

In this section we analyze the protocol for 3-SAT given in Section 3.2 and prove Theorem 3.3. We note that the analysis is very standard in the PCP literature, and once the soundness of the low-degree test has been established virtually no additional complications are introduced from the consideration of entangled-player strategies (except maybe in terms of notational overhead).

Let φ be a 3-SAT formula on n variables, $\varepsilon > 0$ and $(|\Psi\rangle, A, B, C, D, E, F)$ an r-prover strategy with success $1-\varepsilon$ in the $(\varphi, n, r, \mathbb{F})$ 3-SAT test described in Figure 3. The following claim summarizes some initial consequences of the players' success in the test. For any clause $C \in \varphi$ on variables $x, y, z \in [n]$ we let $S(C)$ be the set of all degree-4 curves in $\mathbb{F}^m$ going through the points $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{z}$. For any $c \in S(C)$, we let $S(C,c)$ be the set of degree-4 curves in $\mathbb{F}^{m'}$ that go through $\#\boldsymbol{x}, \#\boldsymbol{y}, \#\boldsymbol{z}$, where the coordinate map $\#$ is determined by c.

Claim 7.1. *Under the assumptions of Theorem 3.3, there exists a measurement $\{M^g\}_{g\in\mathcal{P}_{dd''}(\mathbb{F}^m)}$, where $d'' = 2\lceil \log(d+1)\rceil$, such that the following hold:*

$$\mathrm{E}_{\boldsymbol{w}\in\mathbb{F}^m} \sum_{g,a:\, a\neq g(\boldsymbol{w})} \big\langle M^g, A^a_{\boldsymbol{w}} \big\rangle_\Psi \;=\; O\big(\varepsilon^{c_2}\big), \tag{56}$$

$$\mathrm{E}_{C\in\varphi}\mathrm{E}_{c\in S(C)}\mathrm{E}_{c'\in S(C,c)}\mathrm{E}_{\boldsymbol{w}\in c'} \sum_{g,a:\, a\neq g(\#\boldsymbol{w})} \big\langle F^g_{c,c'}, A^a_{\boldsymbol{w}} \big\rangle_\Psi \;=\; O\big(\varepsilon\big), \tag{57}$$

where $c_2 > 0$ is the constant from Theorem 3.2.

Proof. First we observe that the strategy $(|\Psi\rangle, A, B, C)$ must have success at least $1-2\varepsilon$ in the $(d, m, r, \mathbb{F})$ two-level low-degree test performed in step 2a. Provided d_3 is chosen small enough compared to d_2, Theorem 3.2 implies the existence of a measurement $\{M^g\}$, with outcomes in $\mathcal{P}_{dd'}(\mathbb{F}^m)$, that is $O(\varepsilon^{c_2})$-consistent with A, proving (56). To show (57), we first note that in step 2(b)ii the point $\boldsymbol{w}'$ is uniformly distributed in c', hence that test in particular enforces that

$$\mathrm{E}_{C\in\varphi}\mathrm{E}_{c\in S(C)}\mathrm{E}_{c'\in S(C,c)}\mathrm{E}_{\boldsymbol{w}'\in c'} \sum_{g,a:\, a\neq g(\#\boldsymbol{w}')} \big\langle F^g_{c,c'}, D^a_{c,\#\boldsymbol{w}'} \big\rangle_\Psi \;=\; O(\varepsilon). \tag{58}$$

Similarly, the first check performed as part of step 2(b)i in the protocol enforces that

$$\mathrm{E}_{C\in\varphi}\mathrm{E}_{c\in S(C)}\mathrm{E}_{c'\in S(C,c)}\mathrm{E}_{\boldsymbol{w}'\in c'} \sum_{a\neq b} \big\langle A^a_{\boldsymbol{w}'}, D^b_{c,\#\boldsymbol{w}'} \big\rangle_\Psi \;=\; O(\varepsilon). \tag{59}$$

Eq. (57) is proved by combining (58) and (59). □

For every polynomial $g \in \mathcal{P}_{dd''}(\mathbb{F}^m)$ and variable $x \in [n]$, let $Z(g,x) := g(\boldsymbol{x})$, where $\boldsymbol{x} \in \mathbb{F}^m$ is the point associated to variable x, be the assignment that g implicitly associates to x. Let $Z(g) \subseteq \{0,1\}^n$ denote the assignment to all variables implied by g. Let $S(\varphi) \subseteq \{0,1\}^n$ be the set assignments satisfying a fraction at least $1 - C_3\varepsilon^{c_3}$ of clauses of φ, where c_3, C_3 are constants as in the statement of Theorem 3.3 and defined in the proof of Claim 7.2 below.

Claim 7.2. *Under the assumptions of Theorem 3.3 it holds that*

$$\sum_{g:\, Z(g)\in S(\varphi)} \big\langle M^g, \mathrm{Id} \big\rangle_\Psi \;\geq\; 1 - C_3\varepsilon^{c_3}.$$

Note that the claim implies in particular that provided ε is small enough φ *has* an assignment to its variables satisfying a fraction at least $1 - C_3\varepsilon^{c_3}$ of clauses, proving Theorem 3.3 provided K_3 is chosen small enough.

Proof. Let $C = (x,y,z)$ be a clause, and $c = c(\boldsymbol{w})$ the degree-4 curve through $(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z},\boldsymbol{w})$, where $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z} \in \mathbb{F}^m$ are the points associated to the variables x,y,z respectively. For $(b,d,e) \in \{0,1\}^3$ we write $(b,d,e) \vdash C$ to indicate that the assignment $(x,y,z) := (b,d,e)$ satisfies the clause C. In step 2(b)ii of the protocol the referee accepts with probability at least

$$\begin{aligned}
1 - 4\varepsilon &\leq \mathrm{E}_{C=(x,y,z)\in\varphi} \mathrm{E}_{\substack{c\in S(C)\\ c'\in S(C,c)}} \sum_{(b,d,e)\vdash C} \sum_{\substack{g:\, g(\#\boldsymbol{x})=b, g(\#\boldsymbol{y})=d,\\ g(\#\boldsymbol{z})=e}} \big\langle F^g_{c,c'}, \mathrm{Id} \big\rangle_\Psi \\
&\leq \mathrm{E}_{C=(x,y,z)\in\varphi} \mathrm{E}_{\substack{c\in S(C)\\ c'\in S(C,c)\\ \boldsymbol{w}'\in c'}} \sum_{(b,d,e)\vdash C} \sum_{\substack{g:\, g(\#\boldsymbol{x})=b, g(\#\boldsymbol{y})=d, h:h(\boldsymbol{w}')=g(\#\boldsymbol{w}')\\ g(\#\boldsymbol{z})=e}} \mathrm{Tr}_\rho\big(F^g_{c,c'} \otimes M^h\big) + O\big(\varepsilon^{c_2}\big), \quad (60)
\end{aligned}$$

where the second equality follows from (56) and (57). The restriction of h to the curve c is a univariate polynomial of degree at most $4dd''$. Using variable substitution it is mapped to a polynomial on $\mathbb{F}^{m'}$ of total degree also at most $4dd''$, which when restricted to the degree-4 curve c' has degree at most $16dd''$. This polynomial is either equal to the degree-d' polynomial g, or, by the Schwartz-Zippel lemma, intersects it in a fraction at most $O(dd''/|\mathbb{F}|)$ of points, which is less than ε provided the constant d_3 is chosen large enough. Hence from (60) we get

$$\begin{aligned}
1 - O\big(\varepsilon^{c_2}\big) &\leq \mathrm{E}_{C=(x,y,z)\in\varphi} \mathrm{E}_{\substack{c\in S(C)\\ c'\in S(C,c)\\ \boldsymbol{w}'\in c'}} \sum_{(b,d,e)\vdash C} \sum_{\substack{g:\, g(\boldsymbol{x})=b, g(\boldsymbol{y})=d,\\ g(\boldsymbol{z})=e}} \big\langle F^{g_{|c,c'}}_{c,c'}, M^g \big\rangle_\Psi + \varepsilon \\
&\leq \mathrm{E}_{C=(x,y,z)\in\varphi} \mathrm{E}_{\substack{c\in S(C)\\ c'\in S(C,c)\\ \boldsymbol{w}'\in c'}} \sum_{(b,d,e)\vdash C} \sum_{\substack{g:\, g(\boldsymbol{x})=b, g(\boldsymbol{y})=d,\\ g(\boldsymbol{z})=e}} \big\langle M^g, \mathrm{Id} \big\rangle_\Psi + \varepsilon \\
&= \sum_{g\in\mathcal{P}_d(\mathbb{F}^m)} \mathrm{E}_{\substack{C=(x,y,z)\in\varphi\\ (g(\boldsymbol{x}),g(\boldsymbol{y}),g(\boldsymbol{z}))\vdash C}} \big\langle M^g, \mathrm{Id} \big\rangle_\Psi + \varepsilon, \quad (61)
\end{aligned}$$

where the last line is obtained by simplifying the expression. Given a polynomial g, let $\kappa(g)$ denote the fraction of clauses satisfied by the assignment to the variables of φ implicitly defined by g. Eq. (61) shows that

$$\sum_{g\in\mathcal{P}_d(\mathbb{F}^m)} \kappa(g) \langle M^g, \mathrm{Id}\rangle_\Psi \;\geq\; 1 - O\big(\varepsilon^{c_2}\big).$$

Since $(\langle M^g, \mathrm{Id}\rangle_\Psi)$ is a probability distribution over polynomials g, Markov's inequality implies that all but a fraction at most $O(\varepsilon^{c_2/2})$ of g chosen according to this distribution are such that $\kappa(g) \geq 1 - O(\varepsilon^{c_2/2})$. This proves the claim for an appropriate choice of constants $c_3 = c_2/2$ and C_3 large enough. □

7.2 The QUADEQ test

In this section we sketch the proof of Lemma 3.5. The analysis of the QUADEQ test as described in Figure 5 is rather standard (see e.g. [AB09, Theorem 11.19]). Here the only additional complications introduced by the consideration of entangled players appear in the analysis of the linearity test, which was already stated in Theorem 3.4.

First we note that the players' success probability of $1-\varepsilon$ implies a success probability of at least $1-16\varepsilon$ in each of the four linearity steps performed in step 1.1. of the protocol. Applying Theorem 3.4 four times, for each of the measurements A_1, A_2, B and C there exists a corresponding "linear" measurement $\{M^u_{A,1}\}_{u\in\mathbb{F}_2^{n/2}}$, $\{M^u_{A,2}\}_{u\in\mathbb{F}_2^{n/2}}$, $\{M^v_B\}_{v\in\mathbb{F}_2^n}$ and $\{M^z_C\}_{z\in\mathbb{F}_2^{n^2}}$ respectively that is $O(\sqrt{\varepsilon})$-consistent with it. Replacing the players' actions in steps 1.2–1.4. in the protocol by the ones induced by these linear measurements still results in them being accepted with probability at least $1-O(\sqrt{\varepsilon})$.

It is not hard to argue (see the proof of Claim 7.2 for a similar argument) that Step 1.4 in the protocol enforces that for a fraction at least $1-O(\varepsilon^{1/4})$ of outcomes z of the measurement M_C (under the distribution given by $(\langle M^z_C, \mathrm{Id}\rangle_\Psi)$) it holds that

$$\Pr_{w\in\mathbb{F}_2^{n^2}}\Big(\sum_k w_k\Big(\sum_{ij} z_{ij}\,a^{(k)}_{ij}\Big) \;=\; \sum_k w_k\,c^{(k)}\Big) \;\geq\; 1-O\big(\varepsilon^{1/4}\big).$$

For any such z, provided ε is small enough it is standard analysis to deduce that z defines an assignment to the n^2 "variables" x_ix_j that must satisfy *all* K equations in φ.

Finally, step 1.3 in the protocol enforces that a fraction at least $1-O(\sqrt{\varepsilon})$ of outcomes z of M_C are of the form $z = x\otimes x$ for some $x\in\mathbb{F}^n$. Indeed, any outcome which does not have this form will fail the test performed in step 1.3 with constant probability (over the choice of the questions and the outcomes of the other two measurements) whenever it is obtained.

Applying a union bound, we deduce that a fraction at least $1-O(\varepsilon^{1/4})$ of outcomes z of M_C are of the form (x,x) for some x defining a satisfying assignment to the variables in φ. Hence

$$\sum_{x\vdash\varphi}\langle M^{(x,x)}_C, \mathrm{Id}\rangle_\Psi \;=\; 1-O\big(\varepsilon^{1/4}\big), \tag{62}$$

and in particular whenever ε is small enough there must exist at least one such assignment, proving the first part of the lemma provided K_4 is chosen small enough.

To show the "furthermore" part of the lemma, we use step 1.2. of the protocol. The purpose of the test performed in that step is to enforce that the measurement M_B associated to a particular instance φ_t is consistent with the measurements $M_{A,i}$ and $M_{A,j}$ obtained from the two chunks ℓ_i and ℓ_j of variables appearing in φ_t, where here $M_{A,i}$ depends only on the label ℓ_i but not on the instance φ_t. Hence the players' success $1-4\varepsilon$ in that test together with (62) (and the consistency between M_B and M_C enforced in step 1.3) implies that

$$\sum_{(u_i,u_j)\vdash\varphi_t}\langle M^{u_i}_{A,i}, M^{u_j}_{A,j}\rangle_\Psi \;=\; 1-O\big(\varepsilon^{1/4}\big).$$

This finishes the proof of the lemma provided the constants c_4, C_4 are chosen appropriately.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, Dec 1982.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[Ara02] P. K. Aravind. The magic squares and Bell's theorem. Technical report, arXiv:quant-ph/0206070, 2002.

[AS97] Sanjeev Arora and Madhu Sudan. Improved low-degree testing and its applications. pages 485–495, New York, NY, USA, 1997. ACM.

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[Bel64] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Comput. Complexity*, 1:3–40, 1991.

[BFLS91] László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking computations in polylogarithmic time. pages 21–32, New York, NY, USA, 1991. ACM.

[BGLR93] Mihir Bellare, Shafi Goldwasser, Carsten Lund, and Alexander Russell. Efficient probabilistically checkable proofs and applications to approximations. pages 294–304, New York, NY, USA, 1993. ACM.

[BGS98] Mihir Bellare, Oded Goldreich, and Madhu Sudan. Free bits, PCPs, and nonapproximability—towards tight results. *SIAM J. Comput.*, 27(3):804–915, June 1998.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, 1993.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[CHTW04] Richard Cleve, Peter Høyer, Ben Toner, and John Watrous. Consequences and limits of non-local strategies. In *Proc. 19th IEEE Conf. on Computational Complexity (CCC'04)*, pages 236–249. IEEE Computer Society, 2004.

[DFK+11] Irit Dinur, Eldar Fischer, Guy Kindler, Ran Raz, and Shmuel Safra. PCP characterizations of NP: Toward a polynomially-small error-probability. *Comput. Complexity*, 20:413–504, 2011.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[FGL+96] Uriel Feige, Shafi Goldwasser, Laszlo Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *J. ACM*, 43(2):268–292, 1996.

[Gis91] Nicolas Gisin. Bell's inequality holds for all non-product states. *Phys. Lett. A*, 154:201 – 202, 1991.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charlie Rackoff. The knowledge complexity of interactive proof-systems. In *Proc. 17th STOC*, pages 291–304, New York, NY, USA, 1985. ACM.

[Hås01] Johan Håstad. Some optimal inapproximability results. *J. ACM*, 48:798–859, 2001.

[IKM09] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. pages 217–228, 2009.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled provers. Technical report, 2012. arXiv:1207.0550.

[KKM+11] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. *SIAM J. Comput.*, 40(3):848–877, 2011.

[KRR13] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. Delegation for bounded space. 2013.

[KRT10] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. *SIAM J. Comput.*, 39(7):3207–3229, 2010.

[KV10] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. Technical report, arXiv:1012.4728v2, 2010. Full version of [KV11].

[KV11] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proc. 43rd STOC*, pages 353–362, 2011.

[MR08] Dana Moshkovitz and Ran Raz. Sub-constant error low degree test of almost-linear size. *SIAM J. Comput.*, 38(1):140–180, 2008.

[MR10] Dana Moshkovitz and Ran Raz. Sub-constant error probabilistically checkable proof of almost-linear size. *Comput. Complexity*, 19(3):367–422, September 2010.

[Pre07] Daniel Preda, 2007. Unpublished.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27:763–803, 1998.

[RS96] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. Comput.*, 25(2):252–271, February 1996.

[RS97] Ran Raz and Shmuel Safra. A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP. pages 475–484, New York, NY, USA, 1997. ACM.

[Sch35] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 1935.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):707–717, 1980.

[Tsi80] Boris S. Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4:93–100, 1980.

[Vid11] Thomas Vidick. *The Complexity of Entangled Games*. PhD thesis, UC Berkeley, 2011.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation: An International Symposiumon on Symbolic and Algebraic Manipulation (EUROSM)*, volume 72, pages 216–226, 1979.