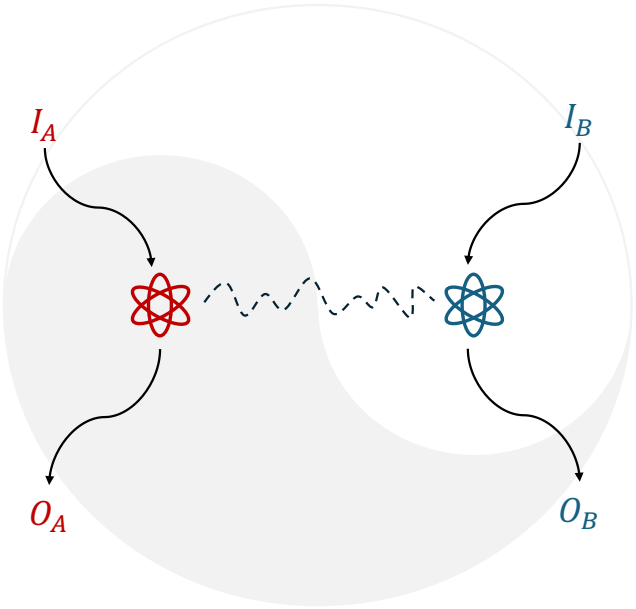
UNIVERSITY OF COPENHAGEN
DEPARTMENT OF MATHEMATICAL SCIENCES



Ph.d. thesis

Ranyiliu Chen

Black-box protocols for certification of quantum devices

Supervisor: Laura Manvcinska

This thesis has been submitted to the PhD School of The Faculty of Science, University of Copenhagen.

Institute:	QMATH
Department	Institut for Matematiske Fag
Author(s):	Ranyiliu Chen
Email:	ranyiliu.chen@outlook.com

Title:	Black-box protocols for certification of quantum devices
Supervisor:	Laura Mančinska, *Københavns Universitet*
Date of Submission:	31st October, 2024
Date of Defence:	10th January, 2025

ISBN:	978-87-7125-235-4

Assessment Committee:	Albert H. Werner (chair), *Københavns Universitet*
	Antonio Acín, *ICFO-Institut de Ciencies Fotoniques*
	Remigiusz Augusiak, *Polish Academy of Sciences*

This thesis has been submitted to the PhD School of The Faculty of Science, University of Copenhagen, Denmark. It received funding from European Union under the Grant Agreement No 101017733, VERIqTAS and VILLUM FONDEN via Villum Young Investigator grant (No 37532) and the QMATH Centre of Excellence (Grant No 10059).

Abstract

While the Born's rule allows us to predict the output statistics of quantum devices, inferring the underlying quantum functionality from these statistics without any prior knowledge of the device is generally difficult. Intriguingly, this challenge can be overcome by self-testing, a phenomenon where certain non-local statistics is exclusively produced by certain configuration of the devices.

This thesis contributes to a refined mathematical framework of self-testing from three aspects. First, via a detailed analysis of Naimark dilation, restriction, and purification transformations within non-local strategies we systematically remove the common assumptions under natural conditions. We can eliminate assumptions of purity, full-rankness, and projectivity, thereby lifting many existing self-testing protocols to their strongest form. We further identify specific instances where these assumptions remain necessary, by identifying a statistic that admit no pure, full-rank projective realization. A no-go result shows non-projective measurements can never be self-tested in the strongest sense.

Second, we delve into the issue of complex conjugate, refining the formulation of complex local dilation and complex self-testing where the definition of self-testing is relaxed to allow complex conjugation. A conjecture on the operator-algebraic structure of complex self-testing is proposed. Additionally, we revisit the notion of "reality" in quantum strategies, examining what it means for a strategy to be "real" and addressing subtleties within this concept.

Lastly, we introduce the first robust, assumption-free self-testing protocol applicable to any real projective measurement. This is achieved through a new theoretical method, post-hoc self-testing, which enables construction of self-tests from established ones. We further generalise this method in an iterative manner, paving the way for future developments in self-testing protocols across different classes of measurements.

Resumé

Selvom Born-reglen tillader os at forudsige output-statistikken af kvanteapparater, er det generelt svært at udlede den underliggende kvantefunktionalitet fra sådanne statistikker uden nogen forudgående viden om apparatet. Interessant nok kan denne udfordring overvindes ved selvtestning, et fænomen hvor visse ikke-lokale statistikker udelukkende produceres af bestemte konfigurationer af apparaterne.

Denne afhandling bidrager til en raffineret matematisk ramme for selvtestning ud fra tre aspekter. For det første fjerner vi systematisk de almindelige antagelser via en detaljeret analyse af Naimark-udvidelse, begrænsning og renheds-transformationer inden for ikke-lokale strategier. Vi kan eliminere antagelser om renhed, fuld rang og projektivitet og derved løfte eksisterende selvtestningsprotokoller til deres stærkeste form. Vi identificerer endvidere specifikke tilfælde, hvor disse antagelser forbliver nødvendige, ved at identificere en statistik, der ikke tillader nogen ren, fuldrang og projektiv strategi. Et no-go-resultat viser, at ikke-projektive målinger aldrig kan selvtestes i den stærkeste forstand.

For det andet dykker vi ned i spørgsmålet om kompleks konjugation og forfiner formuleringen af kompleks, lokal udvidelse og kompleks selvtestning, hvor definitionen af selvtestning er lempet for at tillade kompleks konjugation. En formodning om den operator-algebraiske struktur af kompleks selvtestning foreslås. Derudover genbesøger vi begrebet 'realitet' i kvantestrategier og undersøger, hvad det vil sige, at en strategi er 'reel', og adresserer subtile aspekter ved dette begreb.

Til sidst introducerer vi den første robuste, forudsætningsfrie selvtest-protokol, der kan anvendes til enhver reel projektiv måling. Dette opnås ved hjælp af en ny teoretisk metode, post-hoc selvtestning, som gør det muligt at konstruere selvtest ud fra allerede etablerede selvtest. Vi generaliserer yderligere denne metode på en iterativ måde, hvilket baner vejen for fremtidig udvikling af selvtestningsprotokoller på tværs af forskellige klasser af målinger.

Acknowledgement

At the very top of this long list of thank-yous is my highest appreciation for my PhD supervisor, Laura Mančinska. She is not only a renowned expert in my field but also an amazing mentor for a junior researcher. From her, I learned how to conduct rigorous and responsible research and how to present results in a comprehensive way. She has been invaluable in helping me build confidence and expand my professional network. I feel incredibly fortunate not only for her unending support but also for our shared interests and taste on scientific research—a feeling I hope is mutual.

I am also deeply grateful to two of my senior colleagues, Jurij Volčič and Simon Schmidt. Their vast knowledge and patience in answering my many (stupid) questions shaped the way I approach mathematics. Although we only worked together in person for two years, our collaboration continued even after they left Copenhagen, and I hope it will endure in the years to come. I wish them all the best for their futures.

I extend my thanks to all QMATH members for fostering such a vibrant and supportive working environment. I know it is rare to find such an engaging and non-hierarchical atmosphere in academia, and I appreciate everyone's efforts in building this remarkable team. My gratitude goes especially to Matthias Christandl and Jan Philip Solovej for their leadership, and administrative staff Suzanne Andersen and Lise Steen Nielsen, as well as my PhD/-postdoc fellows Pedro Baptista, Yuming Zhao, Lubashan Pathirana, Sigurd Storgaard, Elias Theil, Jakob Günther, Taro Spirig, Dylan Harley, Lukas Junge, Bhavik Kumar, Martin Dam Larsen, Vincent Steffan, Frederik Ravn Klausen, August Andersen Bjerg, for all the fun we had in group outings/weekend footballs. I am grateful for the sense of community here and glad to have contributed through events like Kulturnatten and master thesis's seminars.

My PhD journal was enriched by several academic visits. On this I would like to thank Māris Ozols for generously hosting my two-month exchange in QuSoft, Amsterdam. The discussions with him and other QuSoft members were consistently inspiring. I am also thankful to Zhengfeng Ji, Xin Wang, and Simeng Wang for their warm hospitality during my shorter visits. I thank the many peers I met during short visits and conferences, including but not limited to Randy Lin, Mengyao Hu, Kshiti Sneh Rai, Xingjian Li, Chengkai Zhu, Benchi Zhao, Xuanqiang Zhao, who offered valuable feedback and fresh insights on my work.

Lastly, I am grateful to my family and friends for their support to my life beyond research. My parents, Jun Chen and Jie Liu, have unconditionally supported my academic journey for over thirty years, and I can never thank them enough. My best friend in Copenhagen, Li Quan, not only brought fun to my life but also offered fresh perspectives on my research as

a talented computer scientist. Finally, I want to express my heartfelt gratitude to my wife, Huiying Wu. Navigating life abroad on my own was a challenge, especially as we maintained a long-distance relationship. Her unwavering support, patience, and encouragement helped me through the most difficult times of my PhD journey. She was always there to lift my spirits and provide perspective when I needed it most. Her strength and love have been my greatest source of motivation, and I am endlessly grateful for her presence in my life.

Statement of Contributions

This thesis is based on the following works:

- [BCK+23] Pedro Baptista, Ranyiliu Chen, Jędrzej Kaniewski, David Rasmussen Lolck, Laura Mančinska, Thor Gabelgaard Nielsen, and Simon Schmidt. A mathematical foundation for self-testing: Lifting common assumptions. arXiv:2310.12662, 2023.
- [CV] Ranyiliu Chen and Jurij Volčič. A study of complex self-testing. In preparation.
- [CMV24] Ranyiliu Chen, Laura Mančinska, and Jurij Volčič. All real projective measurements can be self-tested. Nature Physics, 20(10): 1642–1647, Oct 2024.

More specifically, the contents of Sect. 3 are based on [BCK+23]; the contents of Sect. 4 are based on [CV]; the contents of Sect. 5 are based on [CMV24].

Contributions during doctoral program not included in this thesis:

- [FVS+24] Máté Farkas, Jurij Volčič, Sigurd A. L. Storgaard, Ranyiliu Chen, and Laura Mančinska. Maximal device-independent randomness in every dimension. arXiv:2409.18916, 2024
- [HOZC24] Jaròn Has, Māris Ozols, Jeroen Zuiddam, and Ranyiliu Chen. Entanglement-assisted Shannon capacity of graphs. Contributed to the Master Thesis of Jaròn Has, 2024.

Table of content

1 Introduction

With the fast advancement of quantum technology, we are now witnessing the construction of increasingly large and powerful quantum computers. The potential applications of these devices, from complicated simulations in physics and chemistry [CRO+19] to transformative impacts in cryptography [PAB+20], are vast and promising. Soon, we may see practical use cases emerging, where quantum computers deliver capabilities that surpass the limits of classical computation. This however, leads to a natural question of trust and reliability: How can we be assured of the accuracy and integrity of the results provided by quantum devices, especially when they are likely to be more powerful than the classical systems available to users?

A number of approaches to quantum certification have been explored, tailored to different types of applications and levels of required rigour [MW16]. One traditional method is quantum state and process tomography [BCD+09], which aims to obtain complete information about the quantum system in question. However, tomography requires significant quantum resources and expertise from the verifier, as it depends on the ability to perform quantum measurements on the system directly. Indeed, due to the immense cost and complexity of their construction, for the foreseeable future quantum resources may only be accessed by the general public and most researchers remotely through service providers like AWS [AWS] and IBM [IBM]. Thus, a remote verification method that relies solely on classical communication is more practical and highly desirable.

In this spirit, self-testing offers a verification approach where the verifier interacts with the quantum device in a "black-box" manner. The interaction is modelled as sending input questions to the device (imagine pressing one of the buttons on a box) and receiving responses (the box shows an answer on a display). After repeated interactions, the verifier may post process these response data to determine whether the device is operating correctly. This black-box certification requires minimal assumptions about the internal workings of the device, thus is refereed to as the strongest form of verification. However, black-box verification alone faces a critical limitation: without further constraints (like running time restrictions), even a classical system could mimic a quantum device's behaviour, thus passing the test without actually performing any quantum computations[1].

The solution to this impossibility came with the study of Bell nonlocality, a foundational concept in quantum mechanics. In the 1960s, John Bell [Bel64] first showed that

[1]Black-box verification for computationally bounded quantum devices has been studied [KLVY22, NZ23, CMM+24, KMP+24], which relies on certain computational hardness assumptions.

two spatially separated devices could exhibit correlations that could not be explained by any classical theory, formulating what are now known as Bell's Inequalities. The CHSH inequality [CHSH69] is the most famous and simplest form of them. In the 1980s, Tsirelson established the maximal violation of CHSH inequality achievable by quantum mechanics, showing that this violation is achieved uniquely by a specific quantum state and measurement configuration [Tsi87]. Later, Mayers and Yao formalized this uniqueness property as a method of device certification, formally introducing the concept of self-testing [MY04].

Since its inception, self-testing has evolved into an active and expanding field of research. Numerous new Bell-type inequalities have been discovered, some of which admit unique, maximally violating quantum configurations that support self-testing [JHCL19, SBJ+23, PPW23]. The utility of self-testing extends well beyond certification alone; it underpins applications across quantum information science including protocols for delegated quantum computation [CGJV19], verifiable randomness generation [BCM+18], device-independent cryptography [MY04, VV14], Bell nonlocality [Col20], and quantum complexity theory. The breakthroughs $\mathsf{MIP}^* = \mathsf{RE}$ [JNV+20] in both complexity theory and operator algebra takes self-testing techniques as a key ingredient. Despite these successes, the mathematical formulation of self-testing have not kept pace with its applications. The need to bridge the gap between the expanding applications of self-testing and a rigorous mathematical framework is increasingly evident, making such formalism essential for its continued development.

In this thesis we advance the field of self-testing by addressing several fundamental problems concerning its power and limit from a mathematics point of view. The central contributions of this work are threefold: first, we propose new concepts together with a novel framework for non-local strategies, enabling a rigorous approach that systematically removes common assumptions that could potentially restricted the applicability of self-testing protocols. Secondly, we conduct a thorough examination of complex self-testing by formalizing complex local dilation and presenting insights aimed at advancing understanding in this area. Lastly, we demonstrate that all real projective measurements can be incorporated to some self-testing strategies via developing a handy way for developing new self-tests.

In the remainder of the introduction, we provide more context about those problems and outline our main results.

1.1 Common assumptions in self-testing

In self-testing, the black-box framework allows for certain "free manipulations" on the devices that remain undetectable to the verifier through classical statistics alone. For instance, the

device might alter its frame of reference or possess extra resources that are not engaged in the interaction. To capture these free manipulations mathematically researchers introduced the notion of "equivalence up to local isometry" (e.g., in [SB20]), which was later formalized as "local dilation" by [MPS24]. However, additional transformations can be applied to the device's mathematical formulation (called strategies, the tuple of shared state and local measurements) that preserve observed statistics but lack a clear physical interpretation. These transformations include purification, Naimark dilation, restriction to the support of the state, and complex conjugation.

As a result, many authors limit their analyses to specific types of strategies rather than the full generality allowed by quantum mechanics (POVM measurements on a mixed quantum state). For example, one may assume the state shared by the devices is pure, as one can always consider the purification of the state. A priori this constraint might weaken the theoretical notion of self-testing, contradicting the idea of 'black-box verification' that untrusted devices should have unrestricted power. Most self-testing in the literature to date adopt at least one of the following standard assumptions: the state is pure, the state is full-rank (or measurements act only on the support), or measurements are projective.

In Sect. 3, we start by closely examining Naimark dilation, restriction, and purification of non-local strategy. Built on these our main result shows that in "natural" cases—covering most instances in the literature—these three transformations are incorporated by local dilation. Consequently, in these cases, assumptions about purity, full-rankness, and projectivity can be lifted, allowing existing self-testing results to be promoted to assumption-free variants. We also identify specific scenarios where these assumptions are essential, as we pinpoint a statistics that admit no realization with pure, full-rank PVM strategy. Additionally, we establish a limitation of self-testing: non-projective measurements can never be self-tested in the assumption-free manner.

1.2 Issue of complex conjugate

In the previous discussion, we set aside the complex conjugate, which warrants more detailed consideration. This transformation is not problematic if the devices are expected to perform real measurements on a real state. However, if we aim to verify a complex strategy that has no real matrix representation in any basis (e.g., a strategy involving all three Pauli measurements), the device could potentially "cheat" by implementing its complex conjugate. This is problematic with the standard definition because taking the complex conjugate generally cannot be achieved through local isometries. Consequently, researchers have had to relax the

definition of self-testing to allow for any combination of the expected strategy and its complex conjugate. Relevant work in this area includes [MM11, APVW16, BSCA18, JMS20], though the mathematical underpinnings of this relaxed framework remain largely unexplored.

In Section 4, we explore complex self-testing in depth, examining its foundational concepts and offering insights which in hope could shed some light on the study of this field. We rigorously define complex local dilation and complex self-testing, establishing several basic properties. Inspired by [PSZZ24], we propose a conjecture on the operator-algebraic formulation of complex self-testing. Lastly, we revisit the concept of "realness" in quantum strategies, examining what it means for a strategy to be "real" and highlighting key nuances within this notion.

1.3 Self-testing any real projective measurement

In the discussion of the limit of self-testing we have shown that non-projective measurements cannot be self-tested, and likewise, complex measurements are not self-testable in the standard sense. This raises the natural question: can all real projective measurements be self-tested? By self-testing a measurement, we mean constructing a strategy that incorporates that specific measurement. Current protocols are largely confined to low-dimensional quantum systems or specific measurements within higher-dimensional spaces. For example, in two-level systems, self-testing protocols for Pauli measurements are well-established [MY04], and later work demonstrates that any two-dimensional projective measurement can be self-tested [YN13]. Higher-dimensional cases are also partially explored: tensor products of Pauli matrices have been successfully self-tested [McK17, Col17], and a specific pair of d-output measurements was self-tested in [SSKA21]. Constant-sized self-tests for measurements with particular properties have also been developed [MPS24, Fu22]. We also remark that, while the question regarding self-testing an arbitrary states has been extensively studied in [CGS17, SBR$^+$23], self-testing of arbitrary (higher-dimensional) measurements has remained out of reach.

In Sect. 5, we present the first robust, assumption-free self-testing protocol for any real projective measurements. To accomplish this, we formalize a new theoretical approach called post-hoc self-testing which facilitates the development of new self-tests by building upon existing ones. Additionally, we generalise this approach and introduce iterative self-testing, and describe measurements self-testable via this technique in terms of real Jordan algebras.

2 Preliminaries and notation

Throughout this thesis all Hilbert spaces (denoted by $\mathcal{H}$, with subscripts indicating the party they belong to) are assumed to be over complex field and finite-dimensional unless specified otherwise. The set of bounded operator on Hilbert space is denoted by $B(\mathcal{H})$. The identity operator of a d-dimensional Hilbert space is denoted by Id_d, which is simplified to be Id if the dimension is clear from the context. The norm of a vector $v \in \mathcal{H}$ is denoted by $\|v\| := \sqrt{\langle v, v\rangle}$. We write $u \approx_\varepsilon v$ if $\|u - v\| \leq \varepsilon$.

2.1 Quantum states and measurements

For a more detailed introduction of quantum computing and quantum information, we refer the readers to nice textbooks by Nielsen and Chuang [NC10] and Watrous [Wat18].

A state of a quantum system is described by a density operator in complex Hilbert spaces. In finite-dimensional cases it can be presented by a positive semidefinite operator $\rho \in B(\mathcal{H}), \rho \geq 0$ with unit trace $\mathsf{Tr}\,\rho = 1$. If a state has rank 1, then it is called a pure state, and thus takes the form $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$. In this sense we also refer to a pure state by $|\psi\rangle$. On the other hand, a state witch is not pure is called a mixed state. Any mixed state has purification: given its density operator $\rho \in B(\mathcal{H})$, there exist an auxiliary space $\mathcal{H}_P$ and a pure state $|\psi\rangle \in \mathcal{H}_P \otimes \mathcal{H}$ such that $\rho = \mathsf{Tr}_P\,|\psi\rangle\langle\psi|$.

The composition of quantum systems is described by the tensor product of the corresponding Hilbert spaces. In a composed bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$, any pure state $|\psi\rangle_{AB}$ admits a Schmidt decomposition:

$$|\psi\rangle = \sum_{i=0}^{k-1} \alpha_i |e_i\rangle \otimes |f_i\rangle ,$$

for some integer k, where $\alpha_i > 0$ and $\{|e_i\rangle\}_i \in \mathcal{H}_A, \{|f_i\rangle\}_i \in \mathcal{H}_B$ are orthonormal vector sets. The integer k is the Schmidt rank of the state. When $k = 1$ the state is called separable, otherwise entangled. And if $k = \mathsf{dim}\,\mathcal{H}_A = \mathsf{dim}\,\mathcal{H}_B$ holds we call the state full-rank. For the general case, we define the support of the state by $\mathsf{supp}_A\,|\psi\rangle = \mathsf{span}\{|e_i\rangle\}_i \subseteq \mathcal{H}_A$, $\mathsf{supp}_B\,|\psi\rangle = \mathsf{span}\{|f_i\rangle\}_i \subseteq \mathcal{H}_B$.

A measurement of a quantum system is characterised by a set of self-adjoint positive semidefinite operators $\{E_i\}_i$ satisfying $\sum_i E_i = \mathsf{Id}$. The probability of getting outcome i when measuring a system in state ρ is given by $\mathsf{Tr}[E_i\rho]$. Such a measurement is called a positive, operator-valued measurement (POVM). If further it holds that E_i are projectors,

i.e., $E_i^2 = E_i$ for all i, then we call it a projection-valued measure (PVM).

2.2 Bell Scenario

In a (bipartite) Bell scenario [Bel64, BCP+14], a classical verifier interacts with two spatially separated quantum devices, usually referred to as Alice and Bob. The verifier sends questions $x \in \mathcal{I}_A$ to Alice and $y \in \mathcal{I}_B$ to Bob, and they respond with answers $a \in \mathcal{O}_A$ and $b \in \mathcal{O}_B$, respectively. Although Alice and Bob cannot communicate during the interaction, they may beforehand share an entangled quantum state ρ_{AB}. They can measure this shared state locally, using sets of measurements $\{E_{xa} : a \in \mathcal{O}_A, x \in \mathcal{I}_A\}$ for Alice and $\{F_{yb} : b \in \mathcal{O}_B, y \in \mathcal{I}_B\}$ for Bob to produce outputs a and b. The statistics observed by the verifier are then governed by the probability distribution $p(a, b|x, y) = \mathsf{Tr}[E_{xa} \otimes F_{yb}\rho_{AB}]$, which can be estimated by repeating such interaction[2].

In such scenarios, the behaviour of Alice and Bob are described as quantum strategies.

Definition 2.1 ([BCK+23], Quantum strategy)**.** *A (tensor-product) quantum strategy is a tuple*

$$S = (\rho_{AB}, \{E_{xa} : x \in \mathcal{I}_A, a \in \mathcal{O}_A\}, \{F_{yb} : y \in \mathcal{I}_B, b \in \mathcal{O}_B\}), \tag{1}$$

consisting of a shared state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$, where $\mathcal{H}_A$, $\mathcal{H}_B$ are Hilbert spaces of Alice and Bob, respectively. For each $x \in \mathcal{I}_A$, the set $\{E_{xa}\}_{a\in\mathcal{O}_A} \subset B(\mathcal{H}_A)$ is a POVM on $\mathcal{H}_A$, and for each $y \in \mathcal{I}_B$, the set $\{F_{yb}\}_{b\in\mathcal{O}_b} \subset B(\mathcal{H}_B)$ is a POVM on $\mathcal{H}_B$. We identify the following special cases (which are not mutually exclusive):

- *If $\rho_{AB} = |\psi\rangle\langle\psi|$ is a pure state for some $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, we refer to the quantum strategy as* pure*. In this case, we may replace ρ_{AB} with $|\psi\rangle$ in* (1)*.*
- *If both marginal states $\rho_A := \mathsf{Tr}_B[\rho_{AB}], \rho_B := \mathsf{Tr}_A[\rho_{AB}]$ have rank equal to the dimension of corresponding Hilbert space, we may refer to the quantum strategy as* full-rank*. In the case of pure state $\rho_{AB} = |\psi\rangle$, this is equivalent to $|\psi\rangle$ having full Schmidt rank.*
- *If all measurements $\{E_{xa}\}$ and $\{F_{yb}\}$ are PVMs, then we refer to the quantum strategy as* projective*. Otherwise, we call it* non-projective*.*

[2]It is typically assumed that the devices are prepared independently and identically distributed (IID) for each round. Extending beyond the IID assumption [Cao22] has become a significant trend in information theory research, though self-testing in non-IID settings remains largely unexplored.

We will write $\{E_{xa} : x \in \mathcal{I}_A, a \in \mathcal{O}_A\}$ as $\{E_{xa}\}$ when from the context it is clear that the set is indexed over the sets $\mathcal{I}_A$ and $\mathcal{O}_A$. We will use analogous notation for Bob's measurements $\{F_{yb}\}$.

As mentioned earlier, the statistics $p(a, b|x, y)$ is determined by the strategy $p(a, b|x, y) = \mathsf{Tr}[E_{xa} \otimes F_{yb}\rho]$. It is also referred to as a correlation in this thesis. We call a strategy δ-approximately generates the correlation $p(a, b|x, y)$ if $|p(a, b|x, y) - \mathsf{Tr}[E_{xa} \otimes F_{yb}\rho]| \leq \delta$ for all a, b, x, y.

2.3 Local dilation and Self-testing

In a self-testing protocol, the verifier aims to deduce the underlying behaviour of quantum devices based solely on observed statistics. It is therefore essential for the behaviour producing a given statistics to be unique. However, at least two types of transformations—changing frames of reference and appending additional unused systems—leave the statistics unaffected. To account for these transformations, the concept of local dilation was introduced. In this thesis, we adopt the following definition of approximate local dilation, as it is critical in defining robust self-testing.

Definition 2.2 ([BCK+23], Local ε-dilation)**.** *Given two strategies*

$$S = (\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B), \{E_{xa}\}, \{F_{yb}\}) \text{ and}$$
$$\tilde{S} = (|\tilde{\psi}\rangle \in \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\})$$

we say that $\tilde{S}$ is a local ε-dilation of S *and write* $S \overset{\varepsilon}{\hookrightarrow} \tilde{S}$ *if for any purification* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P$ *of* ρ_{AB} *there exist spaces* $\mathcal{H}_{\hat{A}}, \mathcal{H}_{\hat{B}}$*, a local isometry* $U = U_A \otimes U_B$*, with* $U_A : \mathcal{H}_A \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\hat{A}}$*,* $U_B : \mathcal{H}_B \to \mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{\hat{B}}$ *and a state* $|\mathsf{aux}\rangle \in \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{\hat{B}} \otimes \mathcal{H}_P$ *such that for all* a, b, x, y *we have*

$$\begin{aligned} (U \otimes \mathsf{Id}_P) |\psi\rangle &\approx_\varepsilon |\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle , \\ (U \otimes \mathsf{Id}_P)(E_{xa} \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P) |\psi\rangle &\approx_\varepsilon (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}}) |\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle , \\ \|(U \otimes \mathsf{Id}_P)(\mathsf{Id}_A \otimes F_{yb} \otimes \mathsf{Id}_P) |\psi\rangle &\approx_\varepsilon (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb}) |\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle . \end{aligned} \tag{2}$$

In case we want to name the local isometry and the auxiliary state, we write $S \xhookrightarrow[U,|\mathsf{aux}\rangle]{\varepsilon} \tilde{S}$*. We will use this notation only when* ρ_{AB} *is pure to avoid ambiguity.*

Remark 2.3.

- Note that local dilations are transitive. That is if $S_X \overset{\varepsilon_1}{\hookrightarrow} S_Y$ and $S_Y \overset{\varepsilon_2}{\hookrightarrow} S_Z$, then $S_X \overset{\varepsilon_1+\varepsilon_2}{\hookrightarrow} S_Z$, see [MPS24, Lemma 4.7].

- If the state $\rho_{AB} = |\psi\rangle\langle\psi|$ in strategy S is pure, we do not need to concern ourselves with purifications of ρ_{AB} in the above definition. That is, the auxiliary state $|\mathsf{aux}\rangle \in \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{\hat{B}}$, and Eq. (2) becomes

$$\begin{aligned} U\,|\psi\rangle &\approx_\varepsilon |\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle\,, \\ U(E_{xa} \otimes \mathsf{Id}_B)\,|\psi\rangle &\approx_\varepsilon (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle\,, \\ U(\mathsf{Id}_A \otimes F_{yb})\,|\psi\rangle &\approx_\varepsilon (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb})\,|\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle\,. \end{aligned}$$

- If $\varepsilon = 0$ holds, we say that $\tilde{S}$ is a local dilation of S and write $S \hookrightarrow \tilde{S}$. For pure states, this is equivalent to finding a local isometry $U = U_A \otimes U_B$ such that

$$U(E_{xa} \otimes F_{yb})\,|\psi\rangle = (\tilde{E}_{xa} \otimes \tilde{F}_{yb})\,|\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle$$

  holds for all a, b, x, y.

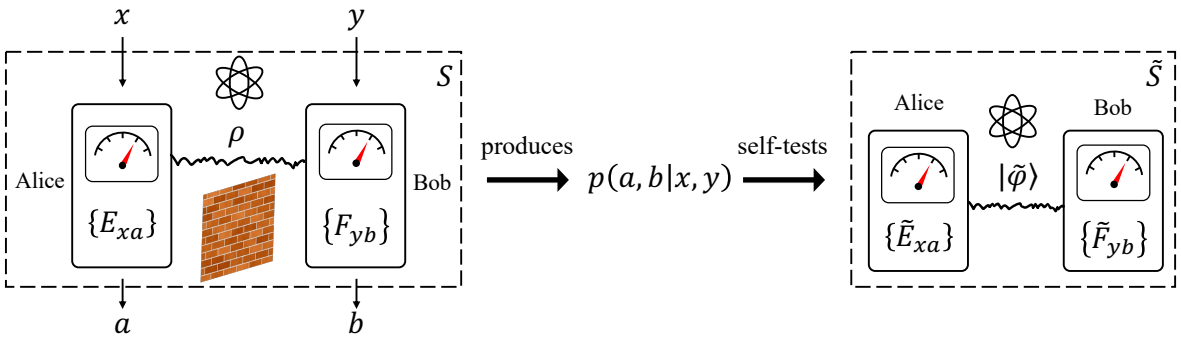


Figure 1: (adapted from [CMV24, Fig. 1]) Self-testing in a Bell scenario involves spatially separated parties, Alice and Bob, who perform local measurements on a shared state (their strategy denoted by S), producing a correlation $p(a, b|x, y)$. In the context of self-testing, this correlation allows Alice and Bob to be verified classically: the only way they can produce the correlation $p(a, b|x, y)$ is by following the specified target state and measurements, represented by $\tilde{S}$, up to local dilation.

Roughly speaking, self-testing requires that any strategy S generating the same correlation as $\tilde{S}$ can be mapped to strategy $\tilde{S}$ via local dilation (see Fig. 1). Robust self-testing enhances this by ensuring that any strategy S generating a correlation close to that of $\tilde{S}$ can

be approximately mapped to $\tilde{S}$. This makes it particularly practical, as correlation may be dampened by noise. With the notion of local dilation we define robust self-testing as follows.

Definition 2.4 ([BCK+23], Robust self-testing)**.** *Let $\tilde{S}$ be a pure strategy that generates correlation $p(a,b|x,y)$. We say that $p(a,b|x,y)$* robust self-tests *$\tilde{S}$ if from every $\varepsilon \geq 0$, there exists $\delta \geq 0$ such that $S \overset{\varepsilon}{\hookrightarrow} \tilde{S}$ for every strategy S that δ-approximately generates $p(a,b|x,y)$.*

We remark that, it is also common to study self-testing in terms of a (non-local) game $\mathcal{G}$ or a Bell expression $\mathcal{B}$. In these cases, Alice and Bob aim to maximize a target function f (depending on $\mathcal{G}$ or $\mathcal{B}$), which is typically a linear function in $p(a,b|x,y)$. A game $\mathcal{G}$ or Bell expression $\mathcal{B}$ is said to self-test its optimal strategy $\tilde{S}$ if $\tilde{S}$ is the unique optimal strategy, up to local dilation. In this thesis, we focus primarily on self-testing from correlations, and we will indicate explicitly when our techniques or results also apply to self-testing from games or Bell expressions.

3 Assumptions in self-testing

The work presented in this section is largely based on the joint work with Pedro Baptista, Jędrzej Kaniewski, David Rasmussen Lolck, Laura Mančinska, Thor Gabelgaard Nielsen, and Simon Schmidt [BCK+23], of which I contributed to Sect. 1, 3, 4, 6. Here

1. Sect. 3.1 is adapted from [BCK+23, Sect. 1], Sect. 3.2 and 3.3 corresponds to [BCK+23, Sect. 3], and Sect. 3.5 corresponds to [BCK+23, Sect. 6], with format and notations' changes to fit with the layout of this thesis.

2. Sect. 3.4.3 is a modification of [BCK+23, Sect. 4], where I generalise the methods in removing purity assumption to self-testing from correlations.

3.1 Motivation

Ideally, self-testing allows us to say that $\tilde{S}$ generates its correlation uniquely among all possible strategies allowed by quantum mechanism. In practice, however, when proving self-testing theorems, authors often impose different restrictions on the set of considered strategies S. Three most common types of assumptions restricting the strategy, S, implemented by the untrusted black-box quantum device are as follows:

1. the state in S is pure (rather than mixed),

2. the state in S is full-rank,

3. the measurements in S are projective (rather than general POVMs).

The above assumptions give rise to a priori different definitions of self-testing. A t-strategy for $t \subseteq \{\text{pure}, \text{full-rank}, \text{PVM}\}$ is a strategy where the states and measurements are restricted according to t. For example, a pure PVM strategy has a pure state and projective measurements, while the rank of the state can be arbitrary. An assumption-free strategy will usually just be called a strategy.

Definition 3.1 (Self-testing with assumptions). *Let $\tilde{S}$ be a pure strategy that generates $p(a,b|x,y)$, and $t \subseteq \{$pure, full-rank, PVM$\}$. We say that $p(a,b|x,y)$* robust t-self-tests *$\tilde{S}$ if from every $\varepsilon \geq 0$, there exists $\delta \geq 0$ such that $S \overset{\varepsilon}{\hookrightarrow} \tilde{S}$ for every t-strategy S that δ-approximately generates $p(a,b|x,y)$.*

It is clear that every t-self-test is also a t'-self-test if t' imposes more restrictions on the strategy than t. For example, every PVM self-test is also a pure PVM self-test. Conversely, if one could show that some t'-self-test is actually a t-self-test, then we say the assumptions in $t' \setminus t$ can be removed. We will refer to an assumption free self-test just as self-test. That is, $t = \emptyset$ and our arbitrary strategies are allowed to have mixed states of any rank and POVM measurements.

To gain intuition of the potential consequences of making unjustified assumptions, consider an example from [CHLM22] where two provers receive a single question each and produce a perfectly correlated bit. This can be achieved with a classical, separable mixed state: no quantum entanglement needed. However, if we assume that the perfectly correlated bit is produced by measuring a pure state, then this state needs to be entangled, leading to an entirely different analysis and conclusions. To give a more practical example, in device-independent random number generation, randomness is secure if it is not predictable by a third party [AM16]. Then the purity assumption oversimplifies and invalidate the security analysis, as there is no way any third party is entangled with a pure state. The assumption that all measurements are projective is sometimes made for the sake of simplicity or due to historical precedent. On the other hand, we know that non-projective measurements are essential for certain tasks in quantum error correction and state discrimination. Adhering to this assumption could therefore unnecessarily restrict the applicability of self-testing methods. From a philosophical standpoint, making additional assumption goes against the idea of self-testing, which aims to make as few assumptions as possible. This is particularly important in cryptographic contexts where fewer assumptions often translate into stronger security guarantees.

The goal of this section is to show that which of these assumptions can or cannot be removed under which condition. The remainder of this section is organized as follows: we start with an introduction to two new concepts: nearly support-preserving and nearly projective strategies in Sect. 3.2. Then in Sect. 3.3 we take a recap of two commonly used tricks: restriction and Naimark dilation, and show their connection to our new concepts. This connection will play a central role in the proof of our main results, which we will elaborate in Sect. 3.4 and 3.5. In particular, Sect. 3.4 shows how to remove certain assumptions and Sect. 3.5 provides a key example indicating when some assumptions cannot be removed.

3.2 New concepts

We noted previously in Definition 2.2 that the local dilation is transitive, so it gives a pre-order on the set of strategies. In general, local dilation is not an equivalence relation, because if we let S' to be S attached with an entangled auxiliary state, then $S' \hookrightarrow S$ but not the other direction. Nevertheless, we can show that if the auxiliary state in the local dilation is separable and both strategies are pure, then the two strategies are essentially 'equivalent':

Proposition 3.2. *If a strategy S_n is a ε-local dilation of a strategy S_m with a separable auxiliary state:*

$$S_m \xhookrightarrow[V_A\otimes V_B,|0\rangle_{\hat{A}}\otimes|0\rangle_{\hat{B}}]{\varepsilon} S_n,$$

then S_m is also a ε-local dilation of S_n (for some separable auxiliary state).

Proof. Without loss of generality, assume that S_n has local dimension n, and S_m has local dimension m. Since $S_m \xhookrightarrow[V_A\otimes V_B,|0\rangle_{\hat{A}}\otimes|0\rangle_{\hat{B}}]{\varepsilon} S_n$, then

$$\begin{aligned}(V_A\otimes V_B)(E_{xa}^{(m)}\otimes F_{yb}^{(m)})\,|\psi_m\rangle \approx_\varepsilon &(|0\rangle_{\hat{A}}\,|0\rangle_{\hat{B}})\otimes(E_{xa}^{(n)}\otimes F_{yb}^{(n)})\,|\psi_n\rangle\\ =&(\mathsf{Id}_{n'_A\times n}\otimes\mathsf{Id}_{n'_B\times n})(E_{xa}^{(n)}\otimes F_{yb}^{(n)})\,|\psi_n\rangle\end{aligned}$$

where $n'_A = n\times\dim\mathcal{H}_{\hat{A}}$, $n'_B = n\times\dim\mathcal{H}_{\hat{B}}$, and $\mathsf{Id}_{x\times y}$ $(y\le x)$ denotes the first y columns of the $x\times x$ identity matrix, which is an isometry.

Express V_A, V_B as $V_A = U_A\mathsf{Id}_{n'_A\times m}, V_B = U_B\mathsf{Id}_{n'_B\times m}$, where U_A, U_B are unitaries. Then

$$\begin{aligned}&(\mathsf{Id}_{n'_A\times m}\otimes\mathsf{Id}_{n'_B\times m})(E_{xa}^{(m)}\otimes F_{yb}^{(m)})\,|\psi_m\rangle\\ \approx_\varepsilon&(U_A^*\mathsf{Id}_{n'_A\times n}\otimes U_B^*\mathsf{Id}_{n'_B\times n})(E_{xa}^{(n)}\otimes F_{yb}^{(n)})\,|\psi_n\rangle\,.\end{aligned}$$

Take the smallest (or any) $n''\ge\mathsf{max}\{n'_A,n'_B\}$ such that n'' is a multiple of m. Then

$$\begin{aligned}&(\mathsf{Id}_{n''\times n'_A}U_A^*\mathsf{Id}_{n'_A\times n}\otimes\mathsf{Id}_{n''\times n'_B}U_B^*\mathsf{Id}_{n'_B\times n})(E_{xa}^{(n)}\otimes F_{yb}^{(n)})\,|\psi_n\rangle\\ \approx_\varepsilon&(\mathsf{Id}_{n''\times m}\otimes\mathsf{Id}_{n''\times m})(E_{xa}^{(m)}\otimes F_{yb}^{(m)})\,|\psi_m\rangle\\ =&(|0\rangle_{\hat{A}'}\,|0\rangle_{\hat{B}'})\otimes(E_{xa}^{(m)}\otimes F_{yb}^{(m)})\,|\psi_m\rangle\,,\end{aligned}$$

where $|0\rangle_{\hat{A}'}\in\mathcal{H}_{\hat{A}'}\cong\mathbb{C}^{n''/m}$, $|0\rangle_{\hat{B}'}\in\mathcal{H}_{\hat{B}'}\cong\mathbb{C}^{n''/m}$. It is clear that both $V_{A'} := \mathsf{Id}_{n''\times n'_A}U_A^*\mathsf{Id}_{n'_A\times n}$ and $V_{B'} := \mathsf{Id}_{n''\times n'_B}U_B^*\mathsf{Id}_{n'_B\times n}$ are isometries. So $S_n \xhookrightarrow[V_{A'}\otimes V_{B'},|0\rangle_{\hat{A}'}\otimes|0\rangle_{\hat{B}'}]{\varepsilon} S_m$. □

3.2.1 Nearly support-preserving strategies

We introduce the idea of support-preserving strategies [Lol22]. Given a pure strategy $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$, in the case where $|\psi\rangle$ is not full-rank, the support of $|\psi\rangle$ may or may not be an invariant subspace of the measurement operators. In a support-preserving strategy, the measurement operators map the state still inside the support of the state. That is, a quantum strategy $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ is called support-preserving if

$$\mathsf{supp}_A\left((E_{xa} \otimes \mathsf{Id}_B)|\psi\rangle\right) \subseteq \mathsf{supp}_A(|\psi\rangle),\ \mathsf{supp}_B\left((\mathsf{Id}_A \otimes F_{yb})|\psi\rangle\right) \subseteq \mathsf{supp}_B(|\psi\rangle),$$

holds for all a, b, x, y. Alternatively, one also can think of it as the measurement operators being block-diagonal in the Schmidt basis of the state, as what the authors of [PSZZ24] independently defined therein, which they refer to as "centrally-supported". It is given by the following condition:

$$[E_{xa}, \Pi_A] = [F_{yb}, \Pi_B] = 0,$$

where Π_A and Π_B is the projection onto $\mathsf{supp}_A(|\psi\rangle)$ and $\mathsf{supp}_B(|\psi\rangle)$, respectively. As the latter form is easier to be generalised in the case of robust self-testing, we adopt it to the following definition of nearly support-preserving strategies.

Definition 3.3 (Nearly support-preserving). *Let $\varepsilon \geq 0$. A pure strategy $S = (|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{E_{xa}\}, \{F_{yb}\})$ is called ε-*support-preserving *if*

$$\|[\Pi_A, E_{xa}]\|_{\sigma_A} \leq \varepsilon,\ \|[\Pi_B, F_{yb}]\|_{\sigma_B} \leq \varepsilon,$$

hold for all a, b, x, y, where Π_A is the projection onto $\mathsf{supp}_A(|\psi\rangle)$ (likewise for Π_B on Bob), $\sigma_A = \mathsf{Tr}_B[|\psi\rangle\langle\psi|]$ is the reduced density matrix on Alice (likewise for σ_B on Bob), and the state dependent norm is defined as $\|X\|_\sigma := \sqrt{\mathsf{Tr}[X^*X\sigma]}$. If further $\varepsilon = 0$, S is called support-preserving *for simplicity.*

Note that $\|[\Pi_A, E_{xa}]\|_{\sigma_A} = \|[\Pi_A, E_{xa}] \otimes \mathsf{Id}_B |\psi\rangle\| = \sqrt{\langle\psi|(E_{xa}^2 - E_{xa}\Pi_A E_{xa}) \otimes \mathsf{Id}_B|\psi\rangle}$. This identity is useful in later calculation. Also note that all full-rank strategies are support-preserving by definition.

We will show that support-preservingness is an invariant property under local dilation. That is, if $S \hookrightarrow \tilde{S}$, then S is support-preserving if and only if $\tilde{S}$ is. So this characteristic would not change as we move along '$\hookrightarrow$'. To prove this, the following characterization of near support-preservingness, inspired by [PSZZ24, Lemma 4.3], is needed.

Lemma 3.4. *Let $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ be a pure strategy.*

(a) If S is ε-support-preserving, then there exist operators $\hat{E}_{xa} \in \mathcal{H}_B, \hat{F}_{yb} \in \mathcal{H}_A$ such that $E_{xa} \otimes \mathsf{Id}_B |\psi\rangle \approx_\varepsilon \mathsf{Id}_A \otimes \hat{E}_{xa} |\psi\rangle$ and $\mathsf{Id}_A \otimes F_{yb} |\psi\rangle \approx_\varepsilon \hat{F}_{yb} \otimes \mathsf{Id}_B |\psi\rangle$ for all a, b, x, y.

(b) If there exist operators $\hat{E}_{xa} \in \mathcal{H}_B, \hat{F}_{yb} \in \mathcal{H}_A$ such that $E_{xa} \otimes \mathsf{Id}_B |\psi\rangle \approx_\varepsilon \mathsf{Id}_A \otimes \hat{E}_{xa} |\psi\rangle$ and $\mathsf{Id}_A \otimes F_{yb} |\psi\rangle \approx_\varepsilon \hat{F}_{yb} \otimes \mathsf{Id}_B |\psi\rangle$ for all a, b, x, y, then S is 2ε-support-preserving.

Proof. To prove (a), consider the Schmidt decomposition of the state

$$|\psi\rangle = \sum_i \lambda_i |e_i\rangle |f_i\rangle, \lambda_i > 0.$$

Define operators

$$\begin{aligned}
\lambda_{A\to B} &:= \sum_i \lambda_i |f_i\rangle\langle e_i|, \\
\lambda^{-1}_{A\to B} &:= \sum_i \lambda_i^{-1} |f_i\rangle\langle e_i|, \\
\lambda_{B\to A} &:= \sum_i \lambda_i |e_i\rangle\langle f_i| = (\lambda_{A\to B})^*, \\
\lambda^{-1}_{B\to A} &:= \sum_i \lambda_i^{-1} |e_i\rangle\langle f_i| = (\lambda^{-1}_{A\to B})^*,
\end{aligned}$$

and let $\hat{E}_{xa} := \lambda_{A\to B} E^\intercal_{xa} \lambda^{-1}_{B\to A} \in \mathcal{H}_B, \hat{B}_{yb} := \lambda_{B\to A} F^\intercal_{yb} \lambda^{-1}_{A\to B} \in \mathcal{H}_A$, where the transpose are with respect to the bases $\{|e_i\rangle_A\}, \{|f_i\rangle_B\}$, respectively. Then

$$\begin{aligned}
\mathsf{Id}_A \otimes \hat{E}_{xa} |\psi\rangle =& \mathsf{Id}_A \otimes \lambda_{A\to B} E^\intercal_{xa} \sum_i |e_i\rangle |e_i\rangle \\
=& \sum_{i,j} \lambda_j \langle e_j | E^\intercal_{xa} | e_i\rangle |e_i\rangle |f_j\rangle \\
=& \sum_{i,j} \lambda_j \langle e_i | E_{xa} | e_j\rangle |e_i\rangle |f_j\rangle \\
=& \Pi_A E_{xa} \otimes \mathsf{Id}_B |\psi\rangle .
\end{aligned}$$

In the last equation we use the identity $\Pi_A = \sum_i |e_i\rangle\langle e_i|$. So

$$\begin{aligned}
&\| E_{xa} \otimes \mathsf{Id}_B |\psi\rangle - \mathsf{Id}_A \otimes \hat{E}_{xa} |\psi\rangle \| \\
=& \| E_{xa}\Pi_A \otimes \mathsf{Id}_B |\psi\rangle - \Pi_A E_{xa} \otimes \mathsf{Id}_B |\psi\rangle \| = \| [\Pi_A, E_{xa}] \|_{\sigma_A}.
\end{aligned}$$

Then $E_{xa} \otimes \mathsf{Id}_B |\psi\rangle \approx_\varepsilon \mathsf{Id}_A \otimes \hat{E}_{xa} |\psi\rangle$ if $\|[\Pi_A, E_{xa}]\|_{\sigma_A} \leq \varepsilon$. The similar argument also works for Bob's operators.

To prove (b), note that $\|[\Pi_A, E_{xa}]\|_{\sigma_A} = \|\Pi_A E_{xa} \otimes \mathsf{Id} |\psi\rangle - E_{xa}\Pi_A \otimes \mathsf{Id} |\psi\rangle \|$. Then

$$\begin{aligned}
\Pi_A E_{xa} \otimes \mathsf{Id} |\psi\rangle &\approx_\varepsilon \Pi_A \otimes \hat{E}_{xa} |\psi\rangle \\
&= \mathsf{Id} \otimes \hat{E}_{xa} |\psi\rangle \\
&\approx_\varepsilon E_{xa} \otimes \mathsf{Id} |\psi\rangle = E_{xa}\Pi_A \otimes \mathsf{Id} |\psi\rangle .
\end{aligned}$$

So $\Pi_A E_{xa} \otimes \mathsf{Id} |\psi\rangle \approx_{2\varepsilon} E_{xa}\Pi_A \otimes \mathsf{Id} |\psi\rangle$. The similar argument also works for Bob's operators. □

The invariance of support-preservingness under local dilation can be stated as follows:

Proposition 3.5. *Let S and $\tilde{S}$ be two pure strategies.*

(a) If $S \hookrightarrow \tilde{S}$, then S is ε-support-preserving if and only if $\tilde{S}$ is ε-support-preserving.

(b) If $S \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$, then $\tilde{S}$ being ε-support-preserving implies that S is $(4\varepsilon' + 2\varepsilon)$-support-preserving, and S being ε-support-preserving implies that $\tilde{S}$ is $(4\varepsilon' + 2\varepsilon)$-support-preserving.

Proof. Let $V_A \otimes V_B$ be the local isometry and $|\mathsf{aux}\rangle$ be the auxiliary state in the exact/near local-dilation.

To prove (a), note that $V_A \Pi_A V_A^* = \Pi_{\tilde{A}} \otimes \Pi_{\hat{A}}$, where $\Pi_{\tilde{A}}$ and $\Pi_{\hat{A}}$ are projections onto $\mathsf{supp}_A |\tilde{\psi}\rangle$ and $\mathsf{supp}_A |\mathsf{aux}\rangle$, respectively. Then

$$\begin{aligned}
\|[\Pi_A, E_{xa}]\|_{\sigma_A}^2 &= \langle\psi|(E_{xa}^2 - E_{xa}\Pi_A E_{xa}) \otimes \mathsf{Id}_B|\psi\rangle \\
&= \langle\psi|E_{xa}V_A^*V_A(E_{xa} - \Pi_A V_A^* V_A E_{xa}) \otimes V_B^* V_B|\psi\rangle \\
&= \langle\tilde{\psi}, \mathsf{aux}|[(\tilde{E}_{xa} \otimes \mathsf{Id}_{A'})(\tilde{E}_{xa} \otimes \mathsf{Id}_{A'} - V_A\Pi_A V_A^*(\tilde{E}_{xa} \otimes \mathsf{Id}_{A'}))] \otimes \mathsf{Id}_{\tilde{B},\hat{B}}|\tilde{\psi}, \mathsf{aux}\rangle \\
&= \langle\tilde{\psi}, \mathsf{aux}|(\tilde{A}_{xa}^2 - \tilde{E}_{xa}\Pi_{\tilde{A}}\tilde{E}_{xa}) \otimes \Pi_{A'} \otimes \mathsf{Id}_{\tilde{B},\hat{B}}|\tilde{\psi}, \mathsf{aux}\rangle \\
&= \langle\tilde{\psi}|(\tilde{A}_{xa}^2 - \tilde{E}_{xa}\Pi_{\tilde{A}}\tilde{E}_{xa}) \otimes \mathsf{Id}_{\tilde{B}}|\tilde{\psi}\rangle = \|[\Pi_{\tilde{A}}, \tilde{E}_{xa}]\|_{\sigma_{\tilde{A}}}^2.
\end{aligned}$$

So $\|[\Pi_A, E_{xa}]\|_{\sigma_A} \leq \varepsilon$ if and only if $\|[\Pi_{\tilde{A}}, \tilde{E}_{xa}]\|_{\sigma_{\tilde{A}}} \leq \varepsilon$. The similar argument also works for Bob's operators.

In (b), we first prove the first implication.

Since $\tilde{S}$ is ε-support-preserving, by Lemma 3.4 there exist $\hat{\tilde{E}}_{xa}$ such that $\tilde{E}_{xa} \otimes \mathsf{Id} \left|\tilde{\psi}\right\rangle \approx_\varepsilon \mathsf{Id} \otimes \hat{\tilde{E}}_{xa} \left|\tilde{\psi}\right\rangle$. From the near local dilation, we have that

$$(V_A V_A^* \otimes V_B V_B^*)(\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle) \approx_\varepsilon (V_A \otimes V_B)(E_{xa} \otimes \mathsf{Id}_B) \left|\psi\right\rangle . \tag{3}$$

Consider the operator $\hat{E}_{xa} := V_B^*(\hat{\tilde{E}}_{xa} \otimes \mathsf{Id}_{\hat{B}})V_B$, then

$$\begin{aligned} V_A \otimes V_B(\mathsf{Id}_A \otimes \hat{E}_{xa} \left|\psi\right\rangle) &= V_A \otimes V_B(\mathsf{Id}_A \otimes V_B^*(\hat{\tilde{E}}_{xa} \otimes \mathsf{Id}_{\hat{B}})V_B \left|\psi\right\rangle) \\ &= (V_A V_A^* \otimes V_B V_B^*(\hat{\tilde{E}}_{xa} \otimes \mathsf{Id}_{\hat{B}}))(V_A \otimes V_B) \left|\psi\right\rangle \\ &\approx_{\varepsilon'} (V_A V_A^* \otimes V_B V_B^* \hat{\tilde{E}}_{xa})(\left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle) \\ &\approx_{\varepsilon} (V_A V_A^* \otimes V_B V_B^*)((\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle) \\ &\approx_{\varepsilon'} V_A \otimes V_B(E_{xa} \otimes \mathsf{Id}_B) \left|\psi\right\rangle . \end{aligned} \tag{4}$$

So $V_A \otimes V_B(\mathsf{Id}_A \otimes \hat{E}_{xa} \left|\psi\right\rangle) \approx_{2\varepsilon'+\varepsilon} V_A \otimes V_B(E_{xa} \otimes \mathsf{Id}_B \left|\psi\right\rangle)$, which implies $(\mathsf{Id}_A \otimes \hat{E}_{xa} \left|\psi\right\rangle) \approx_{2\varepsilon'+\varepsilon} (E_{xa} \otimes \mathsf{Id}_B \left|\psi\right\rangle)$. By Lemma 3.4, $\|[\Pi_A, E_{xa}]\|_{\sigma_A} \leq 4\varepsilon' + 2\varepsilon$ for all x, a. The similar argument holds for Bob's operators. So we conclude that S is $(4\varepsilon' + 2\varepsilon)$-support-preserving.

For the second implication of (b), given the existence of $\hat{E}_{xa}$, consider $\hat{\tilde{E}}_{xa} := V_B \hat{E}_{xa} V_B^*$, then

$$\begin{aligned} \mathsf{Id}_{\tilde{A}} \otimes \hat{\tilde{E}}_{xa} \left|\tilde{\psi}\right\rangle \left|\mathsf{aux}\right\rangle &= \mathsf{Id}_{\tilde{A},\hat{A}} \otimes V_B \hat{E}_{xa} V_B^*(\left|\tilde{\psi}\right\rangle \left|\mathsf{aux}\right\rangle) \\ &\approx_{\varepsilon'} V_A \otimes V_B \hat{E}_{xa} \left|\psi\right\rangle \\ &\approx_{\varepsilon} V_A E_{xa} \otimes V_B \left|\psi\right\rangle \\ &\approx_{\varepsilon'} \tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} \left|\tilde{\psi}\right\rangle \left|\mathsf{aux}\right\rangle . \end{aligned}$$

So by Lemma 3.4, $\|[\Pi_{\tilde{A}}, \tilde{E}_{xa}]\|_{\sigma_{\tilde{A}}} = \|[\Pi_{\tilde{A}} \otimes \Pi_{\hat{A}}, \tilde{E}_{xa} \otimes \mathsf{Id}_{\hat{A}}]\|_{\sigma_{\tilde{A},\hat{A}}} \leq 4\varepsilon' + 2\varepsilon$ for all x, a. The similar argument holds for Bob's operators. So we conclude that $\tilde{S}$ is $(4\varepsilon' + 2\varepsilon)$-support-preserving. □

(It has come to our attention that the exact ($\varepsilon = 0$) case of the "only if" direction of part (a) of Proposition 3.5 was independently developed by [PSZZ24, Proposition 4.6].)

3.2.2 Nearly projective strategies

We introduce the definition of nearly projective strategies. This notion quantifies 'how projective a strategy is on its state'.

Definition 3.6 (nearly projective). *Let $\varepsilon \geq 0$. A strategy $S = (|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{E_{xa}\}, \{F_{yb}\})$ is called ε-*projective *if*

$$\langle \mathsf{Id}_A - E_{xa}, E_{xa} \rangle_{\sigma_A} \leq \varepsilon^2, \langle \mathsf{Id}_B - F_{yb}, F_{yb} \rangle_{\sigma_B} \leq \varepsilon^2$$

hold for all a, b, x, y. Here $\langle X, Y \rangle_\sigma := \mathsf{Tr}[X^* Y \sigma]$.

Note that $\langle \mathsf{Id}_A - E_{xa}, E_{xa} \rangle_{\sigma_A} = \langle \psi | (\mathsf{Id}_A - E_{xa}) E_{xa} \otimes \mathsf{Id}_B | \psi \rangle$, and this identity is useful in some calculations. Also note that being 0-projective does not necessarily imply being projective: a non-projective strategy might be only non-projective outside of the support of the state, so it could be 0-projective. But for full-rank strategies, being projective and 0-projective are equivalent.

The projectiveness of strategies is another invariant property under local dilation. Namely, we have

Proposition 3.7. *Let S and $\tilde{S}$ be two pure strategies.*

(a) If $S \hookrightarrow \tilde{S}$, then S is ε-projective if and only if $\tilde{S}$ is ε-projective.

(b) If $S \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$, then $\tilde{S}$ being ε-projective implies that S is $(\sqrt{3\varepsilon'} + \varepsilon)$-projective, and S being ε-projective implies that $\tilde{S}$ is $(\sqrt{3\varepsilon'} + \varepsilon)$-projective.

Proof. Since (a) is an implication of (b) (by taking $\varepsilon' = 0$), we only need to prove (b).

Given that $S \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$, there exists a local isometry and auxiliary state such that

$$V[E_{xa} \otimes \mathsf{Id} \, |\psi\rangle] \approx_{\varepsilon'} (\tilde{E}_{xa} \otimes \mathsf{Id} \, |\tilde{\psi}\rangle) \otimes |\mathsf{aux}\rangle \, , \forall \; a, s \tag{5}$$

$$V[|\psi\rangle] \approx_{\varepsilon'} |\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle \tag{6}$$

(6) − (5):

$$V[(\mathsf{Id} - E_{xa}) \otimes \mathsf{Id} \, |\psi\rangle] \approx_{2\varepsilon'} ((\mathsf{Id} - \tilde{E}_{xa}) \otimes \mathsf{Id} \, |\tilde{\psi}\rangle) \otimes |\mathsf{aux}\rangle \tag{7}$$

Then the inner product of (5) and (7):

$$\langle \psi | (E_{xa} - E_{xa}^2) \otimes \mathsf{Id} | \psi \rangle \approx_{3\varepsilon'} \langle \tilde{\psi} | (\tilde{E}_{xa} - \tilde{E}_{xa}^2) \otimes \mathsf{Id} | \tilde{\psi} \rangle \, .$$

Note that both sides are real positive numbers, then

$$\begin{aligned}
&|\sqrt{\langle\psi|(E_{xa}-E_{xa}^2)\otimes \mathsf{Id}|\psi\rangle}-\sqrt{\langle\tilde{\psi}|(\tilde{E}_{xa}-\tilde{E}_{xa}^2)\otimes \mathsf{Id}|\tilde{\psi}\rangle}| \\
\leq&|\sqrt{\langle\psi|(E_{xa}-E_{xa}^2)\otimes \mathsf{Id}|\psi\rangle}+\sqrt{\langle\tilde{\psi}|(\tilde{E}_{xa}-\tilde{E}_{xa}^2)\otimes \mathsf{Id}|\tilde{\psi}\rangle}| \\
=&\frac{|\,\langle\psi|(E_{xa}-E_{xa}^2)\otimes \mathsf{Id}|\psi\rangle-\langle\tilde{\psi}|(\tilde{E}_{xa}-\tilde{E}_{xa}^2)\otimes \mathsf{Id}|\tilde{\psi}\rangle\,|}{|\sqrt{\langle\psi|(E_{xa}-E_{xa}^2)\otimes \mathsf{Id}|\psi\rangle}-\sqrt{\langle\tilde{\psi}|(\tilde{E}_{xa}-\tilde{E}_{xa}^2)\otimes \mathsf{Id}|\tilde{\psi}\rangle}|} \\
\Longrightarrow&|\sqrt{\langle\psi|(E_{xa}-E_{xa}^2)\otimes \mathsf{Id}|\psi\rangle}-\sqrt{\langle\tilde{\psi}|(\tilde{E}_{xa}-\tilde{E}_{xa}^2)\otimes \mathsf{Id}|\tilde{\psi}\rangle}|\leq\sqrt{3\varepsilon'}.
\end{aligned}$$

Then the two implications in (b) follows immediately. □

3.3 Folklore tricks

3.3.1 Restrictions of nonlocal strategies

In the literature we often encounter statements such as 'on the state the measurement behaves like...'. This is reasonable because statistics cannot provide information beyond the support of the state. Here we formalize this notion by specifying the restriction of a strategy.

Definition 3.8 (Restriction of a strategy)**.** *Let* $S=(|\psi\rangle_{AB},\{E_{xa}\},\{F_{yb}\})$ *be a pure strategy, and let*

$$|\psi\rangle_{AB}=\sum_{i=0}^{d-1}\lambda_i|e_i\rangle_A|f_i\rangle_B.$$

be its Schmidt decomposition. Define the isometries $U_A:\mathbb{C}^d\to\mathcal{H}_A, U_B:\mathbb{C}^d\to\mathcal{H}_B$ *by*

$$U_A=\sum_{i=0}^{d-1}|e_i\rangle_A\langle i| \qquad \textit{and} \qquad U_B=\sum_{i=0}^{d-1}|f_i\rangle_B\langle i|.$$

Then the restriction *of* S *is the strategy* $S_{\textit{res}}=(|\psi'\rangle,\{E'_{xa}\},\{F'_{yb}\})$*, where*

$$\begin{aligned}
E'_{xa}&=U_A^*E_{xa}U_A,\\
F'_{yb}&=U_B^*F_{yb}U_B,\\
|\psi'\rangle&=\sum_{i=0}^{d-1}\lambda_i|i\rangle|i\rangle=U_A^*\otimes U_B^*|\psi\rangle.
\end{aligned}$$

It is evident from the definition that the restriction always yields a full-rank strategy. In this sense the restriction provides a natural, canonical way of constructing a full-rank strategy. Also note that the projectors $\Pi_A = U_A U_A^* \in B(\mathcal{H}_A), \Pi_B = U_B U_B^* \in B(\mathcal{H}_B)$ projects onto the support of the state $|\psi\rangle_{AB}$.

We will now see that if a non-full-rank strategy S is exactly/nearly support-preserving, then S and its restriction S_{res} (defined as in Definition 3.8) can be mutually exactly/nearly local-dilated.

Proposition 3.9. *If a pure strategy S is ε-support-preserving, then $S_{\mathsf{res}} \overset{\varepsilon}{\hookrightarrow} S$ and $S \overset{\varepsilon}{\hookrightarrow} S_{\mathsf{res}}$, where S_{res} is the restriction of S.*

Proof. We show that $S_{\mathrm{res}} \overset{\varepsilon}{\hookrightarrow} S$ with a separable auxiliary state, then $S \overset{\varepsilon}{\hookrightarrow} S_{\mathsf{res}}$ follows from Proposition 3.2.

Consider isometries U_A, U_B in Definition 3.8, and recall that $U_A U_A^* = \Pi_A, U_B U_B^* = \Pi_B$. Then

$$\begin{aligned} U_A \otimes U_B (A'_{st} \otimes \mathsf{Id}_B) |\psi'\rangle &= U_A U_A^* E_{xa} U_A U_A^* \otimes U_B U_B^* |\psi\rangle \\ &= \Pi_A E_{xa} \Pi_A \otimes \Pi_B |\psi\rangle \\ &\approx_\varepsilon E_{xa} \Pi_A \otimes \Pi_B |\psi\rangle \\ &= E_{xa} \otimes \mathsf{Id}_B |\psi\rangle . \end{aligned}$$

A similar argument holds for Bob's operators. So $S_{\mathsf{res}} \overset{\varepsilon}{\hookrightarrow} S$. □

In general, a projective strategy might become non-projective under restriction. Here, we show that the other way around can never happen: whenever a restriction is projective, the original strategy must be both projective and support-preserving.

Theorem 3.10. *Let $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ be a pure strategy and S_{res} be its restriction.*

(a) If S is ε_1-support-preserving and ε_2-projective, then S_{res} is $(\varepsilon_1 + \varepsilon_2)$-projective.

(b) If S_{res} is ε_3-projective, then S is ε_3-support-preserving and ε_3-projective.

Proof. We prove for Alice's side, and the same argument works also for Bob. By definition,

$$\begin{aligned} \|[\Pi_A, E_{xa}]\|_{\sigma_A}^2 &= \langle\psi| (E_{xa}\Pi_A - \Pi_A E_{xa})(\Pi_A E_{xa} - E_{xa}\Pi_A) \otimes \mathsf{Id} |\psi\rangle \\ &= \langle\psi| (E_{xa}\Pi_A E_{xa} - E_{xa}\Pi_A E_{xa}\Pi_A - \Pi_A E_{xa}\Pi_A E_{xa} + \Pi_A A_{xa}^2 \Pi_A) \otimes \mathsf{Id} |\psi\rangle \\ &= \langle\psi| (E_{xa}^2 - E_{xa}\Pi_A E_{xa}) \otimes \mathsf{Id} |\psi\rangle . \end{aligned}$$

On the other hand, recall that $S_{\text{res}} = (|\psi'\rangle, \{E'_{xa}\}, \{F'_{yb}\})$ where $|\psi'\rangle = U_A^* \otimes U_B^* |\psi\rangle$, $U'_A = U_A^* E_{xa} U_A$, and U_A satisfies $U_A U_A^* = \Pi_A$. So

$$\begin{aligned}\langle \mathsf{Id} - A'_{xa}, A'_{xa} \rangle_{\sigma'_A} &= \langle \psi | (U_A \otimes U_B)((\mathsf{Id} - U_A^* E_{xa} U_A) U_A^* E_{xa} U_A \otimes \mathsf{Id})(U_A^* \otimes U_B^*) | \psi \rangle \\ &= \langle \psi | (\Pi_A E_{xa} \Pi_A - \Pi_A E_{xa} \Pi_A E_{xa} \Pi_A) \otimes \mathsf{Id} | \psi \rangle \\ &= \langle \psi | (E_{xa} - E_{xa} \Pi_A E_{xa}) \otimes \mathsf{Id} | \psi \rangle \,.\end{aligned}$$

Therefore

$$\begin{aligned}\langle \mathsf{Id} - A'_{xa}, A'_{xa} \rangle_{\sigma'_A} - \|[\Pi_A, E_{xa}]\|^2_{\sigma_A} &= \langle \psi | (E_{xa} - E_{xa}^2) \otimes \mathsf{Id} | \psi \rangle \\ &= \langle \psi | ((\mathsf{Id} - E_{xa}) E_{xa}) \otimes \mathsf{Id} | \psi \rangle \\ &= \langle \mathsf{Id} - E_{xa}, E_{xa} \rangle_{\sigma_A} \,.\end{aligned}$$

Then (a) is clear. For (b), note that both $\langle \mathsf{Id} - E_{xa}, E_{xa} \rangle_{\sigma_A}$ and $\|[\Pi_A, E_{xa}]\|^2_{\sigma_A}$ are positive. So if $\langle \mathsf{Id} - A'_{xa}, A'_{xa} \rangle_{\sigma'_A} \leq \varepsilon_3$ then $\langle \mathsf{Id} - E_{xa}, E_{xa} \rangle_{\sigma_A} \leq \varepsilon_3$ and $\|[\Pi_A, E_{xa}]\|^2_{\sigma_A} \leq \varepsilon_3$. □

Corollary 3.11. *The restriction S_{res} is projective if and only S is support-preserving and 0-projective (i.e. projective on the support of the state).*

3.3.2 Naimark dilation of nonlocal strategies

The Naimark dilation theorem (of a single POVM) provides an essential framework for characterizing POVMs, having significant influence not only in this study but also in the broader domains of operator theory and quantum information theory. To apply this in non-local strategies, here we extend this to any given (finite) set of POVMs.

Definition 3.12. *Let $\{R_{ij}\}_{j=1}^{m_i}$, $1 \leq i \leq n$, be a family of POVMs on $\mathcal{H}$. $(\{P_{ij}\}_{j=1}^{m_i}, V)$ is called a* Naimark dilation *of $\{R_{ij}\}_{j=1}^{m_i}$, if $\{P_{ij}\}_{j=1}^{m_i}$ is a family of PVMs on $\mathcal{H}'$, $V : \mathcal{H} \to \mathcal{H}'$, and $R_{ij} = V^* P_{ij} V$ for all i, j.*

The definition above is an abstract one since Naimark dilation has diverse forms, and all of them fit in our we general framework. For the sake of completeness we give an construction below, which it is also 'minimal' in the sense of what we introduce later in Definition 3.33. Another iterative construction of it can be found in [Pau16, Proposition 9.6 and Theorem 9.8] (which is not minimal). it's important to note that while this construction serves to illuminate the intuition behind Naimark dilations, the results we present later in the paper

are not tied to this specific example. Our general theorem applies to any Naimark dilation, regardless of its particular structure.

Construction 3.13. *Let $\{R_{ij}\}_{j=1}^{m_i}$, $1 \leq i \leq n$, be a family of POVM's on d-dimensional Hilbert space $\mathcal{H}$. Let $r_{ij} = rank(R_{ij})$ be the rank of each POVM element, then by spectrum decomposition $R_{ij} = \sum_{k=0}^{r_{ij}-1} x_{ijk}x_{ijk}^*$ for some sub-normalised vector x_{ijk}. Let $d' = \max_i \sum_j r_{ij}$. d' will be the dimension of our projectors.*

The matrix $M_i := [x_{i11}, x_{i12}, ..., x_{i1r_{i1}}, ..., x_{im_ir_{im_i}}]$ then is a $d \times \sum_j r_{ij}$ co-isometry. Pad it with zero vectors on the right to be a $d \times d'$ co-isometry. Then use Gram Schmidt process we can always find a $(d'-d) \times n$ matrix N_i such that $U_i = [M_i, N_i]^\intercal$ is a unitary. Denote the columns of U_i by $U_i := [x'_{i11}, x'_{i12}, ..., x'_{i1r_{i1}}, ..., x'_{im_ir_{im_i}}, ...]$. Define $P_{ij} := \sum_{k=0}^{r_{ij}-1}(x'_{ijk})(x'_{ijk})^*$, and $V = [\mathsf{Id}_d, 0_{d\times(d'-d)}]^\intercal$. It follows from their construction that P_{ij} are projectors and $R_{ij} = V^*P_{ij}V$ for all i, j.

In our subsequent analysis, we show that our results hold for all Naimark dilations, thus are not limited by the specific details of this construction.

Given the Naimark dilation of multiple POVMs, one can talk about the Naimark dilation of a strategy:

Definition 3.14 (Naimark dilation of quantum strategies)**.** *Given a pure strategy $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$, a PVM strategy $S_{\mathsf{Naimark}} = (V_A \otimes V_B |\psi\rangle, \{P_{xa}\}, \{Q_{yb}\})$ is called a Naimark dilation of S, if $(\{P_{xa}\}, V_A)$ is a Naimark dilation of $\{E_{xa}\}$, and $(\{Q_{yb}\}, V_B)$ is a Naimark dilation of $\{F_{yb}\}$.*

And not surprisingly, they generate the same statistics:

Lemma 3.15. *Any pure strategy gives the same correlation as its Naimark dilations.*

Proof. Let $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ and $S_{\mathsf{Naimark}} = (V_A \otimes V_B |\psi\rangle, \{P_{xa}\}, \{Q_{yb}\})$. Using $E_{xa} = V_A^*P_{xa}V_A, F_{yb} = V_B^*Q_{yb}V_B$,we get

$$\langle\psi|E_{xa} \otimes F_{yb}|\psi\rangle = \langle\psi|V^*VE_{xa} \otimes F_{yb}V^*V|\psi\rangle = \langle V\psi|P_{xa} \otimes Q_{yb}|V\psi\rangle,$$

where $V = V_A \otimes V_B$. □

As an analog of Proposition 3.9, we will show that S and S_{Naimark} are mutually locally dilated if S is projective. To prove this, we need the following lemma:

Lemma 3.16. *Let $\{R_{ij}\}_{j=1}^{m}$, $1 \le i \le n$, be a collection of POVM's on $\mathcal{H}$, σ be a density matrix on $\mathcal{H}$, and $|\psi\rangle$ be a purification of σ. Then any Naimark dilation $(\{P_{ij}\}, V)$ of $\{R_{ij}\}$ satisfies*

$$\| VR_{ij} \otimes \mathsf{Id} \, |\psi\rangle - P_{ij}V \otimes \mathsf{Id} \, |\psi\rangle \, \|^2 = \langle \psi | (\mathsf{Id} - R_{ij}) R_{ij} \otimes \mathsf{Id}_B | \psi \rangle \, .$$

Proof. Using $V^* P_{ij} V = R_{ij}$, we get

$$\begin{aligned}
& \| VR_{ij} \otimes \mathsf{Id} \, |\psi\rangle - P_{ij}V \otimes \mathsf{Id} \, |\psi\rangle \, \|^2 \\
&= \langle \psi | (R_{ij} V^* V R_{ij} + V^* P_{ij} P_{ij} V - V^* P_{ij} V R_{ij} - R_{ij} V^* P_{ij} V) \otimes \mathsf{Id} | \psi \rangle \\
&= \langle \psi | (R_{ij}^2 + R_{ij} - R_{ij}^2 - R_{ij}^2) \otimes \mathsf{Id} | \psi \rangle \\
&= \langle \psi | (\mathsf{Id} - R_{ij}) R_{ij} \otimes \mathsf{Id}_B | \psi \rangle \, .
\end{aligned}$$

□

Applying Lemma 3.16 in the context of nonlocal strategies, we have the following proposition:

Proposition 3.17. *If a pure strategy S is ε-projective, then $S \overset{\varepsilon}{\hookrightarrow} S_{\mathsf{Naimark}}$ and $S_{\mathsf{Naimark}} \overset{\varepsilon}{\hookrightarrow} S$, where S_{Naimark} is any Naimark dilation of S.*

Proof. It is clear from Lemma 3.16 that $S \xhookrightarrow[V_A \otimes V_B]{\varepsilon} S_{\mathsf{Naimark}}$, where V_A, V_B are isometries given in Definition 3.12. Then $S_{\mathsf{Naimark}} \overset{\varepsilon}{\hookrightarrow} S$ follows from Proposition 3.2. □

We now show that if a Naimark dilation of a strategy is support-preserving, then the original one must be both projective and support-preserving (an analog of Theorem 3.10).

Theorem 3.18. *Let $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ be a pure strategy and S_{Naimark} be any Naimark dilation of S.*

(a) If S is ε_1-support-preserving and ε_2-projective, then S_{Naimark} is $(\varepsilon_1 + \varepsilon_2)$-support-preserving.

(b) If S_{Naimark} is ε_3-support-preserving, then S is ε_3-support-preserving and ε_3-projective.

Proof. We prove for Alice's side, and the same argument works also for Bob. Let Π be the projection on the support of $|\psi\rangle$ on Alice's side. Let $(\{P_{xa}\}, V)$ be the Naimark dilation of

$\{E_{xa}\}$. Note that

$$\begin{aligned}\|[V\Pi V^*, P_{xa}]\|^2_{V\sigma V^*} =&\|P_{xa}V\Pi V^*V\otimes \mathsf{Id}\,|\psi\rangle - V\Pi V^*P_{xa}V\otimes \mathsf{Id}\,|\psi\rangle\,\|^2\\ =&\langle\psi|E_{xa}\otimes \mathsf{Id}|\psi\rangle - \langle\psi|E_{xa}\Pi E_{xa}\otimes \mathsf{Id}|\psi\rangle\,.\end{aligned}$$

And

$$\begin{aligned}\|[\Pi, E_{xa}]\|^2_{\sigma} =&\|\Pi E_{xa}\otimes \mathsf{Id}\,|\psi\rangle - E_{xa}\Pi\otimes \mathsf{Id}\,|\psi\rangle\,\|^2\\ =&\langle\psi|A^2_{xa}\otimes \mathsf{Id}|\psi\rangle - \langle\psi|E_{xa}\Pi E_{xa}\otimes \mathsf{Id}|\psi\rangle\,.\end{aligned}$$

So

$$\begin{aligned}&\|[V\Pi V^*, P_{xa}]\|^2_{V\sigma V^*} - \langle \mathsf{Id}-E_{xa}, E_{xa}\rangle_\sigma\\ =&\langle\psi|A^2_{xa}\otimes \mathsf{Id}|\psi\rangle - \langle\psi|E_{xa}\Pi E_{xa}\otimes \mathsf{Id}|\psi\rangle\\ =&\|[\Pi, E_{xa}]\|^2_{\sigma}.\end{aligned}$$

Then (a) is clear. For (b), note that both $\langle \mathsf{Id}-E_{xa}, E_{xa}\rangle_\sigma$ and $\|[\Pi, E_{xa}]\|^2_\sigma$ are positive. So S_{Naimark} being ε_3-support-preserving implies that S is ε_3-projective and ε_3-support-preserving. □

Corollary 3.19. *The Naimark dilation S_{Naimark} is support-preserving if and only if S is support-preserving and 0-projective (i.e. projective on the support of the state).*

Finally, we summarize the interaction of the concepts introduced in this section by Fig. 2.

3.4 Removing assumptions

In this section, we aim to remove the assumptions that are commonly made in the literature. Specifically, we will establish the following theorem.

Theorem 3.20. *Let $\tilde{S}$ be a pure strategy that generates a correlation $p(a,b|x,y)$ that satisfies certain geometric properties (will be specified later) in the quantum set of correlation. Then the following two implications hold:*

(a) If $\tilde{S}$ is full-rank and $p(a,b|x,y)$ robust pure PVM self-tests $\tilde{S}$, then $p(a,b|x,y)$ robust assumption-free self-tests $\tilde{S}$.

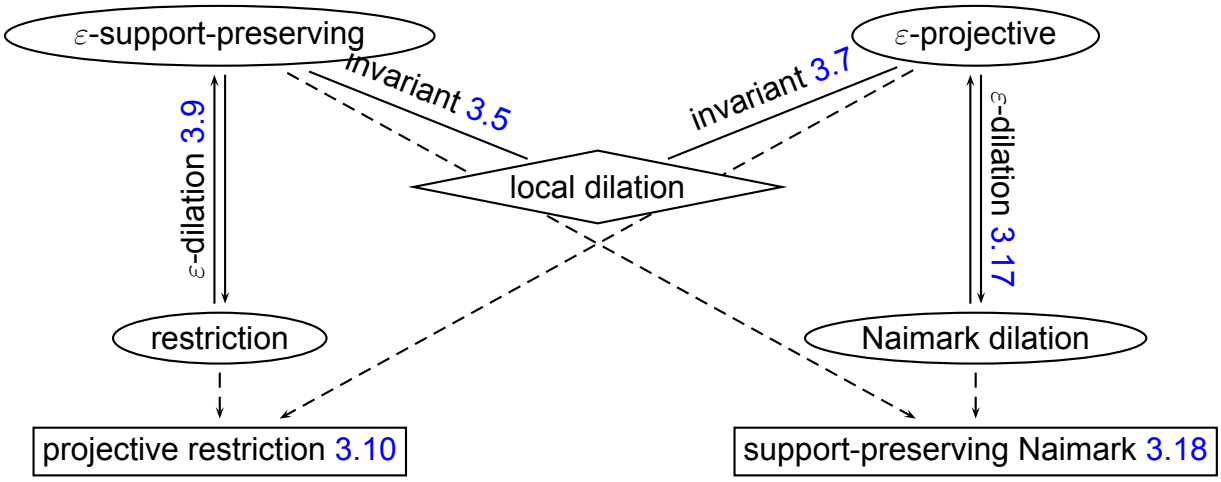


Figure 2: Local dilation "$\hookrightarrow$" is the central concept of self-testing. We introduce the idea of support-preservingness and projectiveness for strategies, which are invariant under local dilations. There are two canonical ways of obtaining a support-preserving strategy and a projective strategy, respectively: restriction and Naimark dilation. If a strategy S is support-preserving/projective, then we can locally dilate S to its restriction/Naimark dilation and vice versa. Finally, if the restriction of S is projective, or if its Naimark dilation is support-preserving, then S must be both projective and support-preserving.

(b) If $\tilde{S}$ is projective and $p(a,b|x,y)$ robust pure full-rank self-tests $\tilde{S}$, then $p(a,b|x,y)$ robust assumption-free self-tests $\tilde{S}$.

We will prove Theorem 3.20 (a) and (b) both in two steps. For part (a), we first show how to get rid of the PVM assumption in the following subsections. Similarly, we show that we can remove the full-rank assumption in part (b) in Subsection 3.4.2. Then, for both Theorem 3.20 (a) and (b), we get from pure to mixed states in Subsection 3.4.3.

As a final remark before we go into the steps of the proof of Theorem 3.20, we note that most of the results in this section also apply to self-tests from games/Bell expressions.

3.4.1 Removing the PVM assumption

Here we show that robust pure PVM self-test implies robust pure self-test if the canonical strategy is full-rank, with the building blocks from Section 3.2.

Theorem 3.21. *If $p(a,b|x,y)$ robust pure PVM self-tests a full-rank canonical strategy $\tilde{S}$. Then*

(a) $\tilde{S}$ is a projective strategy, and

(b) $(a, b|x, y)$ *is also a robust pure self-test for* $\tilde{S}$.

Proof. We first prove (a). Note that robust self-tests always imply exact self-tests by taking $\varepsilon = 0$ (which causes $\delta = 0$).

For any S that generates the same correlation of $\tilde{S}$, consider its Naimark dilation S_{Naimark}. Since G is a PVM self-test for $\tilde{S}$, it holds that $S_{\text{Naimark}} \hookrightarrow \tilde{S}$. By the invariance of projectiveness (Proposition 3.7), $\tilde{S}$ is 0-projective, thus projective.

Now we prove (b). For any ε, let $\varepsilon' = \varepsilon/5$. Since $p(a, b|x, y)$ robust pure PVM self-tests $\tilde{S}$, for such ε' there exist δ' such that, any δ'-optimal pure projective strategy S_{proj} for G satisfies $S_{\text{proj}} \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$.

Consider a non-projective strategy $S_{\text{non-proj}}$ that is δ'-optimal for G. Since its Naimark dilation S_{Naimark} is projective and δ'-optimal, it holds that $S_{\text{Naimark}} \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$. Note that $\tilde{S}$ is assumed to be full-rank (thus support-preserving), by the invariance of support-preservingness (Proposition 3.5) S_{Naimark} is $4\varepsilon'$-support-preserving. Then by Theorem 3.18 $S_{\text{non-proj}}$ is $4\varepsilon'$-support-preserving. Then $S_{\text{non-proj}} \overset{4\varepsilon'}{\hookrightarrow} S_{\text{Naimark}}$ by Proposition 3.17. By transitivity, $S_{\text{non-full}} \overset{\varepsilon'+4\varepsilon'=\varepsilon}{\hookrightarrow} \tilde{S}$.

Let $\delta = \delta'$. So we conclude that $S_{\text{non-proj}} \overset{\varepsilon}{\hookrightarrow} \tilde{S}$ for any δ-optimal $S_{\text{non-full}}$, that is, $p(a, b|x, y)$ also robust pure self-test $\tilde{S}$. □

Remark 3.22.

- *Previously, work [PSZZ24, Theorem 3.7] shows that in some special cases where the correlation is synchronous or binary, PVM assumption can be removeed for exact self-tests. Here we show that this in fact be done in a more general scenario, and for robust self-tests as well.*
- *Exact version of the (b) part of the theorem and its proof hold automatically by taking* $\varepsilon = 0$ *(which causes* $\delta = 0$*).*
- *If there is already an explicit* (δ, ε) *dependence in the PVM self-test,* e.g., $\varepsilon = O(\delta^2)$*, then our proof still works and give the result that any* δ*-optimal strategy is a* $5O(\delta^2)$*-local-dilation.*

3.4.2 Removing the full-rank assumption

Once again, using the tools from Section 3.2 and 3.3, we will now show we can get rid of the full-rank assumption if our canonical strategy is projective.

Theorem 3.23. *If $p(a,b|x,y)$ robust pure full-rank self-tests a projective canonical strategy $\tilde{S}$. Then*

(a) $\tilde{S}$ is support-preserving, and

(b) $p(a,b|x,y)$ also robust pure self-tests $\tilde{S}$.

Proof. We first prove (a). Note that robust self-tests always imply exact self-tests by taking $\varepsilon = 0$ (which causes $\delta = 0$).

For any S that generates the same correlation of $\tilde{S}$, consider its restriction S_{res}. Since $p(a,b|x,y)$ is a full-rank self-test for $\tilde{S}$ it holds that $S_{\text{res}} \hookrightarrow \tilde{S}$. By the invariance of support-preservingness (Proposition 3.5), $\tilde{S}$ is support-preserving.

Now we prove (b). For any ε, let ε' be the positive number such that $\varepsilon' + \sqrt{3\varepsilon'} = \varepsilon$. Since $p(a,b|x,y)$ is a robust pure full-rank self-test, for such ε' there exist δ' such that, any pure full-rank strategy S_{full} δ'-approximately generates $p(a,b|x,y)$ satisfies $S_{\text{full}} \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$.

Consider a non-full-rank strategy $S_{\text{non-full}}$ that δ'-approximately generates $p(a,b|x,y)$. Since its restriction S_{res} is full-rank and δ'-approximately generates $p(a,b|x,y)$, it holds that $S_{\text{res}} \overset{\varepsilon'}{\hookrightarrow} \tilde{S}$. Note that $\tilde{S}$ is assumed to be projective, by the invariance of projectiveness (Proposition 3.7) S_{res} is $\sqrt{3\varepsilon'}$-projective. Then by Theorem 3.10, $S_{\text{non-full}}$ is $\sqrt{3\varepsilon'}$-support-preserving. Then $S_{\text{non-full}} \overset{\sqrt{3\varepsilon'}}{\hookrightarrow} S_{\text{res}}$ by Proposition 3.9. By transitivity, $S_{\text{non-full}} \overset{\varepsilon'+\sqrt{3\varepsilon'}=\varepsilon}{\hookrightarrow} \tilde{S}$.

Let $\delta = \delta'$. So we conclude that $S_{\text{non-full}} \overset{\varepsilon}{\hookrightarrow} \tilde{S}$ for any δ-optimal $S_{\text{non-full}}$, that is, $p(a,b|x,y)$ also robust pure self-tests $\tilde{S}$. □

Remark 3.24.

- Exact version of the (b) part of the theorem and its proof hold automatically by taking $\varepsilon = 0$ (which causes $\delta = 0$).
- If there is already an explicit (δ, ε) dependence in the full-rank self-test, e.g., $\varepsilon = O(\delta^2)$, then our proof still works and give the result that any δ-optimal strategy is a $O(\delta)$-local-dilation.

3.4.3 Removing the purity assumption

Let us now shift our attention to mixed strategies. We will show that a pure self-test is a mixed self-test as long as the the correlation satisfies certain geometric properties in the quantum set of correlations.

To prove this result, some techniques about convex cone in Euclidean space is required. Given a convex set T (in our case, the set of quantum correlations C_q as a convex set in $\mathbb{R}^{|\mathcal{I}_A|\times|\mathcal{I}_B|\times|\mathcal{O}_A|\times|\mathcal{O}_B|}$) and a boundary point p (in our case, $\vec{p} = [p(a,b|x,y)]_{a,b,x,y}$), consider the convex cone

$$C(T,\vec{p}) := \mathsf{cone}\{T-\vec{p}\} = \{\sum_{i=1}^{k}\lambda_i(q_i-\vec{p})|q_i\in T, \lambda_i\geq 0, k\in\mathbb{N}\}.$$

Notice that the origin moves to $\vec{p}$. The width (also referred to as the maximal angle; see e.g. in [IS05]) of $C(T,\vec{p})$ is defined as

$$w(T,\vec{p}) := \mathsf{sup}\{\|x-y\||x,y\in C(T,\vec{p}), \|x\| = \|y\| = 1\}.$$

$w(T,\vec{p})$ can be understood as the 'sharpness' of the set T at point $\vec{p}$. It is clear from the definition that $0 < w(T,\vec{p}) \leq 2$ for any $T,\vec{p}$, and $w(T,\vec{p}) < 2$ when $\vec{p}$ is exposed in T. The following holds for any convex set T and $\vec{p}$:

Proposition 3.25. *If $a_1,...,a_n \geq 0$ and $p_i,...,p_n \in C(T,\vec{p})$ are unit vectors, then*

$$\|\sum_{i=1}^{n}a_np_n\|^2 \geq \frac{1}{2}w^2(T,\vec{p})(\sum_{i=1}^{n}a_i^2) + (1-\frac{1}{2}w^2(T,\vec{p}))(\sum_{i=1}^{n}a_i)^2.$$

Proof. Notice that $w^2(T,\vec{p})$ lower bounds the inner products between unit vectors in $C(T,\vec{p})$ by $\langle x_i,x_j\rangle \geq (1-\frac{1}{2}w^2)$. Expanding the norm of the sum of vectors we have

$$\begin{aligned}
\|\sum_{i=1}^{n}a_np_n\|^2 &= \sum_i a_i^2 + 2\sum_{i\neq j}a_ia_j\,\langle p_i,p_j\rangle \\
&\geq \sum_i a_i^2 + 2\sum_{i\neq j}a_ia_j(1-\frac{1}{2}w^2) \\
&= \sum_i a_i^2 + \left((\sum_i a_i)^2 - \sum_i a_i^2\right)(1-\frac{1}{2}w^2) \\
&= \frac{1}{2}w^2(T,p)(\sum_{i=1}^{n}a_i^2) + (1-\frac{1}{2}w^2(T,p))(\sum_{i=1}^{n}a_i)^2.
\end{aligned}$$

□

Proposition 3.25 tells us that

1. if $w(T,\vec{p}) \leq \sqrt{2}$ i.e. T is sufficiently sharp at $\vec{p}$, then

$$\forall i, a_i^2 \leq \frac{2}{w^2(T,\vec{p})} \| \sum_{i=1}^{n} a_i p_i \|^2.$$

2. if $\sqrt{2} \leq w(T,\vec{p}) \leq 2$, for n small enough such that $n \leq \frac{w^2}{w^2-2}$, we have

$$\forall i, a_i^2 \leq \frac{2}{w^2(T,\vec{p}) + n(2 - w^2(T,\vec{p}))} \| \sum_{i=1}^{n} a_i p_i \|^2.$$

The main result in this subsection is the following.

Theorem 3.26. *Let $t \subseteq \{PVM\}$ and $p(a,b|x,y)$ robust pure t self-tests $\tilde{S}$ with local dimension d, where $\vec{p} = [p(a,b|x,y)]_{a,b,x,y}$ satisfies either $w(C_q,\vec{p}) \leq \sqrt{2}$ or $d^2 \leq \frac{w^2(C_q,\vec{p})}{w^2(C_q,\vec{p})-2}$. Then $p(a,b|x,y)$ also robust mixed t self-tests $\tilde{S}$.*

The following lemma can be seen as a first step in the proof of Theorem 3.26. It identifies the isometry in the local dilation from any purification of a mixed quantum strategy to a quantum strategy that uses the operators of the canonical strategy of the pure self-test.

Lemma 3.27. *Let $p(a,b|x,y)$ robust, pure self-tests $\tilde{S} = \left(|\tilde{\psi}\rangle, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\}\right)$. Let $S = (\rho_{AB}, \{E_{xa}\}, \{F_{yb}\})$ be a mixed strategy that δ-approximately generates $p(a,b|x,y)$. Consider $S^{(1)} = (|\psi\rangle_{ABP}, \{E_{xa}\}, \{F_{yb} \otimes \mathsf{Id}_P\})$, where $|\psi\rangle_{ABP}$ is a purification of ρ_{AB}. Then $S^{(2)} = \left(X |\psi\rangle_{ABP}, \{\tilde{E}_{xa} \otimes \mathsf{Id}_{\check{A}}\}, \{\tilde{F}_{yb} \otimes \mathsf{Id}_{\hat{B}} \otimes \mathsf{Id}_P\}\right)$ is a local 2ε-dilation of $S^{(1)}$, where X is an isometry obtained from the robust, pure self-test.*

Proof. We have two pure strategies, $S^{(1)}$ and $(|\psi\rangle_{ABP}, \{E_{xa} \otimes \mathsf{Id}_P\}, \{F_{yb}\})$, which are δ-optimal. Then by the pure robustness, we have that

$$\begin{aligned}
&V_{AP} \otimes V_B[(E_{xa} \otimes \mathsf{Id}_P) \otimes \mathsf{Id}_B |\psi\rangle_{ABP}] \approx_\varepsilon (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle) \otimes |\mathsf{aux}_1\rangle, \\
&V_{AP} \otimes V_B[(\mathsf{Id}_A \otimes \mathsf{Id}_P) \otimes F_{yb} |\psi\rangle_{ABP}] \approx_\varepsilon (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle) \otimes |\mathsf{aux}_1\rangle, \qquad (8) \\
&V_{AP} \otimes V_B[|\psi\rangle_{ABP}] \approx_\varepsilon |\tilde{\psi}\rangle \otimes |\mathsf{aux}_1\rangle, \qquad (9) \\
&W_A \otimes W_{BP}[E_{xa} \otimes (\mathsf{Id}_B \otimes \mathsf{Id}_P) |\psi\rangle_{ABP}] \approx_\varepsilon (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle) \otimes |\mathsf{aux}_2\rangle, \qquad (10) \\
&W_A \otimes W_{BP}[\mathsf{Id}_A \otimes (F_{yb} \otimes \mathsf{Id}_P) |\psi\rangle_{ABP}] \approx_\varepsilon (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle) \otimes |\mathsf{aux}_2\rangle, \\
&W_A \otimes W_{BP}[|\psi\rangle_{ABP}] \approx_\varepsilon |\tilde{\psi}\rangle \otimes |\mathsf{aux}_2\rangle. \qquad (11)
\end{aligned}$$

Let $X := W_A \otimes V_B \otimes \mathsf{Id}_P$. We need to show that

$$X[E_{xa} \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P \left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} \otimes \mathsf{Id}_{\check{A}\hat{B}P})X \left|\psi\right\rangle_{ABP},$$
$$X[\mathsf{Id}_A \otimes F_{yb} \otimes \mathsf{Id}_P \left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})X \left|\psi\right\rangle_{ABP}$$

for all a, b, x, y.

Equations (8), (9) imply

$$V_{AP} \otimes V_B[(\mathsf{Id}_A \otimes \mathsf{Id}_P) \otimes F_{yb} \left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\hat{A}\hat{B}P})(V_{AP} \otimes V_B)[\left|\psi\right\rangle_{ABP}].$$

Applying $V_{AP}^* \otimes \mathsf{Id}_{\tilde{B}\hat{B}}$ to the left of both sides yields

$$\mathsf{Id}_{AP} \otimes V_B F_{yb}[\left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} \mathsf{Id}_{AP} \otimes (\tilde{F}_{yb} \otimes \mathsf{Id}_{\hat{B}})V_B[\left|\psi\right\rangle_{ABP}]. \tag{12}$$

Similarly, we obtain

$$W_A E_{xa} \otimes \mathsf{Id}_{BP}[\left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} (\tilde{E}_{xa} \otimes \mathsf{Id}_{\check{A}})W_A \otimes \mathsf{Id}_{BP}[\left|\psi\right\rangle_{ABP}] \tag{13}$$

from the equations (10), (11).

Now, applying $W_A \otimes \mathsf{Id}_{\tilde{B}\hat{B}P}$ to the left of both sides of equation (12) gives us

$$W_A \otimes V_B \otimes \mathsf{Id}_P[\mathsf{Id}_A \otimes F_{yb} \otimes \mathsf{Id}_P \left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP}.$$

Finally, we deduce

$$W_A \otimes V_B \otimes \mathsf{Id}_P[E_{xa} \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P \left|\psi\right\rangle_{ABP}] \approx_{2\varepsilon} (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP}$$

from applying $V_B \otimes \mathsf{Id}_{\tilde{A}\check{A}P}$ to the left of both sides of equation (13). □

The next lemma shows that the strategy we constructed before approximately generates the correlation.

Lemma 3.28. *Let $p(a, b|x, y)$ pure, robust self-tests $\tilde{S}$ and let $S^{(2)}$ be as in Lemma 3.27. Then $S^{(2)}$ is $(\delta + C\varepsilon)$-approximately generates $p(a, b|x, y)$, where C depends only on the Bell scenario.*

Proof. Let $p_1(a, b|x, y)$ and $p_2(a, b|x, y)$ be the correlation of $S^{(1)}$ and $S^{(2)}$, respectively. It

holds

$$
\begin{aligned}
&|p_1(a,b|x,y) - p_2(a,b|x,y)| \\
&= |\mathsf{Tr}(((E_{xa} \otimes F_{yb} \otimes \mathsf{Id}_P) \\
&\qquad\qquad - (W_A \otimes V_B \otimes \mathsf{Id}_P)^*(\tilde{E}_{xa} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P)) \left|\psi\right\rangle \left\langle\psi\right|_{ABP})| \\
&= |\langle (W_A \otimes V_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle, ((W_A \otimes V_B \otimes \mathsf{Id}_P)(E_{xa} \otimes F_{yb} \otimes \mathsf{Id}_P) \\
&\qquad\qquad\qquad\qquad - (\tilde{E}_{xa} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P)) \left|\psi\right\rangle \rangle| \\
&\leq ||(W_A \otimes V_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle || \cdot ||((W_A \otimes V_B \otimes \mathsf{Id}_P)(E_{xa} \otimes F_{yb} \otimes \mathsf{Id}_P) \\
&\qquad\qquad\qquad\qquad - (\tilde{E}_{xa} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P)) \left|\psi\right\rangle || \\
&= ||((W_A \otimes V_B \otimes \mathsf{Id}_P)(E_{xa} \otimes F_{yb} \otimes \mathsf{Id}_P) - (\tilde{E}_{xa} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P)) \left|\psi\right\rangle ||
\end{aligned}
$$

for all a, b, x, y, where the inequality comes from the Cauchy-Schwarz inequality. Since $S^{(2)}$ is a local 2ϵ-dilation of $S^{(1)}$ by Lemma 3.27, we know

$$
\begin{aligned}
&||((W_A \otimes V_B \otimes \mathsf{Id}_P)(E_{xa} \otimes F_{yb} \otimes \mathsf{Id}_P) - (\tilde{E}_{xa} \otimes \tilde{F}_{yb} \otimes \mathsf{Id}_{\check{A}\hat{B}P})(W_A \otimes V_B \otimes \mathsf{Id}_P)) \left|\psi\right\rangle || \\
&\qquad\qquad\qquad\qquad \leq 2\,\mathsf{max}\{|O_A|, |O_B|\}\varepsilon.
\end{aligned}
$$

Since $S^{(1)}$ δ-approximately generates $p(a,b|x,y)$, we deduce that $S^{(2)}$ $(\delta + 2\,\mathsf{max}\{|O_A|, |O_B|\}\varepsilon)$-approximately generates $p(a,b|x,y)$. □

Finally, we will see that the almost optimal strategy from the previous lemma can be ε'-dilated to the canonical strategy of the pure, robust self-test, under the condition that $p(a,b|x,y)$ is 'sharp' enough on the boundary of C_q.

Lemma 3.29. *Let $p(a,b|x,y)$ pure, robust self-tests $\tilde{S}$, and $S^{(2)}$ be as in Lemma 3.27. Then $\tilde{S}$ is a local ε'-dilation of $S^{(2)}$ if $\vec{p} = [p(a,b|x,y)]_{a,b,x,y}$ satisfies either $w(C_q, \vec{p}) \leq \sqrt{2}$ or $d^2 \leq \frac{w^2(C_q,\vec{p})}{w^2(C_q,\vec{p})-2}$, where ε' depends only on the Bell scenario and $w(C_q, \vec{p})$, the width of C_q at $p(a,b|x,y)$.*

Proof. It suffices to show that

$$
\|X \left|\psi\right\rangle_{ABP} - \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle\| \leq \varepsilon'
$$

for some ε'.

Consider the Schmidt decomposition of $X \left|\psi\right\rangle_{ABP}$ with respect to the separation between

$\mathcal{H}_{\tilde{A}\tilde{B}}$ and $\mathcal{H}_{\check{A}\hat{B}P}$

$$X\left|\psi\right\rangle_{ABP} = \sum_{i=0}^{r-1} \alpha_i \left|\varphi_i\right\rangle_{\tilde{A}\tilde{B}} \left|\mathsf{aux}_i\right\rangle_{\check{A}\hat{B}P},$$

where $r \leq d^2$ and d being the local dimension of $\tilde{S}$. Then $p_i(a,b|x,y) := \langle\varphi_i|E_{xa} \otimes F_{yb}|\varphi_i\rangle$ are correlations satisfying

$$\|\sum_i \alpha_i^2 p_i(a,b|x,y) - p(a,b|x,y)\| \leq \delta + C\varepsilon.$$

Take $\vec{p_i} = [p_i(a,b|x,y)]_{a,b,x,y} \in \mathbb{R}^{|\mathcal{I}_A|\times|\mathcal{I}_B|\times|\mathcal{O}_A|\times|\mathcal{O}_B|}$ and similarly $\vec{p} = [p(a,b|x,y)]_{a,b,x,y} \in \mathbb{R}^{|\mathcal{I}_A|\times|\mathcal{I}_B|\times|\mathcal{O}_A|\times|\mathcal{O}_B|}$, it holds that

$$\|\sum_i \alpha_i^2 \vec{p_i} - \vec{p}\| = \|\sum_i \alpha_i^2 (\vec{p_i} - \vec{p})\| \leq C'(\delta + C\varepsilon)$$

where $C' = |\mathcal{I}_A| \times |\mathcal{I}_B| \times |\mathcal{O}_A| \times |\mathcal{O}_B|$. Then Proposition 3.25 tells us that

$$\|\vec{p_i} - \vec{p}\| \leq C''C'(\delta + C\varepsilon)/\alpha_i^2,$$

if either $w(C_q, \vec{p}) \leq \sqrt{2}$ or $d^2 \leq \frac{w^2(C_q,\vec{p})}{w^2(C_q,\vec{p})-2}$ holds, where C'' is a constant depending only on $w^2(C_q, \vec{p})$. Then from pure self-testing there is some ε_i' such that $|\varphi_i\rangle \approx_{\varepsilon_i'} |\tilde{\psi}\rangle$. We therefore get

$$\begin{aligned}\|X\left|\psi\right\rangle_{ABP} - |\tilde{\psi}\rangle \otimes \left|\mathsf{aux}_0\right\rangle\| &= \|\sum_i \alpha_i (|\varphi_i\rangle - |\tilde{\psi}\rangle) \left|\mathsf{aux}_i\right\rangle\| \\ &= \sqrt{\sum_i \alpha_i^2 (\varepsilon_i')^2} := \varepsilon'.\end{aligned}$$

This finishes the proof. □

By putting together the previous lemmas, we can prove Theorem 3.26.

Proof of Theorem 3.26. Let $\varepsilon \geq 0$ and let S be a δ-optimal, mixed strategy, where we choose δ as in the robust pure self-test. Then by Lemmas 3.27 and 3.29 as well as transitivity, we know that $\tilde{S}$ is a local $(2\varepsilon + \varepsilon')$-dilation of the pure quantum strategy $S^{(1)}$ associated to S. □

Remark 3.30.

- To the best of our knowledge, it is unclear how to compute $w(C_q, \vec{p})$ given p even in the simplest cases like CHSH. And in general, deciding w greater or less than $\sqrt{2}$ is hard already for polyhedral (i.e., finitely generated) cones [IS05].

- Theorem 3.26, or more specifically, Lemma 3.29 can be translated to self-testing from games or Bell expressions, as shown in [BCK+23]. Furthermore, in those cases the constant C'' depends on the spectrum gap of the canonical game operator/Bell expression, thus no additional conditions are needed.

3.4.4 Proof of Theorem 3.20

We are now ready to prove our main theorem:

Proof of Theorem 3.20. (a): by Theorem 3.21, G is a robust pure self-test for $\tilde{S}$. Then by Theorem 3.26 G is an assumption-free self-test.

(b): by Theorem 3.23, G is a robust pure self-test for $\tilde{S}$. By Theorem 3.38, $\tilde{S}$ is support-preserving. So we take its restriction $\tilde{S}_{\text{res}}$, and G also robust pure self-tests $\tilde{S}_{\text{res}}$. Then using Theorem 3.26 G is an assumption-free self-test for $\tilde{S}_{\text{res}}$. From Proposition 3.9, G is an assumption-free self-test for $\tilde{S}$. □

3.5 A Counterexample

In Section 3.4 we showed that certain assumptions can be removed when the canonical strategy has nice properties (support-preserving/0-projective). Here we further show that these nice properties are necessary, by identifying self-tests that are only valid when proper assumptions are made. Surprisingly, one can obtain those counterexamples from a single extreme correlation $p_0(a, b|x, y) \in C_q(2, 3, 2, 3)$ (that is, $|\mathcal{I}_A| = |\mathcal{O}_A| = 2, |\mathcal{I}_B| = |\mathcal{O}_B| = 3$).

Theorem 3.31. *There exists a correlation $p_0(a, b|x, y) \in C_q(2, 3, 2, 3)$ satisfying the following:*

(a) $p_0(a, b|x, y)$ is extreme in $C_q(2, 3, 2, 3)$;

(b) $p_0(a, b|x, y)$ pure full-rank self-tests some $\tilde{S}$ (given below);

(c) $p_0(a, b|x, y)$ pure PVM self-tests any Naimark dilation of $\tilde{S}$.

(d) $p_0(a, b|x, y)$ does not pure self-test any strategy.

(e) $p_0(a,b|x,y)$ *does not admit any pure full-rank projective realisation.*

We first give the explicit construction of $\tilde{S}$ which generates $p_0(a,b|x,y)$. Consider the canonical strategy of CHSH game $\tilde{S}_{\text{CHSH}} = (|\Phi^+\rangle, \{\mathcal{X},\mathcal{Z}\}, \{\mathcal{H},\mathcal{G}\})$, where $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and $\mathcal{X},\mathcal{Z},\mathcal{H},\mathcal{G}$ are the measurements corresponding to the binary observables $X, Z, H := \frac{1}{\sqrt{2}}(X+Z), G := \frac{1}{\sqrt{2}}(X-Z)$, respectively. (That is, $\mathcal{X} = \{|+\rangle\langle+|, |-\rangle\langle-|\}$, $\mathcal{Z} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, etc.) It is well-known that the CHSH game is an assumption-free self-test for $\tilde{S}_{\text{CHSH}}$ [MYS12].

Then we incorporate a three-output POVM $\mathcal{M} = \{M_0, M_1, M_2\}$ to Bob's side, where

$$M_0 = \frac{1}{3}(\mathsf{Id} + Z),$$
$$M_1 = \frac{1}{3}(\mathsf{Id} - \frac{1}{2}Z + \frac{\sqrt{3}}{2}X),$$
$$M_2 = \frac{1}{3}(\mathsf{Id} - \frac{1}{2}Z - \frac{\sqrt{3}}{2}X).$$

It is clear that $M_i \geq 0, \sum_i M_i = \mathsf{Id}$, so $\mathcal{M}$ is a valid (non-projective) POVM. Therefore $\tilde{S} = (|\Phi^+\rangle, \{\mathcal{X},\mathcal{Z}\}, \{\mathcal{H},\mathcal{G},\mathcal{M}\})$. Notice that $\tilde{S}$ is full-rank but non-projective.

3.5.1 $p_0(a,b|x,y)$ pure full-rank self-tests $\tilde{S}$

We will show that $p_0(a,b|x,y)$ is extreme and pure full-rank self-test strategy $\tilde{S} = (|\Phi^+\rangle, \{\mathcal{X},\mathcal{Z}\}, \{\mathcal{H},\mathcal{G},\mathcal{M}\})$. For this we need Holder's inequality

$$\mathsf{Tr}[AB] \leq \|A\|_\infty \|B\|_1,$$

where $\|A\|_\infty := \mathsf{sup}_{\|v\|=1} \|Av\|$ is the infinity norm, and $\|B\|_1 := \mathsf{Tr}\,|B| = \mathsf{Tr}[\sqrt{B^*B}]$ is the trace norm.

Proof of Theorem 3.31 (a), (b). Consider any pure full-rank strategy $S = (|\psi\rangle, \{\mathcal{A}_0,\mathcal{A}_1\}, \{\mathcal{B}_0,\mathcal{B}_1,\mathcal{B}_2\})$ that generates $p_0(a,b|x,y)$. Let $\mathcal{A}_i = \{A_i^+, A_i^-\}$, $\mathcal{B}_i = \{B_i^+, B_i^-\}$ for $i = 0,1$ where $A_i^+, A_i^-, B_i^+, B_i^-$ are POVM elements. Define observables $A_i := A_i^+ - A_i^-$ and $B_i := B_i^+ - B_i^-$. Let $\mathcal{B}_2 = \{F_0, F_1, F_2\}$. Define the following two functionals:

$$\beta_0 := \langle\psi| A_0\otimes B_0 + A_0\otimes B_1 + A_1\otimes B_0 - A_1\otimes B_1 |\psi\rangle,$$
$$\beta_1 := \langle\psi| A_0\otimes F_0 - \frac{1}{2}A_0\otimes F_1 + \frac{\sqrt{3}}{2}A_1\otimes F_1 - \frac{1}{2}A_0\otimes F_2 - \frac{\sqrt{3}}{2}A_1\otimes F_2 |\psi\rangle.$$

And, from direct calculation, one can see that $\tilde{S}$ satisfies $\beta_0 = 2\sqrt{2}$ and $\beta_1 = 1$.

To prove (a), we will show that the correlation satisfying $\beta_0 = 2\sqrt{2}$ and $\beta_1 = 1$ is unique in the quantum set.

Since the CHSH inequality is a full-rank self-test, achieving $\beta_0 = 2\sqrt{2}$ implies that there exist unitary U_A, U_B such that

$$\begin{aligned} U_A A_0 U_A^* &= Z \otimes \mathsf{Id}_{A'}, \\ U_A A_1 U_A^* &= X \otimes \mathsf{Id}_{A'}, \\ U_A \otimes U_B \left|\psi\right\rangle &= \left|\Phi^+\right\rangle_{AB} \otimes \left|\mathsf{aux}\right\rangle_{A'B'}. \end{aligned}$$

Let us now consider the three-outcome measurement and define operators:

$$G_j := \mathsf{Tr}_{B'}\left[(\mathsf{Id}_B \otimes \sigma_{B'}^{1/2}) U_B^* F_j U_B (\mathsf{Id}_B \otimes \sigma_{B'}^{1/2})\right],$$

where $\sigma_{B'} = \mathsf{Tr}_{A'}[|\mathsf{aux}\rangle\langle\mathsf{aux}|]$. It is easy to see that the effective operators G_j fully determine the correlation, since the observables of Alice completely ignore the A' system.

Let us also define $\{T_j\}_{j=0}^2$ and note that they can be computed explicitly:

$$\begin{aligned} T_0 &:= \mathsf{Tr}_{AA'B'}\left[U_A^* A_0 U_A \otimes \mathsf{Id}_{BB'} |\psi\rangle\langle\psi|\right] = \frac{1}{2} Z, \\ T_1 &:= \mathsf{Tr}_{AA'B'}\left[U_A^*\Big(-\frac{1}{2}A_0 + \frac{\sqrt{3}}{2}A_1\Big) U_A \otimes \mathsf{Id}_{BB'} |\psi\rangle\langle\psi|\right] = \frac{1}{2}\Big(-\frac{1}{2}Z + \frac{\sqrt{3}}{2}X\Big), \\ T_2 &:= \mathsf{Tr}_{AA'B'}\left[U_A^*\Big(-\frac{1}{2}A_0 - \frac{\sqrt{3}}{2}A_1\Big) U_A \otimes \mathsf{Id}_{BB'} |\psi\rangle\langle\psi|\right] = \frac{1}{2}\Big(-\frac{1}{2}Z - \frac{\sqrt{3}}{2}X\Big). \end{aligned}$$

One can verify that the functional β_1 can be rewritten as:

$$\beta_1 = \sum_j \mathsf{Tr}(T_j G_j).$$

Each term can be upper-bounded using Holder's inequality:

$$\beta_1 \leq \sum_j \|T_j\|_\infty \|G_j\|_1 = \frac{1}{2}\sum_j \mathsf{Tr}\, G_j = 1,$$

where we used the fact that $\|T_j\|_\infty = \frac{1}{2}$. It is easy to determine the conditions under which these inequalities hold as equalities: since for every T_j the positive part is one-dimensional, the G_j operator must be proportional to these rank-1 projectors. The completeness condition

allows us to deduce the proportionality constants, and finally we conclude that:

$$G_0 = \frac{1}{3}(\mathsf{Id} + Z) = M_0,$$
$$G_1 = \frac{1}{3}(\mathsf{Id} - \frac{1}{2}Z + \frac{\sqrt{3}}{2}X) = M_1,$$
$$G_2 = \frac{1}{3}(\mathsf{Id} - \frac{1}{2}Z - \frac{\sqrt{3}}{2}X) = M_2.$$

This allows us to fully compute the statistics, which means that it is indeed the unique correlation satisfying $\beta_0 = 2\sqrt{2}$ and $\beta_1 = 1$. Therefore, this point is an exposed point of the $\beta_0 = 2\sqrt{2}$ face of the quantum set, and it must be (at least) extreme within the entire quantum set.

To prove (b), consider

$$H_j := (\mathsf{Id} \otimes \sigma_{B'}^{1/2}) U_B^* F_j U_B (\mathsf{Id} \otimes \sigma_{B'}^{1/2})$$

and note that $G_j = \mathsf{Tr}_{B'} H_j$. Since G_j are rank-1 PSD operators, we must have

$$H_j = G_j \otimes K_j,$$

for some $K_j \geq 0$ satisfying $\mathsf{Tr}\, K_j = 1$. Now, if $\sigma_{B'}$ is full-rank we can actually reconstruct the original measurement operators:

$$F_j = G_j \otimes (\sigma_{B'}^{-1/2} K_j \sigma_{B'}^{-1/2}).$$

Using the completeness relation $\sum_j F_j = \mathsf{Id}$ and the fact that the G_j operators correspond to an extremal three-outcome measurement on a qubit, we find that the only solution is $K_j = \sigma_{B'}$. Then $F_j = U_B^*(M_j \otimes \mathsf{Id}_{B'}) U_B$. So $\tilde{S}$ is a full-rank self-tested. □

3.5.2 $p_0(a,b|x,y)$ pure PVM self-tests any Naimark dilation of $\tilde{S}$

To prove this result we will need the concept of minimal Naimark dilation [Ben20]. A Naimark dilation $\{P_i \in \mathcal{B}(\mathcal{H}')\}_{i=1}^m$ of POVM $\{R_i \in \mathcal{B}(\mathcal{H})\}_{i=1}^m$ is minimal if and only if $\mathcal{H}' = \mathsf{span}\{P_i V |\psi\rangle : |\psi\rangle \in \mathcal{H}, i \in [1,m]\}$. One important fact about minimal Naimark dilation is that it is unique up to unitary.

Theorem 3.32 ([Ben20], Theorem 2.22). *Let* $(\{P_i\}_{i=1}^m, V)$, $(\{P_i'\}_{i=1}^m, V')$ *be two minimal Naimark dilations of* $\{R_i\}_{i=1}^m$. *Then there exists unitary* U *such that* $V' = UV$ *and* $UP_iU^* =$

P'_i.

We generalise the concept of minimal Naimark dilation in the context of nonlocal strategies.

Definition 3.33. *Let $\{R_{ij}\}_{j=1}^{m_i}$, $1 \leq i \leq n$ be a family of POVMs. A Naimark dilation $(\{P_{ij}\}_{j=1}^{m_i}, V)$ of $\{R_{ij}\}$ is* minimal *if, for at least one $i_0 \in [1,n]$, $(\{P_{i_0 j}\}_j, V)$ is a minimal Naimark dilation of $\{R_{i_0 j}\}_j$.*

Let $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ be a pure strategy. A pure PVM strategy $S' = (V_A \otimes V_B |\psi\rangle, \{P_{xa}\}, \{Q_{yb}\})$ is a minimal *Naimark dilation of S, if $(\{P_{xa}\}, V_A)$ is a minimal Naimark dilation of $\{E_{xa}\}$, and $(\{Q_{yb}\}, V_B)$ is a minimal Naimark dilation of $\{F_{yb}\}$.*

Minimal Naimark dilation of nonlocal strategies always exists, but is not unique (up to local unitary) in general, since those PVM which are non-minimal could be very different outside the support of the state. Nevertheless, we can show that in a special case, the minimal Naimark dilations of S are equivalent up to local dilation.

Lemma 3.34. *Let $\{R_{ij}\}$ be a family of POVMs on $\mathcal{H}$ with at most one non-projective measurement. Then for any two minimal Naimark dilations $(\{P_{ij}\}, V)$, $(\{P'_{ij}\}, V')$, there exist unitary U such that*

$$\begin{aligned} &UV = V' \\ &UP_{ij}V |\psi\rangle = P_{ij}V' |\psi\rangle, \forall |\psi\rangle \in \mathcal{H}. \end{aligned}$$

Proof. The case where all $\{R_{ij}\}$ are projections is trivial, because $\{R_{ij}\}$ is the minimal Naimark dilation of itself. Without loss of generality, we assume $\{R_{1j}\}_j$ to be the non-projective measurement. By definition, $\{P_{1j}\}$ and $\{P'_{1j}\}$ are two minimal Naimark dilations of $\{R_{1j}\}$. So, by Theorem 3.32 there exist unitary U such that $UV = V'$, and $UP_{1j}U^* = P'_{1j}$. Also note that $R_{ij}^2 = R_{ij}$ for all $i \neq 1$, so

$$\begin{aligned} &\| [VV^*, P_{ij}]V |\psi\rangle \|^2 \\ =& \langle\psi|V^*P_{ij}V|\psi\rangle - \langle\psi|V^*P_{ij}VV^*P_{ij}V|\psi\rangle \\ =& \langle\psi|(R_{ij} - R_{ij}^2)|\psi\rangle = 0. \end{aligned}$$

So $P_{ij}V |\psi\rangle = P_{ij}VV^*V |\psi\rangle = VV^*P_{ij}V |\psi\rangle = VR_{ij} |\psi\rangle$. Similarly, $P'_{ij}V' |\psi\rangle = V'R_{ij} |\psi\rangle$.

Then the following holds:

$$\begin{aligned} UP_{1j}V\left|\psi\right\rangle =& UP_{1j}U^*UV\left|\psi\right\rangle = P'_{1j}V'\left|\psi\right\rangle \\ UP_{ij}V\left|\psi\right\rangle =& UVR_{ij}\left|\psi\right\rangle \\ =& V'R_{ij}\left|\psi\right\rangle \\ =& P'_{ij}V'\left|\psi\right\rangle, \ \forall i \neq 1, \end{aligned}$$

as required. □

For the case of single POVM, any Naimark dilation of $\{R_i\}$ is a Naimark dilation of some minimal Naimark dilation of $\{R_i\}$. It is not true in the case of multiple POVMs or for non-local strategies. Nevertheless, we prove the following:

Lemma 3.35. *Let $\{R_{ij} \in B(\mathcal{H})\}_{j=1}^{m_i}$, $1 \leq i \leq n$, be a family of POVMs with at most one non-projective measurement, and let $(\{P_{ij} \in B(\mathcal{H}')\}, V)$ be a Naimark dilation of $\{R_{ij}\}$. Then there exists a minimal Naimark dilation $(\{P_{ij}^{\mathsf{min}} \in B(\mathcal{H}^{\mathsf{min}})\}, V^{\mathsf{min}})$ of $\{R_{ij}\}$ and an isometry $V' : \mathcal{H}^{\mathsf{min}} \to \mathcal{H}'$ such that*

$$\begin{aligned} &V'V^{\mathsf{min}} = V, \\ &V'P_{ij}^{\mathsf{min}}V^{\mathsf{min}}\left|\psi\right\rangle = P_{ij}V\left|\psi\right\rangle, \forall \left|\psi\right\rangle \in \mathcal{H}. \end{aligned}$$

Proof. The case where all $\{R_{ij}\}$ are projections is trivial. We assume $\{R_{1j}\}_j$ to be the non-projective measurement. Consider the subspace

$$\mathcal{H}^{\mathsf{min}} := \bigoplus_{j\in[1,m_1]} \mathcal{H}_j^{\mathsf{min}} \text{ of } \mathcal{H}' \ , \text{ where } \mathcal{H}_j^{\mathsf{min}} := \mathsf{span}\{P_{1j}V\left|\psi\right\rangle : \left|\psi\right\rangle \in \mathcal{H}\}.$$

Here $\bigoplus$ refers to the internal direct sum. It is clear that $V\mathcal{H} \subseteq \mathcal{H}^{\mathsf{min}} \subseteq \mathcal{H}'$. Let V'^{min} be the canonical embedding from $V\mathcal{H}$ to $\mathcal{H}^{\mathsf{min}}$, and V' be the canonical embedding from $\mathcal{H}^{\mathsf{min}}$ to $\mathcal{H}'$. Let U be the unitary from $\mathcal{H}$ to $V\mathcal{H}$. Let $V^{\mathsf{min}} := V'^{\mathsf{min}}U$.

We construct

$$P_{1j}^{\mathsf{min}} := (V')^*P_{1j}V',$$

$$P_{i1}^{\mathsf{min}} := V^{\mathsf{min}}R_{i1}(V^{\mathsf{min}})^* + (I - V^{\mathsf{min}}(V^{\mathsf{min}})^*), i \neq 1$$

$$P_{ij}^{\mathsf{min}} := V^{\mathsf{min}}R_{ij}(V^{\mathsf{min}})^*, i \neq 1, j \neq 1.$$

It is clear that P_{ij}^{min} are projections for $i \neq 1$. For P_{1j}^{min}, note that $\mathcal{H}_j^{\mathsf{min}} \subseteq \mathsf{Range}(P_{1j})$, so P_{1j}

commutes with $(V')^*V'$. Then $(P_{1j}^{\mathsf{min}})^2 = P_{1j}^{\mathsf{min}}$. Also note that $\mathcal{H}^{\mathsf{min}} = \mathsf{span}\{P_{1j}V|\psi\rangle : |\psi\rangle \in \mathcal{H}, j \in [1, m_1]\}$, so $\{P_{ij}^{\mathsf{min}}\}$ is a minimal Naimark dilation of $\{R_{ij}\}$. The following holds:

$$\begin{aligned} V'P_{1j}^{\mathsf{min}}V^{\mathsf{min}}|\psi\rangle =& V'(V')^*P_{1j}V'V^{\mathsf{min}}|\psi\rangle \\ =& P_{1j}V'(V')^*V'V^{\mathsf{min}}|\psi\rangle = P_{1j}V|\psi\rangle, \\ V'P_{ij}^{\mathsf{min}}V^{\mathsf{min}}|\psi\rangle =& V'V^{\mathsf{min}}R_{ij}|\psi\rangle = VR_{ij}V^*V|\psi\rangle = P_{ij}V|\psi\rangle, \forall i \neq 1. \end{aligned}$$

So we conclude that $(\{P_{ij}^{\mathsf{min}}\}, V^{\mathsf{min}})$ satisfies the required property. □

Applying Lemma 3.34 and 3.35 in the context of non-local strategies, we have the following:

Proposition 3.36. *Let $\tilde{S}$ be a pure full-rank strategy with at most one non-projective measurement on each side. Then any Naimark dilations of $\tilde{S}$ are local-dilations of each other.*

Proof. Consider two Naimark dilations S_1 and S_2 of $\tilde{S}$. By Lemma 3.35, there exists minimal Naimark dilations $\tilde{S}_1^{\mathsf{min}}$ and $\tilde{S}_2^{\mathsf{min}}$ of $\tilde{S}$ such that $\tilde{S}_1^{\mathsf{min}} \hookrightarrow S_1$, $\tilde{S}_2^{\mathsf{min}} \hookrightarrow S_2$. Then from Proposition 3.2

$$S_1 \hookrightarrow \tilde{S}_1^{\mathsf{min}}, S_2 \hookrightarrow \tilde{S}_2^{\mathsf{min}}.$$

Also, from Lemma 3.34 we know that $\tilde{S}_1^{\mathsf{min}}$ and $\tilde{S}_2^{\mathsf{min}}$ are local dilations of each other. So we conclude that $S_1 \hookrightarrow S_2$ and $S_2 \hookrightarrow S_1$. □

Theorem 3.37. *Let $\tilde{S}$ be a pure full-rank strategy with at most one non-projective measurement on each side. Then if p full-rank self-tests $\tilde{S}$, p also PVM self-tests any Naimark dilation of $\tilde{S}$.*

Proof. Consider a pure PVM strategy S_{PVM} that generates the same correlation as $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\})$. From full-rank self-test, the restriction of S_{PVM} is equivalent to $\tilde{S}$ attached with some auxiliary state up to local unitary. In other words, S_{PVM} is a Naimark dilation of $\tilde{S} \otimes |\mathsf{aux}\rangle = (|\tilde{\psi}\rangle|\mathsf{aux}\rangle, \{\tilde{E}_{xa} \otimes \mathsf{Id}_{\mathsf{aux},A}\}, \{\tilde{F}_{yb} \otimes \mathsf{Id}_{\mathsf{aux},B}\})$. Note that $|\tilde{\psi}\rangle|\mathsf{aux}\rangle$ is also full-rank, then from Proposition 3.36 and the transitivity of local dilation,

$$S_{\mathsf{PVM}} \hookrightarrow \tilde{S}_{\mathsf{Naimark}} \otimes |\mathsf{aux}\rangle \hookrightarrow \tilde{S}_{\mathsf{Naimark}}$$

for any Naimark dilation $\tilde{S}_{\mathsf{Naimark}}$ of $\tilde{S}$. □

Proof of Theorem 3.31 (c). By part (b) $p_0(a,b|x,y)$ pure full-rank self-tests $\tilde{S}$. Since $\mathcal{M}$ is the only non-projective measurement in $\tilde{S}$, Theorem 3.37 implies that $p_0(a,b|x,y)$ also pure PVM self-tests any Naimark dilation of $\tilde{S}$. □

For the sake of completeness we give a construction of a minimal Naimark dilation for $\tilde{S}$. Since the measurements for Alice are projective, they are minimal themselves. For Bob, let V be the canonical embedding $\mathbb{C}^2 \to \mathbb{C}^3$ (that is, in the computational basis $V = \mathsf{Id}_{3\times 2}$). Then for $\mathcal{M}$, let rank-1 projections $M'_i = |e_i\rangle\langle e_i|$ for $i = 0,1,2$, where

$$|e_0\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} \sqrt{2} \\ 0 \\ 1 \end{pmatrix}, \tag{14}$$

$$|e_1\rangle = \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ -\sqrt{3} \\ \sqrt{2} \end{pmatrix}, \tag{15}$$

$$|e_2\rangle = \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ \sqrt{3} \\ \sqrt{2} \end{pmatrix}. \tag{16}$$

And let $\mathcal{M}' = \{M'_0, M'_1, M'_2\}$. By definition, $(\mathcal{M}', V)$ is a minimal Naimark dilation of $\mathcal{M}$. For $\mathcal{G}$ and $\mathcal{H}$, since they are projective themselves, we just need to ensure their projectiveness outside the range of V when we extend them. To do this, we let $H_\pm$, $G_\pm$ be the ± 1-eigenspace projection of H, G, respectively. Define $H'_+ = VH_+V^* + \mathsf{Id} - VV^*$, $H'_- = VH_-V^*$ (that is, $H'_+ = H_+ \oplus \mathsf{Id}, H'_- = H_- \oplus 0$), and $G'_+ = VG_+V^* + \mathsf{Id} - VV^*$, $G'_- = VG_-V^*$. Then $(\mathcal{H}' = \{H'_+, H'_-\}, V)$, $(\mathcal{G}' = \{G'_+, G'_-\}, V)$ are Naimark dilations if $\mathcal{H}$ and $\mathcal{G}$, respectively. So we conclude that $\tilde{S}_{PVM} = (\mathsf{Id} \otimes V\,|\Phi^+\rangle, \{\mathcal{X}, \mathcal{Z}\}, \{\mathcal{H}', \mathcal{G}', \mathcal{M}'\})$ is a minimal Naimark dilation of $\tilde{S}$.

3.5.3 $p_0(a,b|x,y)$ does not pure full-rank PVM self-test any strategy

We show this result by proving that any pure self-tested strategy has to be both support-preserving and 0-projective:

Theorem 3.38. *If $p(a,b|x,y)$ pure self-tests $\tilde{S}$, then $\tilde{S}$ must be 0-projective and support-preserving. Furthermore, one can always take the canonical strategy $\tilde{S}$ to be both projective and full-rank without loss of generality.*

Proof. Take any pure strategy S that generates $p(a,b|x,y)$, then so does its Naimark dilation S_{Naimark} and its restriction S_{res}. Since G is an assumption-free self-test, it is also a pure self-test. So $S_{\mathsf{res}} \hookrightarrow \tilde{S}$, which implies that $\tilde{S}$ is support-preserving using Proposition 3.5 and the fact that S_{res} is support-preserving. Similarly, $S_{\mathsf{Naimark}} \hookrightarrow \tilde{S}$ implies $\tilde{S}$ to be 0-projective by Proposition 3.7 and the fact that S_{Naimark} is projective.

Since $\tilde{S}$ is 0-projective and support-preserving, $\tilde{S} \hookrightarrow \tilde{S}_{\mathrm{res}}$. So $p(a,b|x,y)$ assumption-free self-tests $\tilde{S}_{\mathrm{res}}$ as well. □

(This result was shown also in [PSZZ24, Proposition 4.14] via a different approach.) We note that, we can never show that a canonical strategy is projective and full-rank: consider $\tilde{S}' = (|\tilde{\psi}\rangle \otimes |0\rangle_A |0\rangle_B, \{\tilde{E}_{xa} \otimes \mathsf{Id}\}, \{\tilde{F}_{yb} \otimes \mathsf{Id}\})$. Then $\tilde{S}' \hookrightarrow \tilde{S}$ and $\tilde{S} \hookrightarrow \tilde{S}'$. So G also self-tests $\tilde{S}'$.

Proof of Theorem 3.31 (d), (e). Part (d) follows directly from Theorem 3.38, since $\tilde{S}$ is not 0-projective. Part (e) follows from Part (b): since $p_0(a,b|x,y)$ pure full-rank self-tests $\tilde{S}$, any full-rank realisation of $p_0(a,b|x,y)$ must not be 0-projective, as $\tilde{S}$ is not 0-projective and ε-projectivity is invariant under local dilation. □

$p_0(a,b|x,y)$ is also the first found correlation that cannot be realized by locally measuring a shared state of full Schmidt rank with projective measurements.

3.5.4 Separating (standard) self-tests and abstract state self-tests

We show that Part (c) of Theorem 3.31 also answers an open question raised in [PSZZ24], separating abstract state self-testing defined therein and (standard) self-testing in a case where there is no full-rank strategy in a certain class of strategies (namely, the class of all pure PVM strategies). Recall that, in an abstract state self-test the higher order moments are the same for all strategy inducing the correlation.

Definition 3.39 ([PSZZ24]). *Let $t \subseteq \{$pure, full-rank, PVM$\}$. A correlation $p(a,b|x,y)$ is an abstract state t self-test if for every $k,l \geq 1$, $a_1,\ldots,a_k \in \mathcal{O}_A$, $x_1,\ldots,x_k \in \mathcal{I}_A$, $b_1,\ldots,b_l \in \mathcal{O}_B$, $y_1,\ldots,y_l \in \mathcal{I}_B$, the value*

$$\langle\psi|E_{x_1a_1}\cdots F_{x_kx_k} \otimes F_{y_1b_1}\cdots F_{y_lb_l}|\psi\rangle$$

is the same across all t strategies generating $p(a,b|x,y)$.

Proposition 3.40. *Let $p_0(a,b|x,y)$ be the correlation generated by the pure non-projective strategy $\tilde{S} = (|\Phi^+\rangle, \{\mathcal{X}, \mathcal{Z}\}, \{\mathcal{H}, \mathcal{G}, \mathcal{M}\})$. Then $p_0(a,b|x,y)$ is not an abstract state PVM self-test.*

Proof. According to the definition of abstract state self-testing, it suffices to find two pure PVM strategies for p that give different higher-order moments.

Define $S^1_{PVM} = (\mathsf{Id} \otimes V |\Phi^+\rangle, \{\mathcal{X}, \mathcal{Z}\}, \{\mathcal{H}', \mathcal{G}', \mathcal{M}'\})$ as in the previous subsection. Now consider another dilation $\mathcal{H}''$ of $\mathcal{H}$, namely, $H''_+ = VH_+V^*$, $H''_- = VH_-V^* + \mathsf{Id} - VV^*$ (that is, $H''_+ = H_+ \oplus 0, H''_- = H_- \oplus \mathsf{Id}$). Let $S^2_{PVM} = (\mathsf{Id} \otimes V |\Phi^+\rangle, \{\mathcal{X}, \mathcal{Z}\}, \{\mathcal{H}'', \mathcal{G}', \mathcal{M}'\})$. Then direct calculation shows that

$$\langle\Phi^+|(\mathsf{Id} \otimes V^*)(\mathsf{Id} \otimes (M'_0 H'_+ M'_0))(\mathsf{Id} \otimes V)|\Phi^+\rangle = \frac{4-\sqrt{2}}{18},$$
$$\langle\Phi^+|(\mathsf{Id} \otimes V^*)(\mathsf{Id} \otimes (M'_0 H''_+ M'_0))(\mathsf{Id} \otimes V)|\Phi^+\rangle = \frac{2-\sqrt{2}}{18}.$$

So S^1_{PVM} and S^2_{PVM} are of different higher order moments. □

Note that by to [PSZZ24, Theorem 3.5], abstract state self-testing is equivalent to (standard) self-testing under the condition that $p_0(a,b|x,y)$ is extreme and there exists a full-rank t strategies inducing the correlation $p_0(a,b|x,y)$. Therefore, our results indicates that the condition of [PSZZ24, Theorem 3.5] is crucial: there exists extreme correlation $p_0(a,b|x,y)$ such that, the class of PVM strategies admits no full-rank strategy for $p_0(a,b|x,y)$, where $p_0(a,b|x,y)$ is a (standard) PVM-self-test but not an abstract state PVM-self-test.

4 On complex self-testing

The work presented in this section is based on an unpublished work [CV].

4.1 Motivation

As we it's been discussed in the Introduction, there are (at least) three types of 'free' manipulation in non-local strategies. Definition 2.4 incorporates the freedom of unused resource (auxiliary state) and changing frames of reference (local isometry), but not taking the complex conjugate into consideration. This is not an problem if our canonical strategy is real (has a real matrix representation) since it is then equivalent to the complex conjugate of itself. However, for strategies without real matrix representation[3] Definition 2.4 might not fit, as there might be no local unitary taking the strategy to its complex conjugate. To address this issue, the notion of complex self-testing [MM11] was introduced, and works alone this line includes [MM11, APVW16, BSCA18, JMS20]. Roughly speaking, a complex self-test allows the devices to concurrently adopt either the canonical strategy or its complex conjugate.

In this section, we will take a careful examination of the notion of complex self-testing, and provide some observations which in hope could shed some light on the study of this field. In Sect. 4.2 we formalize the notion of complex local dilation and complex self-testing, providing two equivalent ways of understanding it. In Sect. 4.3 we prove some properties of complex self-testing, including ones related to real simulation of strategies. In Sect. 4.4 we give a conjecture on the operator-algebraic formulation of complex self-testing. Finally, we revisit the 'realness' of quantum strategies in Sect. 4.5, providing some subtleties in the notion of real strategies.

For the sake of simplicity, all the results in this section are presented in terms of exact (rather than robust) pure (all states are assumed to be pure) self-testing.

4.2 Definition of complex dilation and self-testing

Similar to the standard self-testing, we first formulate the 'complex' counterpart of the local dilation notation. A common approach in the literature is to introduce additional Hilbert space $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, on which the devices perform measurements on an entangled state to concurrently decides to employ the canonical strategy or its complex conjugate. Since the

[3] A good example to keep in mind is a strategy contains all three Pauli measurements $\sigma_X, \sigma_Y, \sigma_Z$

additional measurements $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ has binary outcomes, without loss of generality we can take $\mathcal{H}_{A'} \cong \mathcal{H}_{B'} \cong \mathbb{C}^2$, and the state can take the form of $\alpha |00\rangle + \beta |11\rangle$. Also, notice that the real coefficients α, β can be absorbed to the auxiliary states. We then define complex local dilation as follows.

Definition 4.1 (Complex local dilation). *A strategy* $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\})$ *is a* complex local dilation *of a strategy* $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$*, if there exist local isometry*

$$U_A : \mathcal{H}_A \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{A'},$$

$$U_B : \mathcal{H}_B \to \mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{\hat{B}} \otimes \mathcal{H}_{B'},$$

$U = U_A \otimes U_B$ *such that*

$$\begin{aligned} & U[E_{xa} \otimes \mathsf{Id}_B |\psi\rangle_{AB}] \\ =& (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} + (\overline{\tilde{E}_{xa}} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} \qquad (17) \\ & U[\mathsf{Id}_A \otimes F_{yb} |\psi\rangle_{AB}] \\ =& (\mathsf{Id}_{\tilde{A}} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} + (\mathsf{Id}_{\tilde{A}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} \qquad (18) \end{aligned}$$

hold for all a, b, x, y*, where* $|\mathsf{aux}_{0,1}\rangle$ *are subnormalized states (not necessarily orthogonal):* $\langle \mathsf{aux}_0 | \mathsf{aux}_0 \rangle + \langle \mathsf{aux}_1 | \mathsf{aux}_1 \rangle = 1$.

We denote this relation by $S \hookrightarrow_{\mathbb{C}} \tilde{S}$. Without loss of generality we take all the states $|\psi\rangle, |\tilde{\psi}\rangle, |\mathsf{aux}_{0,1}\rangle$ to be real, due to the existence of Schmidt decomposition of bipartite states. Clearly, if $\tilde{S}$ is already a real strategy, then complex local dilation becomes equivalent to standard local dilation (take $\varepsilon = 0$ in Definition 2.2).

Alternatively, complex local dilation could be also understood as a convex combination of $\tilde{S}$ and its complex conjugate, in the sense introduced in [MNP21]. To see this, first note that if local systems are direct sum of subsystems:

$$\mathcal{H}_A = \mathcal{H}_{A_0} \oplus \mathcal{H}_{A_1}, \mathcal{H}_B = \mathcal{H}_{B_0} \oplus \mathcal{H}_{B_1},$$

then the whole system

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \cong \mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0} \oplus \mathcal{H}_{A_0} \otimes \mathcal{H}_{B_1} \oplus \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_0} \oplus \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}.$$

And if we only care about vectors exactly in the subspace

$$\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0} \oplus \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1} \subsetneq \mathcal{H}_A \otimes \mathcal{H}_B,$$

we then use the diagonal direct sum notation for vectors $v_0 \in \mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0}, v_1 \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$:

$$v_0 \oplus_\Delta v_0 := v_0 \oplus \vec{0}_{\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_1}} \oplus \vec{0}_{\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_0}} \oplus v_1 \in \mathcal{H}_{AB},$$

that is, $v_0 \oplus_\Delta v_1$ should be understood as an vector in the subspace $\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0} \oplus \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1} \subsetneq \mathcal{H}_{AB}$.

Definition 4.2 (complex local dilation, alternative)**.** *A strategy* $\tilde{S} = \{|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\}\}$ *is a complex local dilation of* $S = \{|\psi\rangle_{AB}, \{E_{xa}\}, \{F_{yb}\}\}$*, if there exist local isometry*

$$U_A : \mathcal{H}_A \to \mathcal{H}_{\tilde{A}_0} \otimes \mathcal{H}_{A'_0} \oplus \mathcal{H}_{\tilde{A}_1} \otimes \mathcal{H}_{\hat{A}_1},$$

$$U_B : \mathcal{H}_B \to \mathcal{H}_{\tilde{B}_0} \otimes \mathcal{H}_{B'_0} \oplus \mathcal{H}_{\tilde{B}_1} \otimes \mathcal{H}_{\hat{B}_1},$$

$U = U_A \otimes U_B$ *such that*

$$U[E_{xa} \otimes \mathsf{Id}_B |\psi\rangle_{AB}] = (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}_0} |\tilde{\psi}\rangle_{\tilde{A}_0\tilde{B}_0}) |\mathsf{aux}_0\rangle_{\hat{A}_0\hat{B}_0} \oplus_\Delta (\overline{\tilde{E}}_{xa} \otimes \mathsf{Id}_{\tilde{B}_1} |\tilde{\psi}\rangle_{\tilde{A}_1\tilde{B}_1}) |\mathsf{aux}_1\rangle_{\hat{A}_1\hat{B}_1}, \tag{19}$$

$$U[\mathsf{Id}_A \otimes F_{yb} |\psi\rangle_{AB}] = (\mathsf{Id}_{\tilde{A}_0} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle_{\tilde{A}_0\tilde{B}_0}) |\mathsf{aux}_0\rangle_{\hat{A}_0\hat{B}_0} \oplus_\Delta (\mathsf{Id}_{\tilde{A}_1} \otimes \overline{\tilde{F}}_{yb} |\tilde{\psi}\rangle_{\tilde{A}_1\tilde{B}_1}) |\mathsf{aux}_1\rangle_{\hat{A}_1\hat{B}_1} \tag{20}$$

hold for all a, b, x, y*, where* $|\mathsf{aux}_{0,1}\rangle$ *are subnormalized state (not necessarily orthogonal):* $\langle \mathsf{aux}_0 | \mathsf{aux}_0 \rangle + \langle \mathsf{aux}_1 | \mathsf{aux}_1 \rangle = 1$.

Lemma 4.3. *Definition 4.2 and Definition 4.1 imply each other.*

Proof. We show that Eq. (17) and Eq. (19) implies each other, and the rest can be proved similarly. Assume in Eq. (17) $\mathcal{H}_{\hat{A}_0\hat{B}_0} \cong \mathcal{H}_{\hat{A}_1\hat{B}_1}$ as we can always extend the smaller space to the larger one. Let

$$\begin{aligned} v_0 :=& (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}_0} |\tilde{\psi}\rangle_{\tilde{A}_0\tilde{B}_0}) |\mathsf{aux}_0\rangle_{\hat{A}_0\hat{B}_0} \in \mathcal{H}_{\tilde{A}_0\tilde{B}_0\hat{A}_0\hat{B}_0} =: V_0, \\ v_1 :=& (\overline{\tilde{E}}_{xa} \otimes \mathsf{Id}_{\tilde{B}_1} |\tilde{\psi}\rangle_{\tilde{A}_1\tilde{B}_1}) |\mathsf{aux}_1\rangle_{\hat{A}_1\hat{B}_1} \in \mathcal{H}_{\tilde{A}_1\tilde{B}_1\hat{A}_1\hat{B}_1} =: V_1, \end{aligned}$$

then V_0 and V_1 has the same dimension, and $V_0 \oplus V_1 \cong V_0 \otimes \mathbb{C}^2$. Then

$$Eq.\ (17) = v_0 \oplus_\Delta v_1 \cong v_0 \otimes |0\rangle_{\mathbb{C}^2} + v_1 \otimes |1\rangle_{\mathbb{C}^2}, Eq.\ (19) = v_0 \otimes |00\rangle_{A'B'} + v_1 \otimes |11\rangle_{A'B'}.$$

By embedding $\mathbb{C}^2$ into $\mathcal{H}_{A'B'}$ as its subspace spanned by $\{|00\rangle, |11\rangle\}$ we have Eq. (19) $\Longleftarrow$ Eq. (17). Similarly by projecting $\mathcal{H}_{A'B'}$ onto its subspace $\mathsf{span}\{|00\rangle, |11\rangle\} \cong \mathbb{C}^2$ we have Eq. (17) $\Longleftarrow$ Eq. (19). □

In this thesis we will work with Definition 4.1. Then complex self-testing is defined in terms of complex local dilation:

Definition 4.4 (complex self-testing). *A strategy* $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\})$ *is* complex self-tested *by a correlation* p *if it is a complex local dilation of all strategy producing* p.

4.3 Some properties of complex local dilation

The first two properties we show about complex local dilation are that, similar to its standard counterpart, complex local dilation preserves (exact) support-preservingness and projectiveness.

Proposition 4.5 (Analog of Proposition 3.5). *If* $S \hookrightarrow_{\mathbb{C}} \tilde{S}$, *then* S *is support preserving if and only if* $\tilde{S}$ *is support-preserving.*

Proof. First, if $S \hookrightarrow_{\mathbb{C}} \tilde{S}$, then

$$\begin{aligned}
&(\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} + (\overline{\tilde{E}_{xa}} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} \\
=&(U_A \otimes U_B)(E_{xa} \otimes \mathsf{Id}) |\psi\rangle \\
=&(U_A E_{xa} U_A^* \otimes \mathsf{Id})(U_A \otimes U_B) |\psi\rangle \\
=&(U_A E_{xa} U_A^* \otimes \mathsf{Id}) |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} + (U_A E_{xa} U_A^* \otimes \mathsf{Id}) |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'}.
\end{aligned}$$

And note that $|\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'}$ and $|\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'}$ are always orthogonal. So

$$\begin{aligned}
(\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} &= (U_A E_{xa} U_A^* \otimes \mathsf{Id}) |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} \\
(\overline{\tilde{E}_{xa}} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} &= (U_A E_{xa} U_A^* \otimes \mathsf{Id}) |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'}.
\end{aligned}$$

And we take the complex conjugate of the second line:

$$(\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} = (\overline{U_A E_{xa}} U_A^\intercal \otimes \mathsf{Id}) |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'}. \quad (21)$$

Recall that a strategy $(|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ is support-preserving if and only if there exist $\hat{E}_{xa}$, $\hat{F}_{yb}$ such that $E_{xa} \otimes \mathsf{Id} |\psi\rangle = \mathsf{Id} \otimes \hat{E}_{xa} |\psi\rangle$ and $\mathsf{Id} \otimes F_{yb} |\psi\rangle = \hat{F}_{yb} \otimes \mathsf{Id} |\psi\rangle$. Also without loss of generality we take the local isometry such that $|\psi\rangle, |\mathsf{aux}_{0,1}\rangle$ are real. Then $V_A \otimes V_B |\psi\rangle = \overline{V_A} \otimes \overline{V_B} |\psi\rangle$.

'If' part: Since $\tilde{S}$ is support-preserving, there exist operators $\hat{\tilde{E}}_{xa}$ such that $\tilde{E}_{xa} \otimes \mathsf{Id} |\tilde{\psi}\rangle = \mathsf{Id} \otimes \hat{\tilde{E}}_{xa} |\tilde{\psi}\rangle$. Taking the complex conjugate of both sides we get $\overline{\tilde{E}_{xa}} \otimes \mathsf{Id} |\tilde{\psi}\rangle = \mathsf{Id} \otimes \overline{\hat{\tilde{E}}_{xa}} |\tilde{\psi}\rangle$. Consider operators

$$\hat{E}_{xa} := U_B^*[(\hat{\tilde{E}}_{xa} \otimes |0\rangle\langle 0|_{B''} + \overline{\hat{\tilde{E}}_{xa}} \otimes |1\rangle\langle 1|_{B''}) \otimes \mathsf{Id}_{B'}] U_B.$$

Then

$$\begin{aligned}
(U_A \otimes U_B)(\mathsf{Id} \otimes \hat{E}_{xa}) |\psi\rangle =& (\mathsf{Id}_A \otimes U_B U_B^* \hat{\tilde{E}}_{xa}) |\tilde{\psi}\rangle |\mathsf{aux}_0\rangle |00\rangle + (\mathsf{Id}_A \otimes U_B U_B^* \overline{\hat{\tilde{E}}_{xa}}) |\tilde{\psi}\rangle |\mathsf{aux}_1\rangle |11\rangle \\
=& (\tilde{E}_{xa} \otimes U_B U_B^*) |\tilde{\psi}\rangle |\mathsf{aux}_0\rangle |00\rangle + (\overline{\tilde{E}_{xa}} \otimes U_B U_B^*) |\tilde{\psi}\rangle |\mathsf{aux}_1\rangle |11\rangle \\
=& (U_A \otimes U_B)(E_{xa} \otimes \mathsf{Id}) |\psi\rangle .
\end{aligned}$$

So S is support-preserving.

'Only if' part: Since S is support-preserving, there exist operators $\hat{E}_{xa}$ such that $E_{xa} \otimes \mathsf{Id} |\psi\rangle = \mathsf{Id} \otimes \hat{E}_{xa} |\psi\rangle$. Taking the complex conjugate of both sides we get $\overline{E_{xa}} \otimes \mathsf{Id} |\psi\rangle = \mathsf{Id} \otimes \overline{\hat{E}_{xa}} |\psi\rangle$. Consider operators

$$\hat{\tilde{E}}_{xa} := (|0\rangle\langle 0|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) U_B \hat{E}_{xa} U_B^* + (|1\rangle\langle 1|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) \overline{U_B} \overline{\hat{E}_{xa}} U_B^\intercal .$$

Then

$$\begin{aligned}
& (\mathsf{Id}_{\tilde{A}} \otimes \hat{\tilde{E}}_{xa} |\tilde{\psi}\rangle)(|\mathsf{aux}_0\rangle |00\rangle + |\mathsf{aux}_1\rangle |11\rangle)) \\
=& (\mathsf{Id}_{\tilde{A},A',A''} \otimes (|0\rangle\langle 0|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) U_B \hat{E}_{xa} U_B^*)(U_A \otimes U_B) |\psi\rangle \\
+& (\mathsf{Id}_{\tilde{A},A',A''} \otimes (|1\rangle\langle 1|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) \overline{U_B} \overline{\hat{E}_{xa}} U_B^\intercal)(\overline{U_A} \otimes \overline{U_B}) |\psi\rangle \\
=& U_A \otimes ((|0\rangle\langle 0|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) U_B \hat{E}_{xa}) |\psi\rangle + \overline{U_A} \otimes ((|1\rangle\langle 1|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) \overline{U_B} \overline{\hat{E}_{xa}}) |\psi\rangle \\
=& (U_A E_{xa} \otimes (|0\rangle\langle 0|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) U_B) |\psi\rangle + (\overline{U_A E_{xa}} \otimes (|1\rangle\langle 1|_{B''} \otimes \mathsf{Id}_{\tilde{B},B'}) \overline{U_B}) |\psi\rangle \\
=& (U_A E_{xa} U_A^* \otimes \mathsf{Id}) |\tilde{\psi}\rangle |\mathsf{aux}_0\rangle |00\rangle + (\overline{U_A E_{xa}} U_A^\intercal \otimes \mathsf{Id}) |\tilde{\psi}\rangle |\mathsf{aux}_1\rangle |11\rangle \\
=& (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle)(|\mathsf{aux}_0\rangle |00\rangle + |\mathsf{aux}_1\rangle |11\rangle) \text{ (by Eq. (21)).}
\end{aligned}$$

So $\tilde{E}_{xa} \otimes \mathsf{Id}_{A'A''}$ and $\Pi_{\tilde{A}} \otimes \Pi_{\mathsf{aux},A}$ commute. Note that

$$[\tilde{E}_{xa} \otimes \Pi_{A'A''}, \Pi_{\tilde{A}} \otimes \Pi_{\mathsf{aux},A}] = [\tilde{E}_{xa}, \Pi_{\tilde{A}}] \otimes \Pi_{\mathsf{aux},A}.$$

So $\tilde{E}_{xa}$ and $\Pi_{\tilde{A}}$ commute, and then $\tilde{S}$ is support-preserving. □

Proposition 4.6 (Analog of Proposition 3.7). *If $S \hookrightarrow_{\mathbb{C}} \tilde{S}$, then S is 0-projective if and only if $\tilde{S}$ is 0-projective.*

Proof. Note that

$$\begin{aligned}
U[E_{xa} \otimes \mathsf{Id}_B |\psi\rangle_{AB}] =& (\tilde{E}_{xa} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} \\
&+ (\overline{\tilde{E}_{xa}} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} \\
U[(\mathsf{Id}_A - E_{xa}) \otimes \mathsf{Id}_B |\psi\rangle_{AB}] =& ((\mathsf{Id}_{\tilde{A}} - \tilde{E}_{xa}) \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_0\rangle_{\hat{A}\hat{B}} |00\rangle_{A'B'} \\
&+ ((\mathsf{Id}_{\tilde{A}} - \overline{\tilde{E}_{xa}} \otimes \mathsf{Id}_{\tilde{B}} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) |\mathsf{aux}_1\rangle_{\hat{A}\hat{B}} |11\rangle_{A'B'} .
\end{aligned}$$

Take the inner product of the above two equations, one have that

$$\begin{aligned}
\langle\psi|E_{xa}(\mathsf{Id}_A - E_{xa}) \otimes \mathsf{Id}_B|\psi\rangle =& \langle\tilde{\psi}|\tilde{E}_{xa}(\mathsf{Id}_{\tilde{A}} - \tilde{E}_{xa}) \otimes \mathsf{Id}_{\tilde{B}}|\tilde{\psi}\rangle \langle\mathsf{aux}_0|\mathsf{aux}_0\rangle \\
&+ \langle\tilde{\psi}|\overline{\tilde{E}_{xa}}(\mathsf{Id}_{\tilde{A}} - \overline{\tilde{E}_{xa}}) \otimes \mathsf{Id}_{\tilde{B}}|\tilde{\psi}\rangle \langle\mathsf{aux}_1|\mathsf{aux}_1\rangle .
\end{aligned}$$

On one hand, if $\langle\tilde{\psi}|\tilde{E}_{xa}(\mathsf{Id}_{\tilde{A}} - \tilde{E}_{xa}) \otimes \mathsf{Id}_{\tilde{B}}|\tilde{\psi}\rangle = 0$, then so is $\langle\tilde{\psi}|\overline{\tilde{E}_{xa}}(\mathsf{Id}_{\tilde{A}} - \overline{\tilde{E}_{xa}}) \otimes \mathsf{Id}_{\tilde{B}}|\tilde{\psi}\rangle$, and hence $\langle\psi|E_{xa}(\mathsf{Id}_A - E_{xa}) \otimes \mathsf{Id}_B|\psi\rangle = 0$. On the other hand, since both $\tilde{E}_{xa}(\mathsf{Id}_{\tilde{A}} - \tilde{E}_{xa})$ and $(\mathsf{Id}_{\tilde{A}} - \overline{\tilde{E}_{xa}})$ are positive, $\langle\psi|E_{xa}(\mathsf{Id}_A - E_{xa}) \otimes \mathsf{Id}_B|\psi\rangle = 0$ implies that $\langle\tilde{\psi}|\tilde{E}_{xa}(\mathsf{Id}_{\tilde{A}} - \tilde{E}_{xa}) \otimes \mathsf{Id}_{\tilde{B}}|\tilde{\psi}\rangle = 0$, hence $\tilde{S}$ is 0-projective. So we conclude that S is 0-projective if and only if $\tilde{S}$ is 0-projective. □

Proposition 4.6 and 4.5 have the following consequence: for a full-rank, PVM strategy to be complex self-tested, it cannot be 'one-sided complex'.

Theorem 4.7. *Let $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{E}_{xa}\}, \{\tilde{F}_{yb}\})$ be a full-rank, PVM strategy with real measurements $\tilde{E}_{xa}$, real state $|\tilde{\psi}\rangle$, and at least one $\tilde{F}_{yb}$ which is not real. Then $\tilde{S}$ cannot be complex self-tested.*

Proof. We prove this by showing $\mathsf{re}\,\tilde{S} := (|\tilde{\psi}\rangle, \{\tilde{E}_{xa}\}, \{\mathsf{re}\,\tilde{F}_{yb}\})$ produces the same correlation as $\tilde{S}$, but cannot be complex local dilated to $\tilde{S}$. First of all, we note that $\mathsf{re}\,\tilde{F}_{yb} = 1/2(\tilde{F}_{yb} + \overline{\tilde{F}_{yb}})$, a convex combination of POVMs. So $\{\mathsf{re}\,\tilde{F}_{yb}\}_b$ gives a valid POVM.

To show that $\mathsf{re}\,\tilde{S}$ produces the same correlation as $\tilde{S}$, notice that $\mathsf{im}\,\tilde{F}_{yb}$ is anti-symmetric. Therefore $\langle\tilde{\psi}|\tilde{E}_{xa}\otimes\mathsf{im}\,\tilde{F}_{yb}|\tilde{\psi}\rangle = 0$ for all a, b, x, y. Then $\langle\tilde{\psi}|\tilde{E}_{xa}\otimes\tilde{F}_{yb}|\tilde{\psi}\rangle = \langle\tilde{\psi}|\tilde{E}_{xa}\otimes\mathsf{re}\,\tilde{F}_{yb}|\tilde{\psi}\rangle$.

To show that $\mathsf{re}\,\tilde{S}$ cannot be complex local dilated to $\tilde{S}$, we first prove that $\{\mathsf{re}\,\tilde{F}_{yb}\}$ is PVM if and only if $\tilde{F}_{yb}$ is real. We have that

$$\mathsf{re}\,\tilde{F}_{yb}^2 = \frac{1}{4}(\tilde{F}_{yb} + \overline{\tilde{F}_{yb}} + \overline{\tilde{F}_{yb}}\tilde{F}_{yb} + \tilde{F}_{yb}\overline{\tilde{F}_{yb}}).$$

So $\mathsf{re}\,\tilde{F}_{yb}$ being projection ($(\mathsf{re}\,\tilde{F}_{yb})^2 = \mathsf{re}\,\tilde{F}_{yb}$) is equivalent to

$$\begin{aligned}&\overline{\tilde{F}_{yb}}\tilde{F}_{yb} + \tilde{F}_{yb}\overline{\tilde{F}_{yb}} = \overline{\tilde{F}_{yb}} + \tilde{F}_{yb}\\ \Leftrightarrow&\tilde{F}_{yb}\overline{\tilde{F}_{yb}}\tilde{F}_{yb} = \tilde{F}_{yb}.\end{aligned}$$

Also note that both $\tilde{F}_{yb}, \overline{\tilde{F}_{yb}}$ are projections of the same rank. So this implies $\tilde{F}_{yb} = \overline{\tilde{F}_{yb}}$.

Since there is at least one $\tilde{F}_{yb}$ which is not real, $\mathsf{re}\,\tilde{S}$ is not PVM. Therefore $\mathsf{re}\,\tilde{S} \hookrightarrow_{\mathbb{C}} \tilde{S}$ does not hold, since complex local dilation preserves projectivity (Proposition 4.6). □

Finally, we discuss properties related to real simulation of quantum strategies [MMG09]. The idea of real simulation is that any quantum correlation can be dilated to a real strategy without affecting its correlation. To achieve this, let $|\pm i\rangle := (|0\rangle \pm i\,|1\rangle)/\sqrt{2}$ be the eigenstate of Pauli matrix σ_Y.

Definition 4.8 (real simulation). *Let $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ be a complex strategy. The real simulation S_R of S is defined as $S_R := (|\psi_R\rangle, \{E_{R,xa}\}, \{F_{R,yb}\})$, where*

$$\begin{aligned}|\psi_R\rangle &:= (|+i+i\rangle\,|\psi\rangle + |-i-i\rangle\,|\overline{\psi}\rangle)/\sqrt{2}\\ E_{R,xa} &:= |+i\rangle\langle+i|\otimes E_{xa} + |-i\rangle\langle-i|\otimes\overline{E_{xa}}\\ F_{R,yb} &:= |+i\rangle\langle+i|\otimes F_{yb} + |-i\rangle\langle-i|\otimes\overline{F_{yb}}.\end{aligned}$$

It is straightforward to verify that $|\psi_R\rangle, A_{R,xa}, B_{R,yb}$ all have real entries, and S_R gives the same correlation as S. We remark that the auxiliary state $|\pm i\rangle$ is not strictly necessary; any state $|\phi\rangle$ satisfying $\langle\phi|\overline{\phi}\rangle = 0$ would suffice. And $|\pm i\rangle$ is the smallest example of such states.

On real simulation and complex local dilation we have the following property:

Proposition 4.9. *If $S \hookrightarrow_{\mathbb{C}} \tilde{S}$, then $S_R \hookrightarrow \tilde{S}_R$.*

Proof. Given that $S \hookrightarrow_{\mathbb{C}} \tilde{S}$, there exist local isometries V_A, V_B and auxiliary states $|\mathsf{aux}_0\rangle, |\mathsf{aux}_1\rangle$ that satisfy the complex local dilation relations. Now consider the action of $V_{A,R} := |+i\rangle\langle+i| \otimes V_A + |-i\rangle\langle-i| \otimes \overline{V_A}, V_{B,R} := V_B \otimes |+i\rangle\langle+i| + \overline{V_B} \otimes |-i\rangle\langle-i|$ on S_R, we have

$$
\begin{aligned}
&(V_{A,R} \otimes V_{B,R}) (E_{xa,R} \otimes F_{yb,R} |\psi_R\rangle) \\
=&(V_{A,R} \otimes V_{B,R}) \frac{1}{\sqrt{2}} \left(|+i+i\rangle (E_{xa} \otimes F_{yb} |\psi\rangle) + |-i-i\rangle (\overline{E_{xa}} \otimes \overline{F_{yb}} |\psi\rangle) \right) \\
=&\frac{1}{\sqrt{2}} \left(|+i+i\rangle (V_A \otimes V_B)(E_{xa} \otimes F_{yb} |\psi\rangle) + |-i-i\rangle (\overline{V_A} \otimes \overline{V_B})(\overline{E_{xa}} \otimes \overline{F_{yb}} |\psi\rangle) \right) \\
=&\frac{1}{\sqrt{2}} (|+i+i\rangle |00\rangle |\mathsf{aux}_0\rangle (\tilde{E}_{xa} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle) + |+i+i\rangle |11\rangle |\mathsf{aux}_1\rangle (\overline{\tilde{E}_{xa}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle) + \\
&|-i-i\rangle |00\rangle |\mathsf{aux}_0\rangle (\overline{\tilde{E}_{xa}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle) + |-i-i\rangle |11\rangle |\mathsf{aux}_1\rangle (\tilde{E}_{xa} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle)) \\
=&\frac{1}{\sqrt{2}} (|00\rangle |\mathsf{aux}_0\rangle) (|+i+i\rangle \tilde{E}_{xa} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle + |-i-i\rangle \overline{\tilde{E}_{xa}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle) + \\
&\frac{1}{\sqrt{2}} (|11\rangle |\mathsf{aux}_1\rangle) (|-i-i\rangle \tilde{E}_{xa} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle + |+i+i\rangle \overline{\tilde{E}_{xa}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle).
\end{aligned}
$$

Let U_i be the 2-dimensional unitary that maps $|\pm i\rangle$ to $|\mp i\rangle$. Then consider the action of local unitary $U := |0\rangle\langle 0| \otimes \mathsf{Id}_{\mathsf{aux}} \otimes \mathsf{Id}_i + |1\rangle\langle 1| \otimes \mathsf{Id}_{\mathsf{aux}} \otimes U_i$. Clearly $U \otimes U$ keeps $|00\rangle |\mathsf{aux}_0\rangle |\pm i \pm i\rangle$ unchanged, and maps $|11\rangle |\mathsf{aux}_1\rangle |\pm i \pm i\rangle$ to $|11\rangle |\mathsf{aux}_1\rangle |\mp i \mp i\rangle$. Therefore,

$$
\begin{aligned}
&(U \otimes \mathsf{Id}_{\tilde{A}} \otimes U \otimes \mathsf{Id}_{\tilde{B}}) (V_{A,R} \otimes V_{B,R}) (E_{xa,R} \otimes F_{yb,R} |\psi_R\rangle) \\
=&\frac{1}{\sqrt{2}} (|00\rangle |\mathsf{aux}_0\rangle) (|+i+i\rangle \tilde{E}_{xa} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle + |-i-i\rangle \overline{\tilde{E}_{xa}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle) + \\
&\frac{1}{\sqrt{2}} (|11\rangle |\mathsf{aux}_1\rangle) (|+i+i\rangle \tilde{E}_{xa} \otimes \tilde{F}_{yb} |\tilde{\psi}\rangle + |-i-i\rangle \overline{\tilde{E}_{xa}} \otimes \overline{\tilde{F}_{yb}} |\tilde{\psi}\rangle) \\
=&(|00\rangle |\mathsf{aux}_0\rangle + |11\rangle |\mathsf{aux}_1\rangle)(\tilde{E}_{xa,R} \otimes \tilde{F}_{yb,R} |\tilde{\psi}_R\rangle).
\end{aligned}
$$

Also notice that $(|00\rangle |\mathsf{aux}_0\rangle + |11\rangle |\mathsf{aux}_1\rangle)$ is a unit vector. We conclude that $S_R \hookrightarrow \tilde{S}_R$ via local isometry $(U \otimes \mathsf{Id}_{\tilde{A}} \otimes U \otimes \mathsf{Id}_{\tilde{B}}) (V_{A,R} \otimes V_{B,R})$. □

4.4 An operator-algebraic characterization

Inspired by the work of [PSZZ24], here we discuss the operator-algebraic picture of complex self-testing. A key observation is that if $\tilde{S}$ is a complex local dilation of S, then $\tilde{S}$ and S has the same real part of their higher order moments.

Proposition 4.10. *If support-preserving $\tilde{S}$ is complex self-tested by $p(a,b|x,y)$, then*

$$\mathsf{re}\,\langle\psi|E\otimes F|\psi\rangle\,.$$

will be the same for all strategy S producing $p(a,b|x,y)$, where $E = E_{x_1a_1}E_{x_2a_2}\cdots E_{x_ka_k}$, $F = F_{y_1b_1}F_{y_2b_2}\cdots F_{y_lb_l}$ are words in the POVM elements from S.

Proof. It is clear that the statement is true with for words of length 0 or 1. Consider $E = E_{x_1a_1}E_{x_2a_2}$. Given any S producing $p(a,b|x,y)$, let $V = V_A\otimes V_B$ be the isometry and $|\mathsf{aux}_{0,1}\rangle$ be the auxiliary state from the complex self-test. We have that

$$\begin{aligned}
&V(E_{x_1a_1}E_{x_2a_2}\otimes \mathsf{Id}_B)\,|\psi\rangle\\
=&(V_AE_{x_1a_1}V_A^*\otimes \mathsf{Id}_B)V(E_{x_2a_2}\otimes \mathsf{Id}_B)\,|\psi\rangle\\
=&(V_AE_{x_1a_1}V_A^*\otimes \mathsf{Id}_B)((\tilde{E}_{x_2a_2}\otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\overline{\tilde{E}_{x_2a_2}}\otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle)\\
=&(V_AE_{x_1a_1}V_A^*\otimes \mathsf{Id}_B)((\mathsf{Id}_{\tilde{A}}\otimes \hat{\tilde{E}}_{x_2a_2})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\mathsf{Id}_{\tilde{A}}\otimes \overline{\hat{\tilde{E}}_{x_2a_2}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle)\\
=&(\tilde{E}_{x_1a_1}\otimes \hat{\tilde{E}}_{x_2a_2})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\overline{\tilde{E}_{x_1a_1}}\otimes \overline{\hat{\tilde{E}}_{x_2a_2}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle \;\text{(by Eq. (21))}\\
=&(\tilde{E}_{x_1a_1}\tilde{E}_{x_2a_2}\otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\overline{\tilde{E}_{x_1a_1}\tilde{E}_{x_2a_2}}\otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle\,.
\end{aligned}$$

(The third equation uses the fact that $\tilde{S}$ is support preserving, and so is S due to Proposition 4.5.) Then by induction we get $V(E\otimes \mathsf{Id})\,|\psi\rangle = (\tilde{E}\otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\overline{\tilde{E}}\otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle$. Similarly for Bob's operator, $V(\mathsf{Id}\otimes F)\,|\psi\rangle = (\mathsf{Id}_{\tilde{A}}\otimes \tilde{F})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\mathsf{Id}_{\tilde{A}}\otimes \overline{\tilde{F}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle$. Then

$$\begin{aligned}
V(E\otimes F)\,|\psi\rangle =&(V_AEV_A^*\otimes \mathsf{Id}_{\tilde{B}\hat{B}B'})V(\mathsf{Id}\otimes F)\,|\psi\rangle\\
=&(V_AEV_A^*\otimes \mathsf{Id}_{\tilde{B}\hat{B}B'})[(\mathsf{Id}_{\tilde{A}}\otimes \tilde{F})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\mathsf{Id}_{\tilde{A}}\otimes \overline{\tilde{F}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle]\\
=&(\mathsf{Id}_{\tilde{A}\hat{A}A'}\otimes \tilde{F})(V_AEV_A^*\otimes \mathsf{Id}_{\tilde{B}\hat{B}B'})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle\\
&+(\mathsf{Id}_{\tilde{A}\hat{A}A'}\otimes \overline{\tilde{F}})(V_AEV_A^*\otimes \mathsf{Id}_{\tilde{B}\hat{B}B'})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle\\
=&(\tilde{E}\otimes \tilde{F})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + (\overline{\tilde{E}}\otimes \overline{\tilde{F}})\,|\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle\,.
\end{aligned}$$

Note that $V\,|\psi\rangle = |\tilde{\psi}\rangle\,|\mathsf{aux}_0\rangle\,|00\rangle + |\tilde{\psi}\rangle\,|\mathsf{aux}_1\rangle\,|11\rangle$. Take the inner product of the two sides respectively, we get

$$\langle\psi|E\otimes F|\psi\rangle = \langle\tilde{\psi}|\tilde{E}\otimes \tilde{F}|\tilde{\psi}\rangle\,|\,|\mathsf{aux}_0\rangle\,|^2 + \langle\tilde{\psi}|\overline{\tilde{E}}\otimes \overline{\tilde{F}}|\tilde{\psi}\rangle\,|\,|\mathsf{aux}_1\rangle\,|^2.$$

And the final statement is achieved by taking the real part of both sides of the equation. □

Note that if $\tilde{S}$ and S already have all-real moment, then it reduces to the case of (standard) self-testing. So our Proposition 4.9 could also be proven from Proposition 4.10.

In the language of C* algebra, such property can be described by having a unique finite dimensional real state on some universal real C* algebra:

Lemma 4.11. *The following two statements are equivalent:*

1. *The real parts of moments*
$$\mathsf{re}\,\langle\psi|E\otimes F|\psi\rangle$$
coincide for all strategy producing $p(a,b|x,y)$*,*

2. *There is a unique finite dimensional real state on* $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},POVM}\otimes_{\min}\mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathbb{R}POVM}$ *that agree with* $p(a,b|x,y)$*.*

Here $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},POVM}$ *is the universal real C* algebra generated by positive contractions* $\{e_{xa}: x\in\mathcal{I}_A, a\in\mathcal{O}_A\}$*, subject to the relations* $\sum_a e_{xa}=1,\forall x\in\mathcal{I}_A$*, and similarly* $\mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{POVM}$ *is generated by* $\{f_{yb}: y\in\mathcal{I}_B, b\in\mathcal{O}_B\}$*. A real state* f *agrees with* $p(a,b|x,y)$ *whenever* $f(e_{xa}\otimes f_{yb})=p(a,b|x,y)$ *holds for all* a,b,x,y*.*

Proof. (1)⇒(2): For any finite dimensional real state f that agrees with p, its real GNS construction (see e.g. [Li03]) gives a representation on a finite dimensional real Hilbert space, whose matrix representation gives raise to a real strategy which is moment-real. By Proposition 4.10, those f then agrees with all the words of generators, so f is determined on the whole real C* algebra from its real linearity.

(2)⇒(1): Suppose $S^{(0)},S^{(1)}$ differs in their real parts of moments, define real states f_0,f_1 by setting $f_0(e_{xa}\otimes f_{yb})=\mathsf{re}\,\langle\psi^{(0)}|E^{(0)}_{xa}\otimes F^{(0)}_{yb}|\psi^{(0)}\rangle$, $f_1(e_{xa}\otimes f_{yb})=\mathsf{re}\,\langle\psi^{(1)}|E^{(1)}_{xa}\otimes F^{(1)}_{yb}|\psi^{(1)}\rangle$, and extending them by real linearity. Then f_0,f_1 are valid real states on $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},\mathrm{POVM}}\otimes_{\min}\mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathbb{R}\mathrm{POVM}}$ but $f_0\neq f_1$. □

Theorem 4.12. *If a support-preserving* $\tilde{S}$ *is complex self-tested by a correlation* p*, then there is a unique finite-dimensional real state on* $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},POVM}\otimes_{\min}\mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathbb{R}POVM}$ *that agrees with* p*.*

Proof. Combining Proposition 4.10 and Lemma 4.11. □

To the best of our knowledge it is yet unclear whether the reversed statement, similar to standard self-testing, is also true for complex self-testing. Therefore we leave it as an conjecture:

Conjecture 4.13. *If there is a unique finite-dimensional real state on $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},POVM} \otimes_{\min} \mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathbb{R},POVM}$ that agrees with p which is extreme in C_q, then there is a support-preserving $\tilde{S}$ such that $\tilde{S}$ is complex self-tested by correlation p.*

As our final remark on this, if one would like to prove the conjecture by reproducing the process in [PSZZ24], then one would need to show that any real state on $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},\mathrm{POVM}} \otimes_{\min} \mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathbb{R},\mathrm{POVM}}$ is actually the real part of a (complex) state on $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathrm{POVM}} \otimes_{\min} \mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}}$. To the best of our knowledge, it is known to be true only if a representation of $\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathbb{R},\mathrm{POVM}} \otimes_{\min} \mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathbb{R},\mathrm{POVM}}$ is obtained from regarding a representation of $(\mathcal{A}^{\mathcal{I}_A,\mathcal{O}_A}_{\mathrm{POVM}} \otimes_{\min} \mathcal{A}^{\mathcal{I}_B,\mathcal{O}_B}_{\mathrm{POVM}})$ as a real C*-algebra [Li03, Proposition 1.1.6].

4.5 Realness of quantum strategies

Theorem 4.12 indicates that the real parts of higher order moments are essential in complex self-testing, and leads our attention to quantum strategies with real moments. An obvious candidate is the family of strategies with a real matrix representation. Then the natural question to ask is, are there any other strategies with real high order moments? If the answer is affirmative then it would be a more appropriate definition of 'real' quantum strategies in the context of self-testing.

Here we solve this problem by fully identifying the family of strategies with real high order moments, which we call 'self-conjugate' strategies. For those strategies the action of complex conjugate is trivial. For simplicity in this section we consider irreducible strategies, that is, the the POVM elements generate the whole matrix algebra as (complex) algebra $\mathsf{Alg}_{\mathbb{C}}(E_{xa} \otimes F_{yb} : a, b, x, y) = B(\mathcal{H}_A \otimes \mathcal{H}_B)$. By the fundamental structure theorem of finite dimensional C*-algebras, any strategy can be decomposed as a direct sum of irreducible ones.

Definition 4.14. *A strategy S is:*

1. real *if some matrix representation of S is real;*
2. self-conjugate *if for some basis there exist local unitaries U_A, U_B such that*

$$U_A E_{xa} U_A^* = \overline{E_{xa}},\ U_B F_{yb} U_B^* = \overline{F_{yb}},\ U_A \otimes U_B \left|\psi\right\rangle = \left|\overline{\psi}\right\rangle$$

holds for all x, y, a, b.

3. moment-real *if* $\langle\psi|\, E\otimes F\,|\psi\rangle \in \mathbb{R}$ *for all words* E *of measurements* E_{xa} *and words* F *of measurements* F_{yb}.

Clearly all real strategies are self-conjugate (by taking $U_A = U_B = \mathsf{Id}$), and self-conjugate strategies indeed have real higher order moments: for any word $E\otimes F$,

$$\overline{\langle\psi|E\otimes F|\psi\rangle} = \langle\overline{\psi}|\overline{E\otimes F}|\overline{\psi}\rangle = \langle\psi|U^*U(E\otimes F)U^*U|\psi\rangle = \langle\psi|E\otimes F|\psi\rangle\,.$$

Conversely, it is also true that:

Theorem 4.15. *If a irreducible strategy* $S = (|\psi\rangle, \{E_{xa}\}, \{F_{yb}\})$ *has real higher order moments (*$\langle\psi|E\otimes F|\psi\rangle$ *is real for all words* $E\otimes F$*), then* S *is self-conjugate.*

The proof of Theorem 4.15 relies on the following proposition:

Proposition 4.16 ([Vol22]). *For any irreducible collection* $\{X_1, ..., X_n\} \subseteq B(\mathcal{H})$*, there is* $U \in U(\mathcal{H})$ *such that* $UX_jU^* = \overline{X_j}$ *for* $j = 1, \ldots, n$ *if and only if* $\mathsf{Alg}_{\mathbb{R}}(X_j : j) \neq B(\mathcal{H})$.

Proof of Theorem 4.15. Suppose for contradiction that S has real higher order moments but not self-conjugate. Assume that the conditions in Definition 4.14 at least fail for $\{E_{xa} : x, a\}$. Then by Proposition 4.16 $\{E_{xa} : x, a\}$ generate $B(\mathcal{H}_A)$ as a real algebra. Let $|\psi\rangle = \sum_{i=1}^r |u_i\rangle\,|v_i\rangle$ for linearly independent $|u_i\rangle \in \mathcal{H}_A$ and linearly independent $|v_i\rangle \in \mathcal{H}_B$. Note that

$$\langle\psi|\, E\otimes F\,|\psi\rangle = \sum_{i,j=1}^{r} \langle u_i|\, E\,|u_j\rangle \cdot \langle v_i|\, F\,|v_j\rangle \tag{22}$$

for $E \in B(\mathcal{H}_A)$ and $F \in B(\mathcal{H}_B)$. Since $\{F_{yb}\}$ are irreducible, there exists a word F of $\{F_{yb} : y, b\}$ such that not all $\langle v_i|\, F\,|v_j\rangle$ are 0. In particular, $\langle v_{i_0}|\, F\,|v_{j_0}\rangle \neq 0$ for some i_0, j_0. Since $\{E_{xa}\}$ generate $B(\mathcal{H}_A)$ as a real algebra, there is a real combination $E = \sum_k \alpha_k E_k$ of words E_k of E_{xa} such that

$$\langle u_i|\, E\,|u_j\rangle = \begin{cases} i\overline{\langle v_{i_0}|\, F\,|v_{j_0}\rangle} & \text{if } i = i_0, j = j_0 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\sum_k \alpha_k \langle\psi|\, E_k\otimes F\,|\psi\rangle = \langle\psi|\, E\otimes F\,|\psi\rangle \notin \mathbb{R}$$

by (22), and so $\langle\psi|\, E_k\otimes F\,|\psi\rangle \notin \mathbb{R}$ for some k, which contradicts S having real higher order moments.

Therefore there are $U_A \in U_{d_A}(\mathbb{C})$ and $U_B \in U_{d_B}(\mathbb{C})$ such that

$$U_A E_{xa} U_A^* = \overline{E_{xa}},\ U_B F_{yb} U_B^* = \overline{F_{yb}}$$

for all x, y, a, b. Denote $|\psi'\rangle = U_A^* \otimes U_B^* |\overline{\psi}\rangle$. Clearly,

$$\langle\psi'|E \otimes F|\psi'\rangle = \langle\overline{\psi}|U(E \otimes F)U^*|\overline{\psi})\rangle = \overline{\langle\psi|E \otimes F|\psi\rangle} = \langle\psi|E \otimes F|\psi\rangle$$

for all words E of E_{xa} and words F of F_{yb}. Since both sides are complex linear in E, F, it furthermore follows that it holds for all $\mathsf{Alg}_{\mathbb{C}}(E_{xa}\colon x, a) \otimes \mathsf{Alg}_{\mathbb{C}}(F_{yb}\colon y, b) = B(\mathcal{H}_A \otimes \mathcal{H}_B)$. From [PSZZ24, Lemma 4.11] $|\psi\rangle\langle\psi| = |\psi'\rangle\langle\psi'|$, or $|\psi'\rangle = \alpha |\psi\rangle$ for some phase $\alpha \in \mathbb{C}$ of modulus 1. Therefore we have

$$\overline{E_{xa}} = (\alpha U_A) E_{xa} (\alpha U_A)^*, \quad \overline{F_{yb}} = U_B F_{yb} U_B^*, \quad |\overline{\psi}\rangle = U_A \otimes U_B |\psi'\rangle = (\alpha U_A) \otimes U_B |\psi\rangle$$

for unitaries αU_A and U_B. □

Interestingly enough, there exists self-conjugate strategies which are not real. Such strategies generate the quaternion matrix algebra as real *-algebra, therefore only exist in Hilbert spaces with even local dimensions greater than 2 [Vol22]. So we conclude that

$$\text{Real} \subsetneq \text{Self-conjugate} = \text{Moment real},$$

where the first inclusion becomes the identity when the local dimension is 2 or odd.

5 Self-testing all projective measurements

The work presented in this section was conducted with Laura Mančinska and Jurij Volčič and has been published on Nat. Phys. under the title of "All real projective measurements can be self-tested" [CMV24]. Some format and notations from it might be changes to fit with the layout of this thesis.

5.1 Motivation

Recall that Theorem 3.38 showed that for $\tilde{S}$ to be assumption-free self-tested, it has to be both support-preserving and 0-projective. Then it becomes natural to ask whether all such strategies can possibly be self-tested. The first step towards fully solving this problem is probably to break it down to self-testing of any full-rank state and self-testing of any projective measurement. Here by self-testing of a state $|\tilde{\psi}\rangle$ we mean that constructing a strategy that incorporates $|\tilde{\psi}\rangle$, and similarly for measurements. The question regarding self-testable states has been extensively studied in [CGS17, SBR+23], while the self-testing of general measurements has remained elusive.

In this work we provide the first results for self-testing of general measurements by putting forth a fully explicit assumption-free robust self-testing protocol for any real projective measurement. To achieve we formalise the theoretical method of post-hoc self-testing and identify a sufficient condition for its application in Sect. 5.3. Applying post-hoc self-testing to an established self-test from the recent work [MPS24] allows us to obtain our self-testing construction for any real projective measurement in Sect. 5.4. Additionally, we develop a new technique called iterative self-testing which involves sequential application of post-hoc self-testing in Sect. 5.5. Iterative self-testing is inspired by our self-testing construction, and offers a handy way for developing new self-tests based on pre-existing ones.

5.2 Measurements in the observable picture

Before we delve into the new techniques and results, let us first recap of the observable picture of quantum measurements. It gives an alternative characterization of POVMs, and it turns out to be very useful in our calculations.

In many cases, especially when the measurement is projective (i.e., all operators in the POVMs are projections), it can be more convenient to work with generalized observables instead of operators of POVMs. Given a POVM $\{E_{xa}\}$, its generalized observables are given

by

$$A_x^{(j)} := \sum_{a=0}^{|\mathcal{O}_A|-1} \omega^{aj} E_{xa},$$

where $\omega = e^{i2\pi/|\mathcal{O}_A|}$. Note that $A_x^{(0)} = \mathsf{Id}$ by definition. Due to the invertibility of the transform, $\{E_{xa}\}$ can be recovered from $\{A_x^{(j)}\}$ by $E_a = \frac{1}{|\mathcal{O}_A|} \sum_{j=0}^{|\mathcal{O}_A|-1} \omega^{-aj} A_x^{(j)}$. So $\{A_x^{(j)}\}$ provides an alternative, yet full, description of the measurement. The following properties about the generalized observables hold: (see [KST+19] for a proof)

- For any POVM $\{E_{xa}\}$, $A_x^{(j)} A_x^{(j)*} \leq \mathsf{Id}$, $A_x^{(j)*} A_x^{(j)} \leq \mathsf{Id}$, i.e., $A_x^{(j)}$ are contractions.
- A POVM $\{E_{xa}\}$ is projective if and only if the corresponding $A_x := A_x^{(1)}$ is a unitary matrix of order $|\mathcal{O}_A|$. In this case, we call A_x the observable of $\{E_{xa}\}$, further having that $A_x^{(j)} = A_x^j$. Therefore,
- Projective measurements are fully characterised by its observable:

$$E_{xa} = \frac{1}{|\mathcal{O}_A|} \sum_{j=0}^{|\mathcal{O}_A|-1} \omega^{-aj} A_x^j,$$

  while in general, it might not be possible to recover the POVM elements of a measurement from A_x.

In this section only, we will specify quantum strategies by the tuple

$$S = (\rho_{AB}, \{A_x^{(j)}\}_{x\in\mathcal{I}_A, j\in\mathcal{O}_A}, \{B_y^{(k)}\}_{:y\in\mathcal{I}_B, k\in\mathcal{O}_B}),$$

where $A_x^{(j)} = \sum_{a=0}^{|\mathcal{O}_A|-1} \omega_A^{aj} E_{xa}$, $\omega_A = e^{i2\pi/|\mathcal{O}_A|}$, $B_y^{(k)} = \sum_{b=0}^{|\mathcal{O}_B|-1} \omega_B^{bk} N_{b|y}$, $\omega_B = e^{i2\pi/|\mathcal{O}_B|}$. The correlation is also conveniently specified via

$$\{\mathsf{Tr}[A_x^{(j)} \otimes B_y^{(k)} \rho]\}_{j,k,x,y} = \{\sum_{a,b} \omega_A^{aj} \omega_B^{bk} p(a,b|x,y)\}_{j,k,x,y}.$$

Furthermore, if all the measurements in S are all projective, we denote it by $S = (\rho_{AB}, \{A_x\}_{x\in\mathcal{I}_A}, \{B_y\}_{y\in\mathcal{I}_B})$ for simplicity. In this section only we shall present our results in terms of observables.

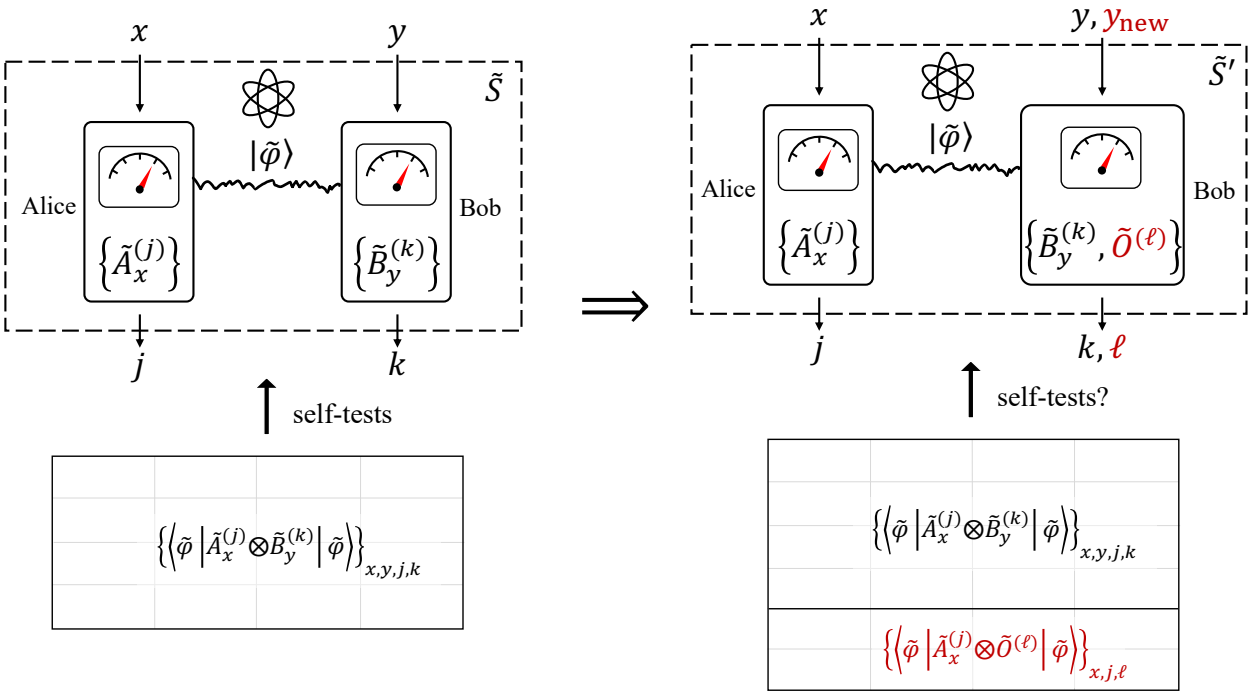


Figure 3: Post-hoc self-testing: starting from a self-tested strategy $\tilde{S}$ (on the left), if it is feasible to infer the new measurement $\tilde{O}^{(\ell)}$ with input y_{new} and output ℓ from correlations $\{\langle\psi|A_x^{(j)}\otimes O^{(\ell)}|\psi\rangle\}$, then extended strategy $\tilde{S}'$ (on the right) remains self-tested.

5.3 Robust post-hoc self-testing of projective measurements

The concept of post-hoc self-testing has been implicitly employed in prior works, such as self-testing of graph states [McK16], randomness certification [ABDC18, WKB+20], and one-sided self-testing [SBJ+23]. The review paper [SB20] was the first to summarize this technique and refer to it as 'post-hoc self-testing'. In this section, we formalise the idea of post-hoc self-testing and establish a sufficient condition for its application.

5.3.1 Definition

In post-hoc self-testing we consider a scenario where we have self-tested strategy $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{A}_x^{(j)}\}_x, \{\tilde{B}_y^{(k)}\}_y)$, and we would like to self-test an additional measurement $\{\tilde{O}^{(\ell)}\}$. We are interested to ask when can $\{\tilde{O}^{(\ell)}\}$ be self-tested by extending $\tilde{S}$. In particular, when is $\tilde{S}' = (|\tilde{\psi}\rangle, \{\tilde{A}_x^{(j)}\}_x, \{\tilde{B}_y^{(k)}, \tilde{O}^{(\ell)}\}_y)$ self-tested by the correlation it produces (Fig. 3)?

Since the reference strategy $\tilde{S} = (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}, \{\tilde{B}_y^{(k)}\})$ is robust self-tested by its correlation, to pass the test up to δ deviation Alice has to honestly perform some measurement

which can be ε-approximately local-dilated to $\{\tilde{A}_x^{(j)}\}$:

$$(U \otimes \mathsf{Id}_P)(A_x^{(j)} \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP} \approx_\varepsilon (\tilde{A}_x^{(j)} \otimes \mathsf{Id}_{\tilde{B}}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle$$

for some purification $\left|\psi\right\rangle_{ABP}$, local isometry U and auxiliary state $\left|\mathsf{aux}\right\rangle$. Then post-hoc self-testing for an additional observable $\tilde{O}^{(l)}$ would ask that the same U and $\left|\mathsf{aux}\right\rangle$ also connect $O^{(l)}$ and $\tilde{O}^{(l)}$ on the same shared state for any $O^{(l)}$ generating correlation close to that of $\tilde{O}^{(l)}$.

Definition 5.1 (robust post-hoc self-testing)**.** *Given the state $\left|\tilde{\psi}\right\rangle = \left|\tilde{\psi}\right\rangle_{\tilde{A}\tilde{B}}$ and generalized observables $\{\tilde{A}_x^{(j)}\}$, a L-output generalized observable $\{\tilde{O}^{(l)}\}$ is* robust post-hoc self-tested *(by the correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}^{(l)}|\tilde{\psi}\rangle\}$) based on $(\left|\tilde{\psi}\right\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\})$ if the following condition holds: for any $\varepsilon' > 0$, there exist $\varepsilon > 0$ and $\delta > 0$ such that:*

if $(U \otimes \mathsf{Id}_P)(A_x^{(j)} \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP} \approx_\varepsilon (\tilde{A}_x^{(j)} \otimes \mathsf{Id}_{\tilde{B}}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle$ for state $\left|\psi\right\rangle_{ABP}$, generalized observables $\{A_x^{(j)}\}$, local isometry $U = U_A \otimes U_B$ and state $\left|\mathsf{aux}\right\rangle_{A'B'}$, then any generalized observable $\{O^{(l)}\}$ having $|\langle\psi|A_x^{(j)} \otimes O^{(l)}|\psi\rangle - \langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}_y^{(l)}|\tilde{\psi}\rangle| < \delta$ satisfies

$$(U \otimes \mathsf{Id}_P)(\mathsf{Id}_A \otimes O_y^{(l)} \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP} \approx_{\varepsilon'} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{O}_y^{(l)}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle$$

for all $l \in [0, L-1]$.

Then post-hoc self-testing extends self-testing protocol in the following sense:

Proposition 5.2. *If correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$ robust self-tests $\tilde{S} = (\left|\tilde{\psi}\right\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}, \{\tilde{B}_y^{(k)}\})$, and correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}^{(k)}|\tilde{\psi}\rangle\}$ robust post-hoc self-tests $\{\tilde{O}^{(l)}\}$ based on $(\left|\tilde{\psi}\right\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\})$, then the extended correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle\} \cup \{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}^{(l)}|\tilde{\psi}\rangle\}$ robust self-tests the extended strategy $\tilde{S}^{Extend} = (\left|\tilde{\psi}\right\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}, \{\tilde{B}_y^{(k)}, \tilde{O}^{(l)}\})$.*

Proof. By robust post-hoc self-testing, for any ε_1 there exist ε_2 and δ_1 such that

$$(U \otimes \mathsf{Id}_P)(\mathsf{Id}_A \otimes O_y^{(l)} \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP} \approx_{\varepsilon_1} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{O}_y^{(l)}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle,$$

if $|\langle\psi|A_x^{(j)} \otimes O^{(l)}|\psi\rangle - \langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}_y^{(l)}|\tilde{\psi}\rangle| < \delta_1$. Since $\tilde{S} = (\left|\tilde{\psi}\right\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}, \{\tilde{B}_y^{(k)}\})$ is robust self-tested, for ε_2 there exist δ_2 such that

$$(U \otimes \mathsf{Id}_P)(A_x^{(j)} \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP} \approx_{\varepsilon_2} (\tilde{A}_x^{(j)} \otimes \mathsf{Id}_{\tilde{B}}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle,$$
$$(U \otimes \mathsf{Id}_P)(\mathsf{Id}_A \otimes B_y^{(k)} \otimes \mathsf{Id}_P) \left|\psi\right\rangle_{ABP} \approx_{\varepsilon_2} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{B}_y^{(k)}) \left|\tilde{\psi}\right\rangle \otimes \left|\mathsf{aux}\right\rangle,$$

if $|\langle\psi|A_x^{(j)}\otimes B_y^{(k)}|\psi\rangle - \langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle| < \delta_2$. Take $\delta = \min\{\delta_1,\delta_2\}$ and $\varepsilon = \max\{\varepsilon_1,\varepsilon_2\}$ one get that the extended strategy $\tilde{S}^{Extend} = (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}, \{\tilde{B}_y^{(k)}, \tilde{O}^{(l)}\})$ is robust self-tested. □

We visualize the extension of the correlation table to help better understand post-hoc self-testing. For simplicity, consider binary observables $\tilde{A}_x, \tilde{B}_y, \tilde{O}$. The correlation generated by $\tilde{S}$ can be written as a $(|\mathcal{I}_A|+1)\times(|\mathcal{I}_B|+1)$ table as in Table 1. Then we say that Table 1 self-tests strategy $\tilde{S}$. Take $\tilde{S}$ as the initial strategy, then add an additional binary observable $\tilde{O}$ on Bob's side; this will extend the correlation table as in Table 2. Intuitively, given self-tested $\{\tilde{A}_x\}$, then for some $\tilde{O}$ it could be the case that $\tilde{O}$ is fully characterized by $\langle I\otimes\tilde{O}\rangle$ and $\{\langle\tilde{A}_x\otimes\tilde{O}\rangle\}_x$. If so, we say that $\tilde{O}$ is post-hoc self-tested based on $\{\tilde{A}_x\}$ and $|\tilde{\psi}\rangle$. Then the extended Table 2 self-tests $\tilde{S}^{Extend}$, because essentially the white part of Table 2 tests $\tilde{S}$, and the yellow part tests $\tilde{O}$.

	I	$\tilde{B}_0$	...	$\tilde{B}_{Y-1}$
I	-	$\langle I,\tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle I,\tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$
$\tilde{A}_0$	$\langle\tilde{A}_0,I\rangle_{\tilde{\psi}}$	$\langle\tilde{A}_0,\tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle\tilde{A}_0,\tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$
...	...	...	...	...
$\tilde{A}_{X-1}$	$\langle\tilde{A}_{X-1},I\rangle_{\tilde{\psi}}$	$\langle\tilde{A}_{X-1},\tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle\tilde{A}_{X-1},\tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$

Table 1: Initiate correlation table. Here $\langle\tilde{A},\tilde{B}\rangle_{\tilde{\psi}}$ is in short for $\langle\tilde{\psi}|\tilde{A}\otimes\tilde{B}|\tilde{\psi}\rangle$, and we take $X=|\mathcal{I}_A|$, $Y=|\mathcal{I}_B|$.

	I	$\tilde{B}_0$	...	$\tilde{B}_{Y-1}$	$\tilde{O}$
I	-	$\langle I,\tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle I,\tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle I,\tilde{O}\rangle_{\tilde{\psi}}$
$\tilde{A}_0$	$\langle\tilde{A}_0,I\rangle_{\tilde{\psi}}$	$\langle\tilde{A}_0,\tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle\tilde{A}_0,\tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle\tilde{A}_0,\tilde{O}\rangle_{\tilde{\psi}}$
...	...	...	...	...	...
$\tilde{A}_{X-1}$	$\langle\tilde{A}_{X-1},I\rangle_{\tilde{\psi}}$	$\langle\tilde{A}_{X-1},\tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle\tilde{A}_{X-1},\tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle\tilde{A}_{X-1},\tilde{O}\rangle_{\tilde{\psi}}$

Table 2: Extended correlation table.

From hereon we shall call $\tilde{S}, |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}$ the initial strategy, initial state, and initial generalized observables, respectively, and call $\tilde{O}^{(l)}$ the additional generalized observables.

5.3.2 Robust post-hoc self-testing criterion for projective strategies

Given the set of initial generalized observables $\{\tilde{A}_x\}$ together with the initial state $|\tilde{\psi}\rangle$, what kind of generalized observable $\tilde{O}$ is post-hoc self-tested based on $(|\tilde{\psi}\rangle, \tilde{A}_x)$? Intuitively, if $\{\langle\tilde{\psi}|(\tilde{A}_x^{(j)}\otimes\tilde{O}^{(\ell)})|\tilde{\psi}\rangle\}_x$ can fully characterize $\{\tilde{O}^{(\ell)}\}$ for all ℓ then Bob also has no choice but

to honestly perform a local dilation of $\tilde{O}^{(\ell)}$ on $|\tilde{\psi}\rangle$. This then gives a criterion of post-hoc self-testing. In proving this criterion, a version of the folklore fact 'any vector is uniquely determined by its inner products with basis vectors' is useful. Explicitly,

Lemma 5.3. *Let $\tilde{v}_0, \ldots, \tilde{v}_{n-1}$ be linearly independent vectors in a Hilbert space. Let $v_0, \ldots, v_{n-1}$ be nearby vectors (in the norm induced by the inner product $\|a\| = \sqrt{\langle a, a\rangle}$),*

$$\forall x \in [0, n-1], \|v_x - \tilde{v}_x\| < \varepsilon.$$

For any vector pair v and $\tilde{v}$ such that $\langle v, v\rangle \leq \langle \tilde{v}, \tilde{v}\rangle$ and $\tilde{v} \in \mathsf{span}_{\mathbb{C}}\{v_0, \ldots, v_{n-1}\}$, if

$$\forall x \in [0, n-1], |\langle v_x, v\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| < \delta$$

then

$$\|v - \tilde{v}\| \leq \left(\frac{4n}{\lambda_{\mathsf{min}}(G)}\right)^{\frac{1}{4}} (\varepsilon\|\tilde{v}\| + \delta)^{\frac{1}{2}} \|\tilde{v}\|^{\frac{1}{2}},$$

where G is the Gram matrix of $\tilde{v}_0, \ldots, \tilde{v}_{n-1}$ with entries $g_{jk} = \langle \tilde{v}_j, \tilde{v}_k\rangle$, and $\lambda_{\mathsf{min}}(G)$ is the minimal eigenvalue of G.

Proof. Since $\tilde{v} \in \mathsf{span}_{\mathbb{C}}\{\tilde{v}_0, \ldots, \tilde{v}_{n-1}\}$, let $\tilde{v} = \sum_x \alpha_x \tilde{v}_x = W\alpha$, where

$$W = \begin{pmatrix} | & & | \\ \tilde{v}_0 & \cdots & \tilde{v}_{n-1} \\ | & & | \end{pmatrix},$$

then

$$\begin{aligned}
\|v-\tilde{v}\|^2 =& \|v\|^2+\|\tilde{v}\|^2-2\,\mathsf{Re}\,\langle v,\tilde{v}\rangle\\
=& \|v\|^2+\|\tilde{v}\|^2-2\|\tilde{v}\|^2-2\,\mathsf{Re}\,\langle v-\tilde{v},\tilde{v}\rangle\\
\leq& -2\,\mathsf{Re}\,\langle v-\tilde{v},\tilde{v}\rangle\\
\leq& 2|\,\langle v-\tilde{v},\tilde{v}\rangle\,|\\
=& 2|\sum_{x=0}^{n-1}\alpha_x\,\langle v-\tilde{v},\tilde{v}_x\rangle\,|\\
\leq& 2\sum_{x=0}^{n-1}|\alpha_x|\cdot|\,\langle v,\tilde{v}_x\rangle-\langle\tilde{v},\tilde{v}_x\rangle\,|\\
=& 2\sum_{x=0}^{n-1}|\alpha_x|\cdot|\,\langle v,\tilde{v}_x\rangle-\langle v,v_x\rangle+\langle v,v_x\rangle-\langle\tilde{v},\tilde{v}_x\rangle\,|\\
\leq& 2\sum_{x=0}^{n-1}|\alpha_x|\cdot(\varepsilon\|v\|+\delta)\\
\leq& 2\|\alpha\|_1(\varepsilon\|\tilde{v}\|+\delta),
\end{aligned}$$

where $\|\cdot\|_1$ is the vector 1-norm. Using the vector norm inequality we have

$$\begin{aligned}
\|\alpha\|_1 \leq& \sqrt{n}\|\alpha\|\\
=& \sqrt{n}\|(W^*W)^{-1}W^*W\alpha\|\\
\leq& \sqrt{n}\|(W^*W)^{-1}W^*\|_\infty\|W\alpha\|,
\end{aligned}$$

where $\|\cdot\|_\infty$ is the spectral norm of operators (Schatten ∞-norm).

Note that W admits a singular value decomposition $W=V\Sigma U^*$, where V is isometry, U is unitary, and $\Sigma=\mathsf{diag}(\sigma_0,\ldots,\sigma_{n-1})$ is positive definite. Then $G=W^*W=U\Sigma^2U^*$. Therefore

$$\|(W^*W)^{-1}W^*\|_\infty=\|(U\Sigma^2U^*)^{-1}U\Sigma V^*\|_\infty=\|U\Sigma^{-1}V^*\|_\infty=\sigma_{\mathsf{max}}(U\Sigma^{-1}V^*)=\frac{1}{\sqrt{\lambda_{\mathsf{min}}(G)}}.$$

Finally,

$$\begin{aligned}\|v-\tilde{v}\|^2 \leq & 2\|\alpha\|_1(\varepsilon\|\tilde{v}\|+\delta)\\ \leq & 2\sqrt{n}\|(W^*W)^{-1}W^*\|_\infty\|W\alpha\|(\varepsilon\|\tilde{v}\|+\delta)\\ = & \frac{2\sqrt{n}}{\sqrt{\lambda_{\min}(G)}}(\varepsilon\|\tilde{v}\|+\delta)\|\tilde{v}\|\\ \implies \quad \|v-\tilde{v}\| \leq & \left(\frac{4n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}}(\varepsilon\|\tilde{v}\|+\delta)^{\frac{1}{2}}\|\tilde{v}\|^{\frac{1}{2}}.\end{aligned}$$

□

The analogue of Lemma 5.3 for unitary operators is crucial in the following proposition. From hereon we assume that the reference strategy is given in a Schmidt basis for its state.

Proposition 5.4. *Let $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} \in \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$ be a state, and $\{\tilde{A}_x\}$, $x \in [0, n-1]$ be unitaries in $B(H_{\tilde{A}})$. Suppose $\tilde{O} \in B(H_{\tilde{B}})$ is a unitary such that*

$$\bar{\tilde{O}}P \in \mathsf{span}_{\mathbb{C}}\{D\tilde{A}_x D\}$$

where P is positive definite and $D = \mathsf{vec}^{-1}(|\tilde{\psi}\rangle) = \mathsf{diag}(\lambda_0, ..., \lambda_{d-1})$, where λ_j are Schmidt coefficients of $|\tilde{\psi}\rangle$.

If states $|\psi\rangle_{ABP} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P, |\mathsf{aux}\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_P$, contractions $\{A_x\}$ in $B(\mathcal{H}_A)$, a contraction $O \in B(\mathcal{H}_B)$, and a local isometry $U = U_A \otimes U_B : \mathcal{H}_A \otimes \mathcal{H}_B \to (\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{B'})$ satisfy

$$\begin{aligned}&\forall x,\ (U \otimes \mathsf{Id}_P)(A_x \otimes \mathsf{Id}_B \otimes \mathsf{Id}_P)\,|\psi\rangle_{ABP} \approx_\varepsilon (\tilde{A}_x \otimes \mathsf{Id}_{\tilde{B}})\,|\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle\,,\\ &(U \otimes \mathsf{Id}_P)\,|\psi\rangle_{ABP} \approx_\varepsilon |\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle\,,\\ &|\,\langle\psi|A_x \otimes O|\psi\rangle - \langle\tilde{\psi}|\tilde{A}_x \otimes \tilde{O}|\tilde{\psi}\rangle\,| < \delta,\end{aligned}$$

then $(U \otimes \mathsf{Id}_P)(\mathsf{Id}_A \otimes O_y^{(l)} \otimes \mathsf{Id}_P)\,|\psi\rangle_{ABP} \approx_{\varepsilon'} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{O}_y^{(l)})\,|\tilde{\psi}\rangle \otimes |\mathsf{aux}\rangle$, where

$$\varepsilon' = \left(\frac{n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}}\left(2\frac{\mathsf{Tr}\,Q}{\lambda_{\min}(Q)}\kappa(D)\right)^{\frac{1}{2}}\left(\left(2\left(\frac{\mathsf{Tr}\,Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}}\lambda_{\max}(D)+1\right)\varepsilon+\delta\right)^{\frac{1}{2}}+\varepsilon. \quad (23)$$

Here $Q = D^{-1}PD^{-1}$, G is the Gram matrix of $\{\tilde{A}_x\}$ with etries $g_{jk} = \mathsf{Tr}[\tilde{A}_j^*\tilde{A}_k]$, and $\kappa(D)$ is the condition number of D, i.e., the ratio of the maximal and the minimal Schmidt coefficient of $|\tilde{\psi}\rangle$.

Proof. Define

$$\begin{aligned}
\tilde{v}_x &:= D' \otimes \sqrt{P}^{-1} D \tilde{A}_x^* D, \\
v_x &:= (I \otimes \sqrt{P^{-1}} D)(U_A A_x^* U_A^*)(D' \otimes D), \\
\tilde{v} &:= (D' \otimes \sqrt{P})(I_{B'} \otimes \tilde{O}^\intercal) = D' \otimes \sqrt{P}\tilde{O}^\intercal, \\
v &:= (D' \otimes \sqrt{P})(U_B O U_B^*)^\intercal.
\end{aligned}$$

where $D' = \mathsf{vec}^{-1}(|\mathsf{aux}\rangle)$. We also consider $|\mathsf{aux}\rangle$ given in its Schmidt basis, so D' is diagonal (while not necessarily full-ranked). Note that $\mathsf{Tr}[D'^2] = \mathsf{Tr}[\rho_A] = 1$. The entries of the Gram matrix G' for $\{\tilde{v}_x\}$ are $g'_{jk} = \mathsf{Tr}[\tilde{v}_j^* \tilde{v}_k] = \mathsf{Tr}[(D^{-1}PD^{-1})^{-1}\tilde{A}_k^* D^2 \tilde{A}_j] = \mathsf{Tr}[(Q)^{-1}\tilde{A}_k^* D^2 \tilde{A}_j]$. Comparing the minimal eigenvalues of G and G', we have that

$$\lambda_{\mathsf{min}}(G') \geq \lambda_{\mathsf{min}}(G)\lambda_{\mathsf{min}}(D^2)\lambda_{\mathsf{min}}(Q^{-1}) = \frac{\lambda_{\mathsf{min}}(G)\lambda_{\mathsf{min}}^2(D)}{\lambda_{\mathsf{max}}(Q)} > \frac{\lambda_{\mathsf{min}}(G)\lambda_{\mathsf{min}}^2(D)}{\mathsf{Tr}\, Q}.$$

To apply Lemma 5.3, one check the conditions:

- $\tilde{v} \in \mathsf{span}_{\mathbb{C}}\{\tilde{v}_x\}$:

$$\begin{aligned}
& \bar{\tilde{O}} P \in \mathsf{span}_{\mathbb{C}}\{D\tilde{A}_x D\} \\
\Rightarrow\ & P(\tilde{O})^\intercal \in \mathsf{span}_{\mathbb{C}}\{D\tilde{A}_x^* D\} \\
\Rightarrow\ & D' \otimes \sqrt{P}(\tilde{O})^\intercal \in \mathsf{span}_{\mathbb{C}}\{D' \otimes \sqrt{P}^{-1} D\tilde{A}_x^* D\} \\
\Rightarrow\ & \tilde{v} \in \mathsf{span}_{\mathbb{C}}\{\tilde{v}_x\}.
\end{aligned}$$

- $\|v\| \leq \|\tilde{v}\|$:

$$\begin{aligned}
\|\tilde{v}\| =& \sqrt{\mathsf{Tr}[D'^2 \otimes \sqrt{P}(\tilde{O})^\intercal((\tilde{O})^\intercal)^* \sqrt{P}]} = \sqrt{\mathsf{Tr}[P]}, \\
\|v\| =& \sqrt{\mathsf{Tr}[(U_B O U_B^*)^\intercal (D' \otimes \sqrt{P})(D' \otimes \sqrt{P})((U_B O U_B^*)^\intercal)^*]} \\
=& \sqrt{\mathsf{Tr}[(U_B O U_B^*)^* (D'^2 \otimes \overline{P})(U_B O U_B^*)]} \\
=& \sqrt{\mathsf{Tr}[(D'^2 \otimes \overline{P}) U_B O U_B^* U_B (O)^* U_B^*]} \\
\leq& \sqrt{\mathsf{Tr}[(D'^2 \otimes \overline{P}) U_B U_B^*]} \\
\leq& \sqrt{\mathsf{Tr}[(D'^2 \otimes \overline{P})]} \\
=& \sqrt{\mathsf{Tr}[P]} = \|\tilde{v}\|,
\end{aligned}$$

where the first inequality comes from O being a contraction, and the second inequality comes from $U_B U_B^* \leq I_{\tilde{B}B'}$ and $D'^2 \otimes \overline{P} \geq 0$.

- for all x, v_x and $\tilde{v}_x$ are close:

$$\begin{aligned}
\|v_x - \tilde{v}_x\| \leq & \|(U_A A_x^* U_A^*)(D' \otimes D) - D' \otimes \tilde{A}_x^* D\| \|\sqrt{P^{-1}} D\|_\infty \\
= & \|(D' \otimes D)(U_A A_x^* U_A^*) - D' \otimes D\tilde{A}_x^*\| \|\sqrt{P^{-1}} D\|_\infty \\
= & \|(U_A A_x U_A^*)(D' \otimes D) - D' \otimes \tilde{A}_x D\| \|\sqrt{P^{-1}} D\|_\infty \\
= & \|(U_A A_x U_A^* \otimes I)(|\mathsf{aux}\rangle \otimes |\tilde{\psi}\rangle) - |\mathsf{aux}\rangle \otimes (\tilde{A}_x \otimes I\, |\tilde{\psi}\rangle)\| \|\sqrt{P^{-1}} D\|_\infty \\
\leq & (\|(U_A A_x U_A^* \otimes I) U[|\psi\rangle] - |\mathsf{aux}\rangle \otimes (\tilde{A}_x \otimes I\, |\tilde{\psi}\rangle)\| + \varepsilon) \|\sqrt{P^{-1}} D\|_\infty \\
= & (\|U[A_x \otimes I\, |\psi\rangle] - |\mathsf{aux}\rangle \otimes (\tilde{A}_x \otimes I\, |\tilde{\psi}\rangle)\| + \varepsilon) \|\sqrt{P^{-1}} D\|_\infty \\
= & \frac{2\varepsilon}{\lambda_{\mathsf{min}}(D^{-1} P D^{-1})^{\frac{1}{2}}} = \frac{2\varepsilon}{\lambda_{\mathsf{min}}(Q)^{\frac{1}{2}}}.
\end{aligned}$$

- the inner products are close:

$$\begin{aligned}
& |\, \langle v_x, v \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| \\
= & |\, \langle (I \otimes \sqrt{P^{-1}} D)(U_A A_x^* U_A^*)(D' \otimes D), (D' \otimes \sqrt{P})(U_B O U_B^*) \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| \\
= & |\, \langle D' \otimes D, (U_A A_x U_A^*)(I \otimes D\sqrt{P^{-1}})(D' \otimes \sqrt{P})(U_B O U_B^*) \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| \\
= & |\, \langle D' \otimes D, (U_A A_x U_A^*)(D' \otimes D)(U_B O U_B^*) \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| \\
= & |\, \langle |\mathsf{aux}\rangle \otimes |\tilde{\psi}\rangle \,, (U_A A_x U_A^* \otimes U_B O U_B^*)(|\mathsf{aux}\rangle \otimes |\tilde{\psi}\rangle) \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| \\
\leq & |\, \langle U[|\psi\rangle], (U_A A_x U_A^* \otimes U_B O U_B^*) U[|\psi\rangle] \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| + 2\varepsilon \\
= & |\, \langle |\psi\rangle \,, A_x \otimes O\, |\psi\rangle \rangle - \langle \tilde{v}_x, \tilde{v} \rangle \,| + 2\varepsilon \\
= & |\, \langle \psi | A_x \otimes O | \psi \rangle - \langle \tilde{\psi} | \tilde{A}_x \otimes \tilde{O} | \tilde{\psi} \rangle \,| + \varepsilon < \delta + 2\varepsilon.
\end{aligned}$$

So all the conditions of Lemma 5.3 hold. By Lemma 5.3, we have

$$\begin{aligned}
\|v-\tilde{v}\| &\leq \left(\frac{4n}{\lambda_{\min}(G')}\right)^{\frac{1}{4}}\left(\frac{2}{\lambda_{\min}(Q)^{\frac{1}{2}}}\varepsilon(\operatorname{Tr}P)^{\frac{1}{2}}+\delta+2\varepsilon\right)^{\frac{1}{2}}(\operatorname{Tr}P)^{\frac{1}{4}} \\
&= \left(\frac{4n\operatorname{Tr}(P)\operatorname{Tr}(Q)}{\lambda_{\min}(G)\lambda_{\min}(D)^2}\right)^{\frac{1}{4}}\left(\left(2\left(\frac{\operatorname{Tr}P}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}}+2\right)\varepsilon+\delta\right)^{\frac{1}{2}} \\
&= \left(\frac{4n(\operatorname{Tr}Q)^2\lambda_{\max}(D)^2}{\lambda_{\min}(G)\lambda_{\min}(D)^2}\right)^{\frac{1}{4}}\left(\left(2\left(\frac{\operatorname{Tr}Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}}\lambda_{\max}(D)+2\right)\varepsilon+\delta\right)^{\frac{1}{2}} \\
&= \left(\frac{n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}}(2(\operatorname{Tr}Q)\kappa(D))^{\frac{1}{2}}\left(\left(2\left(\frac{\operatorname{Tr}Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}}\lambda_{\max}(D)+2\right)\varepsilon+\delta\right)^{\frac{1}{2}},
\end{aligned}$$

which implies

$$\begin{aligned}
&\|U[I\otimes O|\psi\rangle]-|\mathsf{aux}\rangle\otimes(I_{\tilde{A}}\otimes\tilde{O}|\tilde{\psi}\rangle)\| \\
\leq&\|I_{\tilde{A}A'}\otimes U_BOU_B^*(|\mathsf{aux}\rangle\otimes|\tilde{\psi}\rangle)-|\mathsf{aux}\rangle\otimes(I_{\tilde{A}}\otimes\tilde{O}|\tilde{\psi}\rangle)\|+\varepsilon \\
=&\|(D'\otimes D)(U_BOU_B^*)^{\intercal}-(D'\otimes D)(I_{B'}\otimes\tilde{O}^{\intercal})\|+\varepsilon \\
\leq&\|v-\tilde{v}\|\|\sqrt{P^{-1}}D\|_\infty+\varepsilon \\
\leq&\left(\frac{n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}}\left(2\frac{\operatorname{Tr}Q}{\lambda_{\min}(Q)}\kappa(D)\right)^{\frac{1}{2}}\left(\left(2\left(\frac{\operatorname{Tr}Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}}\lambda_{\max}(D)+2\right)\varepsilon+\delta\right)^{\frac{1}{2}}+\varepsilon.
\end{aligned}$$

□

A few remarks of Proposition 5.4:

1. If we fix $P=I$, then the criterion of Proposition 5.4 reduces to $\tilde{\bar{O}}\in\mathsf{span}\{D\tilde{A}_xD\}$, which is foreseeable from the fact that $\langle\tilde{\psi}|\tilde{A}_x\otimes\tilde{O}|\tilde{\psi}\rangle=\mathsf{Tr}[D\tilde{A}_xD\tilde{O}^{\intercal}]=\langle D\tilde{A}_x^*D,\tilde{O}^{\intercal}\rangle$. Our result however, allows for more general $\tilde{O}$ than just the linear combinations of $\{D\tilde{A}_xD\}$.

2. For small ε,δ we have $\varepsilon'=O(\sqrt{C\varepsilon+\delta})$. If the initial strategy has explicit $\varepsilon-\delta$ dependence, by Proposition 5.4 the extended strategy will also have explicit robustness.

3. In the mirror case where we have additional unitary $\tilde{O}$ on Alice's side and Bob's

unitaries are $\tilde{B}_y$, the criterion is similar:

$$\bar{\tilde{O}} P_j \in \mathsf{span}_{\mathbb{C}}\{D\tilde{B}_y D\}.$$

4. In Eq. (23), $\kappa(D)$ and $\lambda_{\mathsf{max}}(D)$ imply that more entanglement enables more robustness, which is intuitive: imagine that $|\tilde{\psi}\rangle$ is weakly entangled (which leads to a large $\kappa(D)$), then Alice and Bob are so weakly correlated that we cannot control O from $\{A_x^{(j)}\}$.

Now we are ready to provide a sufficient condition for $\tilde{O}$ being post-hoc self-tested based on $(|\tilde{\psi}\rangle, \tilde{A}_x\}$. If the condition in Proposition 5.4 is satisfied for all powers of a generalized observable $\tilde{O}$ as required by the definition of robust self-testing, we immediately have the following criterion:

Theorem 5.5. *An additional L-output projective measurement, characterized by observable $\{\tilde{O}\}$, is robust post-hoc self-tested based on a robust self-tested initial observables $\{\tilde{A}_x\}$ and initial state $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$, if there exist positive definite operators $P_l > 0$ such that*

$$\bar{\tilde{O}}^l P_l \in \mathsf{span}_{\mathbb{C}}\{D\tilde{A}_x^j D : x, j\},$$

for every $l \in [0, L-1]$. Here $D = \mathsf{vec}^{-1}(|\tilde{\psi}\rangle) = \mathsf{diag}(\lambda_1, ..., \lambda_d)$, where λ_j are Schmidt coefficients of $|\tilde{\psi}\rangle$. Moreover, the $(\varepsilon', (\varepsilon, \delta))$ dependence of the robustness will be $\varepsilon' = O(\sqrt{C\varepsilon + \delta})$.

Proof. For every $l \in [0, L-1]$, note that $\tilde{A}_x^j$, $\tilde{O}^l$ are unitaries, $A_x^{(j)}$, $O^{(l)}$ are contractions, so we can apply Proposition 5.4 to get $\varepsilon_l' = O(\sqrt{C\varepsilon + \delta})$ by Eq. (23). Taking $\varepsilon' = \mathsf{max}_l\{\varepsilon_l'\} = O(\sqrt{C\varepsilon + \delta})$ then gives the desired conclusion. □

Given concrete $|\tilde{\psi}\rangle, \{\tilde{A}_x), \tilde{O}$, the condition $\tilde{O}^l P_l \in \mathsf{span}_{\mathbb{C}}\{D\tilde{A}_x^j D\}$ can be determined via a feasibility semidefinite program (SDP). Moreover, since P_l has the freedom in scaling and $Q_l = D^{-1} P_l D^{-1}$ is positive definite, we can without loss of generality take $\lambda_{\mathsf{min}}(Q_l) = 1$, and minimize $\mathsf{Tr}\, Q_l$ by the following SDP to get a better robustness:

$$\begin{aligned} \mathsf{min} \quad & \mathsf{Tr}\, Q_l \\ \text{s. t.} \quad & \bar{\tilde{O}}^l D Q_l D = \sum_{j,x} c_{j,x,l} D\tilde{A}_x^j D, \\ & Q_l \geq I, \\ & c_{j,x,l} \in \mathbb{C} \end{aligned}$$

for every k individually. Also note that Theorem 5.5 does not assume measurements to be real, so it works for observables of complex reference measurements as well.

5.3.3 A closed-form criterion for binary observables

While the condition in Theorem 5.5 can be checked through a semidefinite program, the existential nature of it can make it cumbersome to work with in some applications. In order to address this issue, we present a closed-form variant of Theorem 5.5 for the special case where $\tilde{A}_x$ and $\tilde{O}$ are binary measurements. This particular form not only facilitates the proof of our main theorem, but also proves useful in the context of iterative self-testing.

Let all the measurements in $\tilde{S}$ be binary, i.e., $|\mathcal{O}_A| = |\mathcal{O}_B| = 2$. Since $\tilde{A}_x$ and $\tilde{O}$ are now orthogonal matrices (as the projections are real), the condition from Theorem 5.5 simplifies to

$$\tilde{O}P \in \mathsf{span}_{\mathbb{C}}\{D^2, D\tilde{A}_x D\}.$$

(Note that $\tilde{O}^0 P_0 = P_0$ is always in the span by taking $P_0 = D^2$.) Further, we can restrict ourselves in the real span of $\{D^2, D\tilde{A}_x D\}$: if $\tilde{O}P \in \mathsf{span}_{\mathbb{C}}\{D^2, D\tilde{A}_x D\}$, then $\tilde{O}\,\mathsf{Re}(P) \in \mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$ where $\mathsf{Re}(P)$ is positive definite[4]. Thus it suffices to consider

$$\tilde{O}P \in \mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D), \tag{24}$$

where P is real and positive definite.

Since every operator contained in $\mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$ is real Hermitian (or symmetric), consider the following sgn map that takes real Hermitian matrices to real Hermitian matrices with eigenvalues $0, \pm 1$, defined by

$$\begin{aligned} \mathsf{sgn} &: H(\mathbb{R})_d \to H(\mathbb{R})_d \\ H = \sum_j \lambda_j |v_j\rangle\langle v_j| &\mapsto \mathsf{sgn}(H) = \sum_j \mathsf{sgn}(\lambda_j)|v_j\rangle\langle v_j| \end{aligned}$$

where $(|v_j\rangle\}_j$ is an orthonormal basis of eigenvectors for H. That is, sgn is the extension of the sign function via functional calculus. Then we show that the criterion Eq. (24) is equivalent to that $\tilde{O}$ is in the image of $\mathsf{span}\{D^2, D\tilde{A}_x D\}$ via sgn:

Lemma 5.6. *Given d-dimensional orthogonal matrices $\tilde{O}$ and $\{\tilde{A}_x\}$, and $D = \mathsf{diag}(\{\lambda_j\})$*

[4] $\mathsf{Re}(P) = \frac{1}{2}(P + \bar{P})$, where P and $\bar{P}$ are both positive definite.

where $\lambda_j > 0$ for $j \in [0, d-1]$. Then there exist a real positive definite P such that

$$\tilde{O}P \in \mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\},$$

if and only if

$$\tilde{O} \in \mathsf{sgn}(\mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}).$$

Proof. The 'if' part: Let $\tilde{O} = \mathsf{sgn}(H)$ where $H \in \mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$. Since $\tilde{O}$ is non-singular, H is also non-singular. Then $\tilde{O}H = \mathsf{sgn}(H)H$ is positive definite. Take $P = \tilde{O}H$ then $\tilde{O}P = H \in \mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$.

The 'only if' part: Let $\tilde{O}P = H \in \mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$, then $H = H^\intercal = (\tilde{O}P)^\intercal = P\tilde{O}$. So $\tilde{O}$, H, and P commute, therefore are simultaneously diagonalizable. Let $\{b_j\}$, $\{p_j\}$, $\{h_j\}$ be the eigenvalues of O, P, H, respectively; then $o_j p_j = h_j \neq 0$. Also note that $o_j = \pm 1$ and $p_j > 0$, so $p_j = |h_j|$ and $o_j = h_j/|h_j| = \mathsf{sgn}(h_j)$. Therefore $\tilde{O} = \mathsf{sgn}(H)$. □

And the equivalent criterion for post-hoc selt-testing binary observables follows immediately:

Proposition 5.7. *An additional binary (2-output) d-dimensional observable $\tilde{O}$ is robust post-hoc self-tested based on robust self-tested initial binary observables $\{\tilde{A}_x\}$ and initial state $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$, if*

$$\tilde{O} \in \mathsf{sgn}(\mathsf{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D : x\}),$$

where $D = \mathsf{vec}^{-1}(|\tilde{\psi}\rangle)$, and sgn *maps real Hermitian matrices to real Hermitian matrices, defined by*

$$\begin{aligned} \mathsf{sgn} : H(\mathbb{R})_d &\to H(\mathbb{R})_d \\ H = \sum_j \lambda_j |v_j\rangle\langle v_j| &\mapsto \mathsf{sgn}(H) = \sum_j \mathsf{sgn}(\lambda_j)|v_j\rangle\langle v_j|. \end{aligned}$$

Moreover, the $\varepsilon' - (\varepsilon, \delta)$ dependence of the robustness will be $\varepsilon' = O(\sqrt{C\varepsilon + \delta})$.

5.4 Iterative self-testing I: self-testing of arbitrary real projective measurements

Now we introduce the technique of iterative self-testing, by which we show how to self-test arbitrary real projective measurements. From now we restrict to reference strategies with binary observables and a maximally entangled initial state $|\tilde{\psi}\rangle = |\Phi_d\rangle = \sum_j |jj\rangle / \sqrt{d}$. In this case, the criterion in Proposition 5.7 reduces to $\tilde{O} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$, because $D = 1/\sqrt{d}\mathsf{Id}$ is proportional to the identity matrix.

Given initial strategy $\tilde{S} = (U_d, \{\tilde{A}_x\}, \{\tilde{B}_y\})$, if we post-hoc self-test $\tilde{O} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$ on Bob's side, then we can use $\{\tilde{B}_y, \tilde{O}\}$ to post-hoc self-test another measurement $\tilde{O}' \in \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{B}_y, \tilde{O}\})$ for Alice. By doing this in several rounds, starting from a small set of observables $\{\tilde{A}_x\}$ we may eventually self-test many additional observables. We call this process iterative self-testing.

We visualize the extension of the correlation table to help better understand iterative self-testing. Let the initial binary observables to be $\{\tilde{A}_x), \{\tilde{B}_y\}$, and the initial state $|\tilde{\psi}\rangle = |\Phi_d\rangle$ is maximally entangled. Then the correlation generated Table 3 self-tests the initial strategy $\tilde{S}$. Recall that the condition from Proposition 5.7 reduces to $\tilde{O} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$. Now consider an additional binary observable $\tilde{O}$ such that
$\tilde{O} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})\}) \setminus \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$. Since $\tilde{O} \notin \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$ we do not know whether it is post-hoc self-tested by correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}^{(k)}|\tilde{\psi}\rangle\}$ based on $\{\tilde{A}_x\}$. Nevertheless, given $\tilde{O} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})\})$ we can do the following: take the fewest binary observables $\tilde{B}_{|\mathcal{I}_B|}, ..., \tilde{B}_{Y'-1} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$ such that $\mathsf{span}\{\mathsf{Id}, \tilde{B}_0, ..., \tilde{B}_{Y'-1}\} = \mathsf{span}\{\mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})\}$. Then the correlation Table 3 will self-test the corresponding strategy, because the white part tests $\tilde{S}$, and the green part tests the additional binary observables $\tilde{B}_{|\mathcal{I}_B|}, ..., \tilde{B}_{Y'-1} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})$. Now, add $\tilde{O}$ as a new row in the Table 4. Because $\tilde{O} \in \mathsf{sgn}(\mathsf{span}\{\mathsf{sgn}(\mathsf{span}\{\mathsf{Id}, \tilde{A}_x\})\})$, the yellow part of correlation the Table 4 (iteratively) post-hoc self-tests $\tilde{O}$. Thus the correlation Table 4 self-tests the extended strategy including $\tilde{O}$. Evidently, via this construction, the size of the correlation table has the trivial upper bound $\frac{d(d+1)}{2} \times \frac{d(d+1)}{2}$ regardless of the number of iterations.

5.4.1 Self-testing arbitrary real observable

In [MPS24], the authors considered a set of projections summing up to a proportion of I, and showed that the strategy consisting of those projections and the maximally entangled state can be self-tested by the correlation it generates. Here we employ one of those strategies

	I	$\tilde{B}_0$	...	$\tilde{B}_{Y-1}$	$\tilde{B}_Y$	...	$\tilde{B}_{Y'-1}$
I	-	$\langle I, \tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle I, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle I, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle I, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$
$\tilde{A}_0$	$\langle \tilde{A}_0, I\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_0, \tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_0, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_0, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_0, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$
...	...	...	...	...	...	...	...
$\tilde{A}_{X-1}$	$\langle \tilde{A}_{X-1}, I\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_{X-1}, \tilde{B}_0\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_{X-1}, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_{X-1}, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_{X-1}, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$

Table 3: Extended correlation table in the first iteration. We take $X = |\mathcal{I}_A|$, $Y = |\mathcal{I}_B|$, and $Y' = |\mathcal{I}'_B|$ for convenience.

	I	$\tilde{B}_1$	...	$\tilde{B}_{Y-1}$	$\tilde{B}_Y$	...	$\tilde{B}_{Y'-1}$
I	-	$\langle I, \tilde{B}_1\rangle_{\tilde{\psi}}$	...	$\langle I, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle I, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle I, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$
$\tilde{A}_1$	$\langle \tilde{A}_1, I\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_1, \tilde{B}_1\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_1, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_1, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_1, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$
...	...	...	...	...	...	...	...
$\tilde{A}_{X-1}$	$\langle \tilde{A}_{X-1}, I\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_{X-1}, \tilde{B}_1\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_{X-1}, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle \tilde{A}_{X-1}, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle \tilde{A}_{X-1}, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$
$\tilde{O}$	$\langle \tilde{O}, I\rangle_{\tilde{\psi}}$	$\langle \tilde{O}, \tilde{B}_1\rangle_{\tilde{\psi}}$	...	$\langle \tilde{O}, \tilde{B}_{Y-1}\rangle_{\tilde{\psi}}$	$\langle \tilde{O}, \tilde{B}_Y\rangle_{\tilde{\psi}}$	...	$\langle \tilde{O}, \tilde{B}_{Y'-1}\rangle_{\tilde{\psi}}$

Table 4: Extended correlation table in the second iteration.

with a specific construction. It turns out that, with the initial strategy we chose, in two iterations we will be able to self-test arbitrary binary projective measurement using the iterative scheme.

Consider $d+1$ unit vectors $v_0, \ldots, v_d \in \mathbb{R}^d$ which form the vertices of a regular $(d+1)$-simplex centered at the origin. Note that

$$v_x^* v_{x'} = -\frac{1}{d} \tag{25}$$

for $x \neq x'$. Define forms $d+1$ binary observables

$$\tilde{T}_x := 2v_x v_x^* - I.$$

The code in Mathematica for generating the observables is provided in Appendix 5.7. According to [MPS24] the following strategy containing $\tilde{T}_x$ and the maximally entangled state is robust self-tested:

Corollary 5.8. *By Theorem 6.10 in [MPS24], the strategy* $\tilde{S}^{(0)} = (|\Phi_d\rangle, \{\tilde{T}_x\}_{x=0}^d, \{\tilde{T}_y\}_{y=0}^d)$ *is robust self-tested by the correlation it generates.*

Now take the strategy $\tilde{S}^{(0)}$ in Corollary 5.8 as the initial strategy, and consider additional binary observables in the form of $\tilde{T}_{jk} := \mathsf{sgn}(\tilde{T}_j + \tilde{T}_k)$ for $j \neq k$. By Proposition 5.7 they are robust post-hoc self-tested. Specifically, we have the following extended strategy that is

robust self-tested:

Lemma 5.9. *Strategy* $\tilde{S}^{(1)} = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d}, \{\tilde{B}_y\}_{y=0}^{\frac{d(d+1)}{2}-1})$ *is robust self-tested, where*

$$
\begin{aligned}
&|\tilde{\psi}\rangle = |\Phi_d\rangle, \\
&\{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d}, \\
&\{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{y=0}^{d},\ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk} : 1 \le j < k \le d\} \setminus \{\tilde{T}_{12}\}.
\end{aligned}
$$

Proof. Since $\tilde{S}^{(0)} = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d}, \{\tilde{B}_y\}_{y=0}^{d})$ is robust self-tested, and $\tilde{T}_{jk} \in \mathsf{sgn}(\mathsf{span}\{\tilde{T}_x\})$, by Propositions 5.7 and 5.2 we immediately have that the strategy $\tilde{S}^{(1)}$ is robust self-tested by the correlation it generates. □

The extended strategy $\tilde{S}^{(1)} = (|\Phi_d\rangle, \{\tilde{A}_x\}_{x=0}^{d}, \{\tilde{B}_y\}_{y=0}^{\frac{d(d+1)}{2}-1})$ introduces $d(d+1)/2 - d - 1$ additional binary observables to Bob that is post-hoc self-tested based on the initial strategy, which are in the form of $\mathsf{sgn}(\tilde{T}_j + \tilde{T}_k)$ (but not every $j \neq k$ is included). It turns out that the additional binary observables together with the $d+1$ initial ones span the space of all $d \times d$ symmetric matrices. To show this, we require the following lemma:

Lemma 5.10. *For* $d > 2$, $\mathsf{span}_{\mathbb{R}}\{\tilde{T}_{jk} : j, k \in [0, d], j \neq k\} = H_d(\mathbb{R})$ *the space of all* d*-dimensional symmetric matrices.*

Proof. Since $\mathsf{dim}\, H_d(\mathbb{R}) = d(d+1)/2 = \#\{\tilde{T}_{jk} : j, k \in [0, d], j \neq k\}$, it suffice to show that $\{\mathsf{sgn}(\tilde{T}_j + \tilde{T}_k) : 0 \le j < k \le d\}$ is linearly independent.

Note that $\tilde{T}_j + \tilde{T}_k = 2(v_j v_j^* + v_k v_k^* - \mathsf{Id})$. Consider the two-dimensional subspace $\mathcal{H}_1 = \mathsf{span}(v_j, v_k)$. Then $(\tilde{T}_j + \tilde{T}_k)|_{\mathcal{H}_1^\perp} = -2\mathsf{Id}$, and

$$
(\tilde{T}_j + \tilde{T}_k)(v_j - v_k) = \frac{2}{d}(v_j - v_k), \quad (\tilde{T}_j + \tilde{T}_k)(v_j + v_k) = -\frac{2}{d}(v_j + v_k),
$$

so $(\tilde{T}_j + \tilde{T}_k)|_{\mathcal{H}_1}$ has eigenvalues $\pm 2/d$, and the (normalised) eigenvector corresponding to $2/d$ is $w_{jk} := \sqrt{\frac{d}{2(d+1)}}(v_j - v_k)$. Hence, $\mathsf{sgn}(\tilde{T}_j + \tilde{T}_k)$ have eigenvalues 1 with multiplicity 1, and -1 with multiplicity $d-1$. Its eigenvector corresponding to 1 is $w_{jk} = \sqrt{\frac{d}{2(d+1)}}(v_j - v_k)$. Therefore $\tilde{T}_{jk} = 2w_{jk}w_{jk}^* - \mathsf{Id}$.

Suppose $\sum_{j<k} c_{jk}\tilde{T}_{jk} = 0$ for some real coefficients c_{jk}. Then

$$
2\frac{d}{2(d+1)} \sum_{j<k} c_{jk}(v_j - v_k)(v_j^* - v_k^*) = \sum_{j<k} c_{jk}\mathsf{Id}. \tag{26}
$$

By Eq. (25) we have

$$(v_j^* - v_k^*)v_l = \begin{cases} 0 & j,k \neq l \\ -\frac{1}{d} - 1 & j \neq k = l \\ 1 + \frac{1}{d} & l = j \neq k \end{cases}$$

Therefore multiplying Eq. (26) by v_ℓ on the left results in

$$\frac{d}{d+1}\left(\sum_{j<l} c_{jl}(-\tfrac{1}{d} - 1)(v_j - v_l) + \sum_{l<k} c_{lk}(1 + \tfrac{1}{d})(v_l - v_k)\right) = \sum_{j<k} c_{jk} v_l$$

and so

$$\begin{aligned} & \left(\sum_{j<l} c_{jl}(v_l - v_j) + \sum_{l<k} c_{lk}(v_l - v_k)\right) = \sum_{j<k} c_{jk} v_l \\ \Rightarrow \quad & \left(\sum_{j<l} c_{jl} + \sum_{l<k} c_{lk} - \sum_{j<k} c_{jk}\right) v_l - \sum_{j<l} c_{jl} v_j - \sum_{l<k} c_{lk} v_k = 0. \end{aligned}$$

Since $\sum_j v_j = 0$, we further have

$$\left(\sum_{j<l} c_{jl} + \sum_{l<j} c_{lj} - \sum_{j<k} c_{jk}\right) \sum_{j \neq l} v_j - \sum_{j<l} c_{jl} v_j - \sum_{l<j} c_{lj} v_j = 0.$$

Since $\{v_j : j \neq l\}$ is linearly independent, we see that c_{jl} for $j < l$ are equal, and c_{lj} for $l > j$ are equal; therefore $c_{jk} =: c$ for all $j < k$. Thus,

$$\begin{aligned} & c\left(d - \frac{d(d+1)}{2}\right) v_l - c \sum_{j \neq l} v_j = 0 \\ \Rightarrow \quad & c\left(\frac{d - d^2}{2} v_l - \sum_{j \neq l} v_j\right) = 0, \end{aligned}$$

which holds only when $c = 0$ or $d = 2$ or $d = -1$. So we conclude that $c_{jk} = 0$ is the only solution for $\sum_{j<k} c_{jk} \tilde{T}_{jk} = 0$ when $d > 2$. □

Let $T = \{\tilde{T}_j : j \in [0,d]\} \cup \{\tilde{T}_{jk} : j,k \in [0,d], j \neq k\}$. By Lemma 5.10 we know that $\mathsf{span}_{\mathbb{R}}(T) = H_d(\mathbb{R})$. Note that $|T| = d + 1 + \frac{d(d+1)}{2} > \mathsf{dim}\, H_d(\mathbb{R})$. The following proposition gives a maximal linearly independent subset in T:

Proposition 5.11. *Define* $T = \{\tilde{T}_j : j \in [0,d]\} \cup \{\tilde{T}_{jk} : j,k \in [0,d], j \neq k\}$. *Let* $T' =$

$T \setminus \{\tilde{O}_{0j} : j \in [1,d]\}$ *and* $T'' = T' \setminus \{\tilde{O}_{12}\}$. *Then* T'' *is a maximal linearly independent subset in* T.

Proof. Note that $|T''| = \frac{d(d+1)}{2} = \dim H_d(\mathbb{R})$. So it suffice to show that $\tilde{T}_{0j} \in \mathsf{span}_{\mathbb{R}}(T')$ and $\tilde{T}_{12} \in \mathsf{span}_{\mathbb{R}}(T'')$. Also note that the identity matrix $\mathsf{Id} = \frac{d}{(d+1)(2-d)} \sum_j \tilde{T}_j$ belongs to $\mathsf{span}_{\mathbb{R}}(T'')$, and so does $v_j v_j^* = (\tilde{T}_j + \mathsf{Id})/2$.

- $\tilde{O}_{0j} \in \mathsf{span}_{\mathbb{R}}(T')$: note that $\sum_j v_j = 0$. Then for every $j > 0$,

$$\begin{aligned}
\tilde{O}_{0j} =& \frac{d}{d+1}(v_0 - v_j)(v_0^* - v_j) - \mathsf{Id} \\
=& \frac{d}{d+1}(-\sum_{k>0} v_k - v_j)(-\sum_{k>0} v_k^* - v_j^*) - \mathsf{Id} \\
=& \frac{d}{d+1}(\sum_{0<k<l} (v_k v_l^* + v_l v_k^*) + \sum_{k>0} (v_k v_j^* + v_j v_k^*) + \tilde{P}_j) - \mathsf{Id} \in \mathsf{span}_{\mathbb{R}}(T')
\end{aligned}$$

  because $v_x v_y^* + v_y v_x^* = \tilde{P}_x + \tilde{P}_y - \frac{d+1}{d}(\tilde{T}_{xy} - \mathsf{Id}) \in \mathsf{span}_{\mathbb{R}}(T')$ for all $x, y > 0$.

- $\tilde{T}_{12} \in \mathsf{span}_{\mathbb{R}}(T'')$: we show that $\sum_{1 \le j < k \le d} \tilde{T}_{jk} + d v_0 v_0^* + \frac{d(d-3)}{2}\mathsf{Id} = 0$, meaning that $\tilde{T}_{12}$ is a linear combination of elements in T''. Since $\mathsf{span}_{\mathbb{R}}\{v_l : l \in [1,d]\} = \mathbb{R}^d$, it suffices to show that $\sum_{1 \le j < k \le d} \tilde{T}_{jk} v_l + d v_0 v_0^* v_l + \frac{d(d-3)}{2} v_l = 0$ for all $l \in [1,d]$:

$$\begin{aligned}
&\sum_{1 \le j < k \le d} \tilde{T}_{jk} v_l + d\tilde{P}_0 v_l + \frac{d(d-3)}{2} v_l \\
=& \sum_{1 \le j < k \le d} \frac{d}{d-1}(v_j - v_k)(v_j^* - v_k^*) v_l - \frac{d(d-1)}{2} v_l - v_0 + \frac{d(d-3)}{2} v_l \\
=& \sum_{j>0, j \ne l} (v_l - v_j) - \frac{d(d-1)}{2} v_l - v_0 + \frac{d(d-3)}{2} v_l \\
=& (d-1) v_l + \sum_{j>0, j \ne l} (-v_j) - \frac{d(d-1)}{2} v_l - v_0 + \frac{d(d-3)}{2} v_l \\
=& (d-1) v_l + v_0 + v_l - \frac{d(d-1)}{2} v_l - v_0 + \frac{d(d-3)}{2} v_l = 0.
\end{aligned}$$

□

Since $T'' = \{\tilde{B}_y\}$ in $\tilde{S}$ spans the space of all symmetric matrices, every d-dimensional binary observable $\tilde{O}_{\mathsf{binary}}$ belongs to $\mathsf{span}\{\tilde{B}_y\}$. Therefore, by adding $\tilde{O}_{\mathsf{binary}}$ into $\{\tilde{A}_x\}$ we construct a strategy that can self-test any binary observable:

Proposition 5.12. *For any d-dimensional real projective binary measurement, given by observable $\tilde{O}_{\text{binary}}$, the strategy $\tilde{S}^{(2)} = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d+1}, \{\tilde{B}_y\}_{x=0}^{\frac{d(d+1)}{2}-1})$ is robust self-tested, where*

$$
\begin{aligned}
&|\tilde{\psi}\rangle = |\Phi_d\rangle, \\
&\{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d},\ \tilde{A}_{d+1} = \tilde{O}_{\text{binary}}, \\
&\{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{y=0}^{d},\ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk} : 1 \le j < k \le d\} \setminus \{\tilde{O}_{12}\}.
\end{aligned}
$$

Proof. Since $\tilde{O}_{\text{binary}} \in H_d(\mathbb{R}) = \mathsf{span}\{\mathsf{Id}, \tilde{B}_y\}$ for any $\tilde{O}_{\text{binary}}$, by Lemma 5.9 and Proposition 5.2 we immediately have that the strategy $\tilde{S}^{(2)}$ is robust self-tested by the correlation it generates. □

Finally, we generalize the self-testing of binary measurements to the self-testing of arbitrary L-output measurements. Intuitively, we can think of an L-output projective measurement as a collection of L binary ones: given an L-output projective measurement $\tilde{O} = \sum_{a=0}^{L-1} e^{i2\pi a/L}\tilde{E}_a$, consider binary observables $\{2\tilde{E}_a - \mathsf{Id}\}_{a=0}^{L-1}$. If we can self-test every binary observable $2\tilde{E}_a - \mathsf{Id}$, then we should be able to also self-test $\tilde{O}$.

Proposition 5.13. *For any L-output observable $\tilde{O} = \sum_{a=0}^{L-1} e^{i2\pi a/L}\tilde{E}_a$, strategy*

$$\tilde{S}_1 = (|\tilde{\psi}\rangle, \{\tilde{A}_x, \tilde{O} : x\}, \{\tilde{B}_y : y\})$$

is robust self-tested if and only if strategy

$$\tilde{S}_2 = (|\tilde{\psi}\rangle, \{\tilde{A}_x, 2\tilde{E}_a - \mathsf{Id} : x, a\}, \{\tilde{B}_y : y\})$$

is robust self-tested.

Proof. We prove the 'if' part, and the reasoning for the 'only if' part is similar.

Suppose $\tilde{S}_2 = (|\tilde{\psi}\rangle, \{\tilde{A}_x, 2\tilde{E}_a - \mathsf{Id} : x, a\}, \{\tilde{B}_y\})$ is robust self-tested. Then for any $\varepsilon > 0$ there exists $\delta > 0$ such that any strategy $\delta/3$-approximately generating correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}, \tilde{B}_y^{(k)}|\tilde{\psi}\rangle, \langle\tilde{\psi}|(2\tilde{E}_a - \mathsf{Id}) \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$ can be locally ε/L-dilated by $\tilde{S}_2$. Let $S_1 = (|\psi\rangle, \{A_x^{(j)}, O^{(l)}\}, \{B_y^{(k)}\})$ be a strategy that $\delta/3$-approximately generates the correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle, \langle\tilde{\psi}|\tilde{O}^l \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$. Construct a strategy $S_2 := (|\psi\rangle, \{A_x, 2E_a - \mathsf{Id}\}, \{B_y\})$

where $E_a := 1/L \sum_{l=0}^{L-1} e^{-i2\pi al/L} O^{(l)}$. Then

$$\begin{aligned} & |\langle\psi|O^{(l)} \otimes B_y^{(k)}|\psi\rangle - \langle\tilde{\psi}|\tilde{O}^l \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle| \leq \delta/3 \\ \Rightarrow \quad & |\langle\psi|(2E_a - \mathsf{Id}) \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle - \langle\tilde{\psi}|(2\tilde{E}_a - \mathsf{Id}) \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle| \leq \delta. \end{aligned}$$

So S_2 δ-approximately generates correlation $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle, \langle\tilde{\psi}|(2\tilde{E}_a - \mathsf{Id}) \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$. By the hypothesis, $\tilde{S}_2$ is a local ε/L-dilation of S_2, and so

$$\begin{aligned} & U((2E_a - \mathsf{Id}_A) \otimes \mathsf{Id}_B)|\psi\rangle_{AB} \approx_{\varepsilon/L} ((2\tilde{E}_a - \mathsf{Id}_{\tilde{A}}) \otimes I_{\tilde{B}})|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}|\mathsf{aux}\rangle \\ \Rightarrow \quad & U(O^{(l)} \otimes \mathsf{Id}_B)|\psi\rangle_{AB} \approx_{\varepsilon} (\tilde{O}^l \otimes I_{\tilde{B}})|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}|\mathsf{aux}\rangle, \end{aligned}$$

and

$$U(\mathsf{Id}_A \otimes B_y^{(k)})|\psi\rangle_{AB} \approx_{\varepsilon/L} (\mathsf{Id}_{\tilde{A}} \otimes \tilde{B}_y^k)|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}|\mathsf{aux}\rangle$$

Therefore $\tilde{S}_1$ is a local ε-dilation of S_1. Thus $\tilde{S}_1$ is robust self-tested. □

So we conclude that any real projective measurements can be self-tested:

Theorem 5.14. *For any d-dimensional L-output observable $\tilde{O}$, the strategy*

$$\tilde{S}^{(3)} = \left(|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d+1}, \{\tilde{B}_y\}_{y=0}^{\frac{d(d+1)}{2}-1}\right)$$

is robust self-tested, where

$$\begin{aligned} & |\tilde{\psi}\rangle = |\Phi_d\rangle, \\ & \{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d}, \ \tilde{A}_{d+1} = \tilde{O}, \\ & \{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{x=0}^{d}, \ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk} : 1 \leq j < k \leq d\} \setminus \{\tilde{T}_{12}\}. \end{aligned}$$

Proof. Statement is true for $L = 2$ by Proposition 5.12. For $L > 2$, let $\tilde{O} = \sum_a e^{i2\pi a/L} \tilde{E}_a$ be

the L-output observable, consider the strategy $\tilde{S}_2 = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d+L}, \{\tilde{B}_y\}_{x=0}^{\frac{d(d+1)}{2}-1})$ where

$$
\begin{aligned}
&|\tilde{\psi}\rangle = |\Phi_d\rangle, \\
&\{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d}, \ \{\tilde{A}_x\}_{x=d+1}^{d+L} = \{2\tilde{E}_a - I : 0 \le a \le L-1\}, \\
&\{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{y=0}^{d}, \ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk} : 1 \le j < k \le d\} \setminus \{\tilde{T}_{12}\},
\end{aligned}
$$

and $\tilde{E}_a = 1/L \sum_{l=0}^{L-1} e^{-i2\pi al/L} \tilde{O}^l$. By a similar argument in the proof of Propisition 5.12, $\tilde{S}_2$ is robust self-tested. Then the strategy $\tilde{S}^{(3)}$ is robust self-tested by by Proposition 5.13. □

5.5 Iterative self-testing II: general theory

In this section we develop the theory of iterative self-testing in general, whenever the initial state $|\tilde{\psi}\rangle = |\Phi_d\rangle = \sum_j |jj\rangle / \sqrt{d}$ is maximally entangled and all reference measurements are binary and projective, i.e., are described by orthogonal matrices.

Given the initial strategy $\tilde{S} = (|\Phi_d\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y\})$, denote $S_0 = \{\mathsf{Id}, \tilde{A}_x\}$ to be the set of initial binary observables, and $V_0 = \mathsf{span}_{\mathbb{R}}(S_0)$ to be the subspace generated by S_0. Denote by $S_1' = \mathsf{sgn}(V_0) \cap GL_d(\mathbb{R})$ the binary observables that by Proposition 5.7 are post-hoc self-tested on Bob's side, and take $S_1 = S_1' \cup \{\tilde{B}_y\}$. Note that $S_0 \subseteq S_1' \subseteq S_1$ because $\mathsf{sgn}(\tilde{A}_x) = \tilde{A}_x$. Let $V_1 = \mathsf{span}_{\mathbb{R}}(S_1)$; then we also have $V_0 \subseteq V_1$. Now consider the post-hoc self-testing of additional binary observables on Alice's side based on S_1; we get the next set of binary observables $S_2 = \mathsf{sgn}(V_1) \cap GL_d(\mathbb{R}) \supseteq S_1$ that is self-tested, and also the next subspace $V_2 = \mathsf{span}_{\mathbb{R}}(S_1) \supseteq V_1$. By iteratively using this technique, we enlarge the set of self-tested binary observables S_j in each step. We remark that, when trying to make a similar argument for a non-maximally entangled $|\tilde{\psi}\rangle$, it is not clear whether $V_j \subseteq V_{j+1}$ still holds.

Since $\{V_j\}_j$ is an increasing sequence of subspaces of the finite-dimensional real Hermitian matrix space $H_d(\mathbb{R})$, it eventually stabilizes at $V_\infty = \mathsf{lim}_{j\to\infty} V_j$. It is natural to ask, given initial binary observables $\{\tilde{A}_x\}, \{\tilde{B}_y\}$, what is V_∞? Before we answer this question, we make the following observation:

Lemma 5.15. *Given a set of orthogonal matrices $\{\tilde{A}_x\}$, recursively define $V_0 = \mathsf{span}_{\mathbb{R}}\{\mathsf{Id}, \tilde{A}_x\}$ and $V_j = \mathsf{span}_{\mathbb{R}}(\mathsf{sgn}(V_{j-1}))$[5], where sgn is defined as in Proposition 5.7. If $x \in V_j$, then $p(x) \in V_{j+1}$ for any real coefficient polynomial $p \in \mathbb{R}[t]$. Consequently, $x, y \in V_j$ implies $xy + yx \in V_{j+1}$.*

[5]Here we do not exclude the non-singular matrices in S_j. In fact, $\mathsf{span}(\mathsf{sgn}(V_j)) = \mathsf{span}(\mathsf{sgn}(V_j) \cap GL_d(\mathbb{R}))$: for any singular $s = \mathsf{sgn}(x)$ where $x \in V_j$, $\mathsf{sgn}(x \pm \delta\mathsf{Id}) \in \mathsf{sgn}(V_j)$. And for small enough δ, we have $\mathsf{sgn}(x \pm \delta\mathsf{Id}) \in GL_d(\mathbb{R})$ and $2s = \mathsf{sgn}(x + \delta\mathsf{Id}) + \mathsf{sgn}(x - \delta\mathsf{Id})$.

Proof. For any $x \in V_j$, let $x = U\Lambda U^*$ where Λ has diagonal entries $\lambda_1, \ldots, \lambda_d \in \mathbb{R}$ sorted decreasingly. Then $p(x)$ has eigenvalues $p(\lambda_1), \ldots, p(\lambda_d)$. Note that the identity matrix I is in V_1. Now, for each $i \in [1, d-1]$ such that $\lambda_i \neq \lambda_{i+1}$, choose $r_i \in (\lambda_i, \lambda_{i+1})$, and consider

$$x_i := \mathsf{sgn}(x - r_i I) = U\,\mathsf{diag}(\underbrace{1, \ldots, 1}_{i\ 1s}, \underbrace{-1, \ldots, -1}_{(d-i)\ -1s})U^*.$$

So $x_i \in \mathsf{sgn}(V_j) \subseteq V_{j+1}$. Since $\{x_i\}$ forms a basis of $\{p(x) \colon p \in \mathbb{R}[t]\}$, we have that $p(x) \in V_{j+1}$ for every $p \in \mathbb{R}[t]$.

Take $p(t) = t^2$, and notice that

$$xy + yx = \underbrace{(x+y)^2}_{\in V_{j+1}} - \underbrace{x^2}_{\in V_{j+1}} - \underbrace{y^2}_{\in V_{j+1}} \in V_{j+1}.$$

□

Lemma 5.15 allows one to characterize[6] V_∞ in terms of Jordan algebras [Jac68]. A vector subspace of an associative algebra is a (unital) Jordan algebra if it contains the identity and is closed under the Jordan product $a \star b = \frac{1}{2}(ab + ba)$.

Proposition 5.16. *Given a set of Hermitian orthogonal matrices $\{\tilde{A}_x\}$, define $V_0 = \mathsf{span}_{\mathbb{R}}\{\mathsf{Id}, \tilde{A}_x\}$, $V_j = \mathsf{span}_{\mathbb{R}}(\mathsf{sgn}(V_{j-1}))$, where* sgn *is defined as in Proposition 5.7. Then $V_\infty = \mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$, the real Jordan algebra generated by $\{\tilde{A}_x\}$.*

Proof. $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) = \mathsf{JA}_{\mathbb{R}}(\{\mathsf{Id}, \tilde{A}_x\})$ because $I = \tilde{A}_x^2$. From Lemma 5.15 we know that $x, y \in V_\infty$ implies $x \star y \in V_\infty$. So V_∞ is a Jordan algebra, and hence $\mathsf{JA}_{\mathbb{R}}(\{\mathsf{Id}, \tilde{A}_x\}) \subseteq V_\infty$.

On the other hand, for any $x \in H_d(\mathbb{R})$ the matrix $\mathsf{sgn}(x)$ is a polynomial in x, and therefore lies in $\mathsf{JA}_{\mathbb{R}}(\{x\})$. This implies $V_\infty \subseteq \mathsf{JA}_{\mathbb{R}}(\{\mathsf{Id}, \tilde{A}_x\})$. So we conclude that $V_\infty = \mathsf{JA}_{\mathbb{R}}(\{\mathsf{Id}, \tilde{A}_x\}) = \mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$. □

Proposition 5.16 implies that, after sufficiently many steps, every binary observable $\tilde{O} \in \mathsf{JA}_{\mathbb{R}}(\{\mathsf{Id}, \tilde{A}_x\})$ can be iteratively post-hoc self-tested based on the binary strategy $\tilde{S} = (|\Phi_d\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y\})$. We also provide two properties of real Jordan algebras that help analysing $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$. The first one is that $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\})$, the real associative algebra generated by $\{\tilde{A}_x\}$, is $\mathsf{M}_d(\mathbb{R})$ (the real algebra of $d \times d$ real matrices), if and only if $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$,

[6] Here we omit $\{\tilde{B}_y\}$ for simplicity. This simplification only strengthens our result because we now do not ask $\{\tilde{B}_y\}$ to contribute.

the real Jordan algebra generated by $\{\tilde{A}_x\}$, is $H_d(\mathbb{R})$ (the real Jordan algebra of symmetric $d \times d$ matrices).

Lemma 5.17. *For symmetric $d \times d$ matrices $\{\tilde{A}_x\}$, $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\}) = \mathsf{M}_d(\mathbb{R})$ if and only if $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) = H_d(\mathbb{R})$.*

Proof. The 'if' part: it is straightforward to see that every real matrix is a linear combination of products of symmetric matrices.

The 'only if' part: note that $\mathsf{M}_d(\mathbb{R})$ is a simple algebra, and that a Jordan subalgebra of $H_d(\mathbb{R})$ is semisimple. Suppose $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\}) = \mathsf{M}_d(\mathbb{R})$. Then we claim that $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$ is also simple. Indeed; if $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$ were isomorphic to a non-trivial product of simple ones, then $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\})$ would likewise be isomorphic to a non-trivial product of simple algebras, which is a contradiction. By the Jordan–von Neumann–Wigner Theorem [JvNW34], finite-dimensional simple Jordan algebras are isomorphic to one of the following five types:

- The Jordan algebra of $n \times n$ Hermitian real matrices $H_n(\mathbb{R})$,
- The Jordan algebra of $n \times n$ Hermitian complex matrices $H_n(\mathbb{C})$,
- The Jordan algebra of $n \times n$ Hermitian quaternionic matrices $H_n(\mathbb{H})$,
- The 'spin factor' $\mathbb{R}^n \oplus \mathbb{R}$ with the product $(x, \alpha) \star (y, \beta) = (\beta x + \alpha y, \alpha\beta + \langle x, y \rangle)$,
- The Jordan algebra of 3×3 Hermitian octonionic matrices.

Since $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$ is special, we only need to exam the first four cases individually:

- $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) \cong H_n(\mathbb{R})$ for some n. By the 'if' part of the proof, $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\}) \cong M_n(\mathbb{R})$. But $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\}) = \mathsf{M}_d(\mathbb{R})$, so we are only left with the possibility $n = d$.
- $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) \cong H_n(\mathbb{C})$ for some $n \geq 2$. On one hand, complex Hermitian $n \times n$ matrices do not embed into real matrices of size smaller than $2n$, so $2n \leq d$. On the other hand, $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) \cong H_n(\mathbb{C})$ implies that $\mathsf{M}_d(\mathbb{R}) = \mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\})$ is a real subalgebra of $M_n(\mathbb{C})$, so $d^2 \leq 2n^2$, a contradiction.
- $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) \cong H_n(\mathbb{H})$ for some $n \geq 2$. On one hand, quaternion Hermitian $n \times n$ matrices do not embed into real matrices of size smaller than $4n$, so $4n \leq d$. On the other hand, $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) \cong H_n(\mathbb{H})$ implies that $\mathsf{M}_d(\mathbb{R}) = \mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\})$ is a real subalgebra of $M_n(\mathbb{H})$, so $d^2 \leq 4n^2$, a contradiction.

- $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$ is a spin factor $\mathbb{R}^n \oplus \mathbb{R}$ for some $n \geq 3$. It is known that it can be embedded in the Hermitian real matrices of size $2^n \times 2^n$, but not smaller [McC04]; therefore $2^n \leq d$. On the other hand, the spin factor generates a real Clifford algebra of dimension 2^n [Jac68], so $2^n \geq d^2$, a contradiction.

So, we conclude that $\mathsf{Alg}_{\mathbb{R}}(\{\tilde{A}_x\}) = \mathsf{M}_d(\mathbb{R})$ if and only if $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) = H_d(\mathbb{R})$. □

As a consequence of this lemma, if $|\tilde{\psi}\rangle = |\Phi_d\rangle$, and $\{\tilde{A}_x\}$ generate the real matrix algebra of the corresponding dimension, any binary observable will be in V_∞, thus can be self-tested. In Section 5.4 we showed that a self-tested strategy given by [MPS24] can be used for this purpose. However, several of the self-tested strategies across the existing literature consist of a maximally entangled state and operators that generate the full matrix algebra, so they can be used to self-test arbitrary observables (of suitable size) by Proposition 5.16. Notice that $\{\tilde{A}_x\}_x$ generates $M_n(\mathbb{R})$ as a real associative algebra if and only if the only real solutions of the linear system $[S\tilde{A}_x = \tilde{A}_x S \text{ for all } x]$ are $S = cI$ the scalar multiples of I. Hence given $\{\tilde{A}_x\}$, one can check whether it generates the whole matrix algebra in the following way: suppose we have X binary observables (d-dimensional); then $[S\tilde{A}_x = \tilde{A}_x S \text{ for all } x]$ is a linear system of d^2 variables (which are entries of S) with Xd^2 equations. Thus the condition of Lemma 5.17 is equivalent to checking that the coefficient matrix has rank $d^2 - 1$.

Another property we provide can help in upper-bounding the iteration we need for $V_{itr} = V_\infty$. Let U_j denote the span of all the Jordan products of elements in S_0 of length at most j. Then we have the following relation between U_j and V_j:

Lemma 5.18. *For a set of Hermitian orthogonal matrices $S_0 = \{\mathsf{Id}, \tilde{A}_x\}$, define*

$$U_j := \mathsf{span}_{\mathbb{R}}\{a_1 \star \cdots \star a_k, a_i \in S_0, k \leq j),$$

and define V_j as in Proposition 5.16 for $j \geq 0$. Then $U_{2^{(j)}} \subseteq V_j$.

Proof. By definition, $U_1 = V_0$. Now suppose $U_{2^{(j)}} \subseteq V_j$ for some j. By Proposition 5.15 $x \star y \in V_{j+1}$ for every $x, y \in V_j$, so in particular $x \star y \in V_{j+1}$ for every $x, y \in U_{2^{(j)}}$. Since $U_{2^{j+1}} = U_{2 \cdot 2^{(j)}}$ is spanned by $U_{2^{(j)}} \star U_{2^{(j)}}$, we conclude that $U_{2^{j+1}} \subseteq V_{j+1}$. □

Note that while V_j is not straightforward to determine (since sgn is a non-linear map), U_j is easily computable. If $U_j = U_{j+1}$ for some j, then U_j is a Jordan algebra, and so $U_j = V_\infty$; therefore we get an upper bound on the number of iterations as $itr \leq \lceil \mathsf{log}_2\, j \rceil$. A trivial

bound for U_j to stop growing is $\frac{d(d+1)}{2} = \dim H_d(\mathbb{R})$, hence

$$itr \leq \left\lceil \log_2 \frac{d(d+1)}{2} \right\rceil \leq \lceil 2 \log_2 d \rceil.$$

We remark that, for robust self-tested initial strategy with explicit $\varepsilon - \delta$ dependence, we can use Proposition 5.7 repeatedly to get the robustness of the final strategy. For example, some of the robust self-testing results summarized in [SB20] have robustness $\varepsilon = O(\sqrt{\delta})$, and so $O(C\varepsilon + \delta) = O(\sqrt{\delta})$ in Proposition 5.7. If we take these initial strategies, we get

$$\varepsilon_\infty = O(\delta^{\frac{1}{2^{itr}+1}}) = O(\delta^{\frac{1}{4d}}).$$

Summarizing Proposition 5.16 and Lemma 5.18, and applying Proposition 5.13 to argue about many-ouput (rather than just binary-output) measurements, we reach an easy-to-use criterion for a real measurement $\tilde{O}$ to be reachable after iterative self-testing:

Theorem 5.19. *Let $\tilde{S} = (|\Phi_d\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y\})$ be a self-tested strategy using maximally entangled state and binary real projective measurements. A real projective measurement $\{\tilde{E}_\ell, \ell \in [0, L-1]\}$ can be iteratively self-tested if*

$$\tilde{E}_\ell \in \mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) \quad \forall \ell \in [0, L-1],$$

where $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\})$ is the real Jordan algebra generated by $\{\tilde{A}_x\}$. Moreover, the number of the iterations is upper-bounded by $\lceil 2 \log_2 d \rceil$.

In particular, if $\mathsf{JA}_{\mathbb{R}}(\{\tilde{A}_x\}) = H_d(\mathbb{R})$, *i.e.* $\{\tilde{A}_x\}$ generates the whole real Jordan algebra of symmetric $d \times d$ matrices, then every d-dimensional measurement can be self-tested. As what we have shown in Lemma 5.17, it is equivalent to $\{\tilde{A}_x\}$ having a trivial centralizer, which can be checked efficiently.

5.6 Appendix I: Examples for post-hoc self-testing

5.6.1 An analytic image of sgn in the two-dimensional case

Although the image of sgn is hard to describe in general cases, we give an example where $\mathsf{sgn}(\mathsf{span}\{D^2, DA_x^{(j)}D\})$ has an analytic form. In this case the initial state is a partially entangled, $|\tilde{\psi}\rangle = \cos\gamma\,|00\rangle + \sin\gamma\,|11\rangle$ for $\gamma \in (0, \frac{\pi}{4})$, and the binary observable $\tilde{A}_0 = X$ the Pauli X.

We show that there is a 1-parametric family of post-hoc self-tested binary observables $\mathsf{sgn}(\mathsf{span}\{D^2, DA_x^{(j)}D\})$. Note that $D\tilde{A}_xD = \mathsf{sin}\,\gamma\,\mathsf{cos}\,\gamma X$ for $\tilde{A}_0 = X$. Without loss of generality, suppose $\tilde{O} = \mathsf{sgn}(X + aD^2)$ for some real parameter a. If $|a|$ is large, then $X + aD^2$ is diagonally dominant, so $X + aD^2$ will be positive or negative definite, leading to the trivial case $\tilde{O} = \pm I$. So, to obtain a non-trivial $\tilde{O}$, $|a|$ must be bounded, and the upper bound is attained when $X + aD^2$ becomes singular:

$$\mathsf{det}(X + aD^2) = (a\,\mathsf{cos}\,\gamma\,\mathsf{sin}\,\gamma)^2 - 1 = 0 \Rightarrow a = \pm\frac{1}{\mathsf{cos}\,\gamma\,\mathsf{sin}\,\gamma}.$$

When $a \in [-\frac{1}{\mathsf{cos}\,\gamma\,\mathsf{sin}\,\gamma}, \frac{1}{\mathsf{cos}\,\gamma\,\mathsf{sin}\,\gamma}]$, we can calculate $\tilde{O}$ explicitly as a function of parameter a:

$$\tilde{O} = \begin{bmatrix} \frac{a\left(-1+2g^2\right)}{\sqrt{4+a^2(1-2g^2)^2}} & \frac{2}{\sqrt{4+a^2(1-2g^2)^2}} \\ \frac{2}{\sqrt{4+a^2(1-2g^2)^2}} & \frac{a-2ag^2}{\sqrt{4+a^2(1-2g^2)^2}} \end{bmatrix},$$

where $g = \mathsf{cos}\,\gamma$. Let $\tilde{O} = r_xX + r_zZ$, then $r_x = \frac{2}{\sqrt{4+a^2(1-2g^2)^2}}$, ranging from 1 to $\mathsf{sin}\,2\gamma$. Then in this case, the image of the sgn is $\{r_xX \pm \sqrt{1-r_x^2}Z\colon\ \mathsf{sin}(2\gamma) < r_x \leq 1\}$, which is an uncountable set.

We also give an explicit $\tilde{O}$ that cannot be post-hoc self-tested: let $\gamma = \mathsf{arctan}(1/\sqrt{2})$, $\tilde{O} = H = (X+Z)/\sqrt{2} \notin \mathsf{sgn}(\mathsf{span}\{D^2, X\})$. Then a "cheating" POVM $\{\hat{M}_0, \hat{M}_1\}$ is given by

$$\hat{M}_0 = \begin{bmatrix} \frac{6-\sqrt{2}}{8} & \frac{\sqrt{2}}{4} \\ \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{2} \end{bmatrix}, \hat{M}_1 = \begin{bmatrix} \frac{2+\sqrt{2}}{8} & -\frac{\sqrt{2}}{4} \\ -\frac{\sqrt{2}}{4} & 1-\frac{\sqrt{2}}{2} \end{bmatrix}.$$

One can check that this POVM generates the same correlation as $\tilde{O}$, but there is no local isometry connecting them. Indeed; suppose $\Phi[I_A \otimes \hat{M}_j\,|\tilde{\psi}_\gamma\rangle] = I_A \otimes \tilde{E}_j\,|\tilde{\psi}_\gamma\rangle$ for $j = 0, 1$, where $\tilde{E}_j = \frac{\tilde{O}+(-1)^jI}{2}$, then we have

$$0 = \langle\tilde{\psi}_\gamma|I_A \otimes \tilde{E}_0\tilde{E}_1|\tilde{\psi}_\gamma\rangle = \langle\tilde{\psi}_\gamma|I_A \otimes \hat{M}_0\Phi_A^*\Phi_A\hat{M}_1|\tilde{\psi}_\gamma\rangle = \langle\tilde{\psi}_\gamma|I_A \otimes \hat{M}_0\hat{M}_1|\tilde{\psi}_\gamma\rangle \neq 0,$$

a contradiction. Thus $\tilde{O}$ cannot be post-hoc self-tested based on $|\tilde{\psi}\rangle$ and X.

5.6.2 An obstruction to post-hoc self-testing

Here we show that, as soon as the number of inputs is small compared to local dimensions, a post-hoc extension of a self-testing strategy is a highly non-trivial phenomenon. In particular, the main theorem is non-trivial, since self-testing does not extend to "most" binary observables when the local dimension is large compared to the number of inputs.

Proposition 5.20. *Let $(|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{n-1}, \{\tilde{B}_y\}_{y=0}^{n-1})$ be a n-input / 2-output strategy with local dimension d. Assume that $|\tilde{\psi}\rangle$ has full Schmidt rank and the observables $\tilde{B}_y$ have a trivial centralizer in $\mathsf{M}_d(\mathbb{R})$.*

1. *If $\tilde{B}_{-n}, \tilde{B}_n \in \mathsf{M}_d(\mathbb{R})$ are distinct binary observables, then none of the strategies $(|\tilde{\psi}\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y, \tilde{B}_{\pm n}\})$ is a local dilation of the other.*
2. *If either $\lfloor \frac{d^2}{4} \rfloor > n+1$ or $|\psi\rangle$ is maximally entangled and $\lfloor \frac{d^2}{4} \rfloor > n$, then there exist distinct binary observables $\tilde{B}_{-n}, \tilde{B}_n \in \mathsf{M}_d(\mathbb{R})$ such that the strategies $(|\tilde{\psi}\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y, \tilde{B}_{\pm n}\})$ yield the same correlations, but none of them is a local dilation of the other (by 1.).*

Proof. 1. Suppose $(|\tilde{\psi}\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y, \tilde{B}_{-n}\})$ is a local dilation of $(|\tilde{\psi}\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y, \tilde{B}_n\})$. Thus there are isometries Φ_A,Φ_B and an auxiliary state $|\mathsf{aux}\rangle = \sum_i \sigma_i |ii\rangle \in \mathbb{R}^{d'}$ with $\sigma_1 > 0$ such that $\Phi_A \otimes \Phi_B |\tilde{\psi}\rangle = |\mathsf{aux}\rangle \otimes |\tilde{\psi}\rangle$ and

$$(\Phi_A \otimes \Phi_B)(\tilde{A}_x \otimes \tilde{B}_y) |\tilde{\psi}\rangle = |\mathsf{aux}\rangle \otimes ((\tilde{A}_x \otimes \tilde{B}_{|y|}) |\tilde{\psi}\rangle).$$

Then

$$(I \otimes \Phi_B \tilde{B}_y \Phi_B^*)(|\mathsf{aux}\rangle \otimes |\tilde{\psi}\rangle) = (I \otimes I \otimes \tilde{B}_{|y|})(|\mathsf{aux}\rangle \otimes |\tilde{\psi}\rangle)$$

for all $y \in \{0, \dots, n-1, -n\}$. Let $\pi : \mathbb{R}^d \otimes \mathbb{R}^{d'} \to \mathbb{R}^d$ be the projection induced by the projection $\mathbb{R}^{d'} \to \mathbb{R}$ onto the first component. Then

$$(I \otimes \pi \Phi_B \tilde{B}_y \Phi_B^* \pi^*) |\tilde{\psi}\rangle = (I \otimes \tilde{B}_{|y|}) |\tilde{\psi}\rangle$$

Since $|\tilde{\psi}\rangle$ has full Schmidt rank,

$$\pi \Phi_B \tilde{B}_y \Phi_B^* \pi^* = \tilde{B}_{|y|}$$

for all $y \in \{0, \dots, n-1, -n\}$. Let $C = \pi \Phi_B \in \mathbb{R}^{d \times d}$. Note that C is a contraction. Since $C \tilde{B}_y C^* = \tilde{B}_y$ for all $y \geq 0$ and $\tilde{B}_y$ generate the whole $\mathsf{M}_d(\mathbb{R})$ as an $\mathbb{R}$-algebra, it follows that C is invertible (otherwise $\tilde{B}_y$ would have a common kernel). Furthermore, if λ is an

eigenvalue of C^*, then $C^*v = \lambda v$ implies $C(\tilde{B}_y v) = \frac{1}{\lambda}\tilde{B}_y v$ for all $y \geq 0$. Since at least one of $\tilde{B}_y v$ is nonzero if $v \neq 0$, it follows that $\frac{1}{\lambda}$ is an eigenvalue of C. Since C, C^* are both contractions, we conclude that C is unitary. Therefore

$$C\tilde{B}_y = \tilde{B}_{|y|}C$$

for all $y \in \{0, \dots, n-1, -n\}$. Since $\tilde{B}_y$ have a trivial centralizer (also in $\mathsf{M}_d(\mathbb{C})$), it follows that C is a scalar multiple of identity. Therefore $\tilde{B}_{-n} = \tilde{B}_n$, a contradiction.

2. The real algebraic set of binary observables in $\mathsf{M}_n(\mathbb{R})$ has an irreducible component Z of dimension $\lfloor \frac{n^2}{4} \rfloor$ (concretely, Z is the set of binary observables with $\lfloor \frac{n}{2} \rfloor$ positive eigenvalues). Consider the map

$$Z \to \mathbb{R}^{d+1}, \qquad U \mapsto (\langle\psi| \tilde{A}_x \otimes U |\psi\rangle, \langle\psi| I \otimes U |\psi\rangle); \tag{27}$$

if $|\tilde{\psi}\rangle$ is maximally entangled, one can discard the last component $\langle\psi| I \otimes U |\psi\rangle) = \frac{1}{\sqrt{n}} \mathsf{Tr}(U)$ because it is constant on Z. Then (27) is a linear map between semialgebraic sets, so its generic fiber has dimension at least $\lfloor \frac{d^2}{4} \rfloor - n - 1 > 0$ (or $\lfloor \frac{d^2}{4} \rfloor - n > 0$ in the maximally entangled case). Therefore there exist distinct $\tilde{B}_{-n}, \tilde{B}_n \in Z$ such that

$$\langle\tilde{\psi}| I \otimes \tilde{B}_{-n} |\tilde{\psi}\rangle = \langle\tilde{\psi}| I \otimes \tilde{B}_n |\tilde{\psi}\rangle, \quad \langle\tilde{\psi}| \tilde{A}_x \otimes \tilde{B}_{-n} |\tilde{\psi}\rangle = \langle\tilde{\psi}| \tilde{A}_x \otimes \tilde{B}_n |\tilde{\psi}\rangle$$

holds for all x. □

If $|\tilde{\psi}\rangle$ is maximally entangled and $\tilde{A}_y = \tilde{B}_y$, then we know that after sufficiently many post-hoc steps, all binary observables are self-tested (under the given condition on $\tilde{B}_y$). Proposition 5.20(b) guarantees that this cannot always happen immediately after the first step if number of inputs n is sufficiently smaller than the local dimension d; in the case of our preferred strategy with $d+1$ inputs in Section 5.4, Proposition guarantees "bad" binary observables for $d \geq 5$. However, they already exist for $d = 3$:

Example 5.21. *Let $\tilde{A}_0, \dots, \tilde{A}_3 \in M_3(\mathbb{R})$ be the binary observables as in Section 5, and let $|\Phi_3\rangle \in \mathbb{R}^3 \otimes \mathbb{R}^3$ be the maximally entangled state (in its Schmidt basis). Then $\tilde{S} = (|\Phi_3\rangle, \{\tilde{A}_x\}_x, \{\tilde{A}_x\}_x\}$ is self-tested by its correlation, and $\{\tilde{A}_x\}_x$ has trivial centralizer in*

$M_3(\mathbb{R})$. *A direct calculation shows that*

$$\tilde{A}_{\pm 4} = \begin{pmatrix} 0 & -\frac{1}{\sqrt{2}} & \pm\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{2} & \mp\frac{1}{2} \\ \pm\frac{1}{\sqrt{2}} & \mp\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

are binary observables with one positive eigenvalue, and

$$\langle\Phi_3|\, \tilde{A}_x \otimes A_{-4}\, |\Phi_3\rangle = \langle\Phi_3|\, \tilde{A}_x \otimes A_4\, |\Phi_3\rangle \qquad \textit{for } x = 0, \ldots, 3.$$

Therefore the strategies $(|\Phi_3\rangle, \{\tilde{A}_x\}, \{\tilde{A}_x, A_{\pm 4}\})$ *give the same correlation but are not local dilations of each other by Proposition 5.20(a), so they are not self-tested.*

5.7 Appendix II: Recipe for the robust self-tested strategy

We first show how to construct $d+1$ unit vectors $v_0, \ldots, v_d \in \mathbb{R}^d$ that form the vertices of a regular $d+1$-simplex centered at the origin. This can be guaranteed by $\langle v_j, v_k\rangle = -1/d$ for all $j \neq k$. To find vectors satisfying this property, consider any unitary U in $\mathbb{R}^{d+1}$ whose first row is the 'all one' unit vector $a = (1, 1, ..., 1)/\sqrt{d+1}$. Then, apply U to $d+1$ vectors $\{f_j\}$ where f_j is the normalization of $f'_j = e_j - \langle a, e_j\rangle\, a$, and $\{e_j\}_{j=0}^d$ are base vectors. We have that all Uf_j are orthogonal to e_0. So $\{Uf_j\}_{j=0}^d$ spans a d-dimensional subspace. We can also show that $\langle Uf_j, Uf_k\rangle = \langle f_j, f_k\rangle = -1/d$. So we take $v_x = Uf_x$, $\tilde{P}_x = v_x v_x^*$, and $\tilde{T}_x = 2\tilde{P}_x - I$.

```
(*local dimension*)
d = 4;
(*find the unitary*)
allone = Normalize[ConstantArray[1, d + 1]];
unitary = ConstantArray[0, {d + 1, d + 1}];
unitary[[1, All]] = allone;
unitary[[2 ;; d + 1, All]] =
  Table[UnitVector[d + 1, i], {i, 2, d + 1}];
unitary = Orthogonalize[unitary];
(*d+1 vectors*)
vect[x_] := (unitary .
      Normalize[(UnitVector[d + 1, x] -
```

```
        Projection[UnitVector[d + 1, x], allone])][[2 ;; d + 1]] //
   FullSimplify;
(*d+1 projections*)
proj[x_] := Transpose[{vect[x]}] . {vect[x]} // FullSimplify;
(*d+1 binary observables*)
obs[x_] := 2 proj[x] - IdentityMatrix[d];
jordanproduct[x_, y_] := (x . y + y . x)/2;
sgn[x_] :=
  JordanDecomposition[x][[1]] .
    RealSign[JordanDecomposition[x][[2]]] .
    Inverse[JordanDecomposition[x][[1]]] // FullSimplify;
(* alternative sgn map *)
(* sgn[x_] := Inverse[x].MatrixPower[x.x,1/2] *)
```

Based on this one can calculate $\tilde{T}_{jk} = \mathsf{sgn}(\tilde{T}_j + \tilde{T}_k)$, or alternatively $\tilde{T}_{jk} = 2w_{jk}w_{jk}^* - I$, where $w_{jk} := \sqrt{\frac{d}{2(d+1)}}(v_j - v_k)$.

```
obs2[x_, y_] := sgn[obs[x] + obs[y]];
(*alternative O_{jk} operator*)
(*obs2[x_,y_]:=d/(d+1) \
Transpose[{vect[x]-vect[y]}].{vect[x]-vect[y]}//FullSimplify;*)
```

References

[ABDC18] Ole Andersson, Piotr Badziąg, Irina Dumitru, and Adán Cabello. Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant bell inequality. Phys. Rev. A, 97:012314, Jan 2018.

[AM16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. Nature, 540(7632):213–219, Dec 2016.

[APVW16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. Phys. Rev. A, 93:040102, Apr 2016.

[AWS] Aws braket: https://aws.amazon.com/braket/.

[BCD+09] Alessandro Bisio, Giulio Chiribella, Giacomo Mauro D'Ariano, Stefano Facchini, and Paolo Perinotti. Optimal quantum tomography. IEEE Journal of Selected Topics in Quantum Electronics, 15(6):1646–1660, 2009.

[BCK+23] Pedro Baptista, Ranyiliu Chen, Jędrzej Kaniewski, David Rasmussen Lolck, Laura Mančinska, Thor Gabelgaard Nielsen, and Simon Schmidt. A mathematical foundation for self-testing: Lifting common assumptions. arXiv:2310.12662, 2023.

[BCM+18] Zvika Brakerski, Paul F. Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Mikkel Thorup, editor, 59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018, pages 320–331. IEEE Computer Society, 2018.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. Reviews of Modern Physics, 86(2):419–478, Apr 2014.

[Bel64] John Stewart Bell. On the Einstein Podolsky Rosen paradox. Physics Physique Fizika, 1:195–200, Nov 1964.

[Ben20] Roberto Beneduci. Notes on naimark's dilation theorem. Journal of Physics: Conference Series, 1638(1):012006, Oct 2020.

[BSCA18] Joseph Bowles, Ivan Supić, Daniel Cavalcanti, and Antonio Acín. Self-testing of pauli observables for device-independent entanglement certification. Phys. Rev. A, 98(4):042336, 2018.

[Cao22] Longbing Cao. Beyond IID: Non-IID thinking, informatics, and learning. IEEE Intelligent Systems, 37(4):5–17, 2022.

[CGJV19] Andrea Coladangelo, Alex B. Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources. In Yuval Ishai and Vincent Rijmen, editors, Advances in Cryptology – EUROCRYPT 2019, pages 247–277, Cham, 2019. Springer International Publishing.

[CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. Nature Communications, 8(1), May 2017.

[CHLM22] Matthias Christandl, Nicholas Gauguin Houghton-Larsen, and Laura Mancinska. An Operational Environment for Quantum Self-Testing. Quantum, 6:699, Apr 2022.

[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, Oct 1969.

[CMM+24] David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang. A computational tsirelson's theorem for the value of compiled xor games. arXiv:2402.17301, 2024.

[CMV24] Ranyiliu Chen, Laura Mančinska, and Jurij Volčič. All real projective measurements can be self-tested. Nature Physics, 20(10):1642–1647, Oct 2024.

[Col17] Andrea Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. Quantum Info. Comput., 17(9–10):831–865, Aug 2017.

[Col20] Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. Quantum, 4:282, June 2020.

[CRO+19] Yudong Cao, Jonathan Romero, Jonathan P. Olson, Matthias Degroote, Peter D. Johnson, Mária Kieferová, Ian D. Kivlichan, Tim Menke, Borja Peropadre, Nicolas P. D. Sawaya, Sukin Sim, Libor Veis, and Alán Aspuru-Guzik. Quantum chemistry in the age of quantum computing. Chemical Reviews, 119(19):10856–10915, Oct 2019.

[CV] Ranyiliu Chen and Jurij Volčič. A study of complex self-testing. In preparation.

[Fu22] Honghao Fu. Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension. Quantum, 6:614, Jan 2022.

[FVS+24] Máté Farkas, Jurij Volčič, Sigurd A. L. Storgaard, Ranyiliu Chen, and Laura Mančinska. Maximal device-independent randomness in every dimension. arXiv:2409.18916, 2024.

[HOZC24] Jaròn Has, Māris Ozols, Jeroen Zuiddam, and Ranyiliu Chen. Entanglement-assisted Shannon capacity of graphs. Contributed to the Master Thesis of Jaròn Has, 2024.

[IBM] Ibm qiskit https://www.ibm.com/quantum.

[IS05] Alfredo Iusem and Alberto Seeger. On pairs of vectors achieving the maximal angle of a convex cone. Mathematical Programming, 104(2):501–523, Nov 2005.

[Jac68] Nathan Jacobson. Structure and Representations of Jordan Algebras, volume 39 of American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, R.I., 1968.

[JHCL19] C. Jebarathinam, Jui-Chen Hung, Shin-Liang Chen, and Yeong-Cherng Liang. Maximal violation of a broad class of bell inequalities and its implication on self-testing. Phys. Rev. Res., 1:033073, Nov 2019.

[JMS20] Rahul Jain, Carl A. Miller, and Yaoyun Shi. Parallel device-independent quantum key distribution. IEEE Transactions on Information Theory, 66(9):5567–5584, 2020.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE. arXiv:2001.04383, 2020.

[JvNW34] Pascual Jordan, John von Neumann, and Eugene Wigner. On an algebraic generalization of the quantum mechanical formalism. Annals of Mathematics, 35(1):29–64, 1934.

[KLVY22] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. arXiv:2203.15877, 2022.

[KMP+24] Alexander Kulpe, Giulio Malavolta, Connor Paddock, Simon Schmidt, and Michael Walter. A bound on the quantum value of all compiled nonlocal games. arXiv:2408.06711, 2024.

[KST+19] Jędrzej Kaniewski, Ivan Supić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. Quantum, 3:198, Oct 2019.

[Li03] Bingren Li. Real Operator Algebras. World Scientific, 2003.

[Lol22] David R. Lolck. The Role of Classical Randomness in Self-Testing. Project report, UCPH, 2022.

[McC04] Kevin McCrimmon. A taste of Jordan algebras. Universitext. Springer-Verlag, New York, 2004.

[McK16] Matthew McKague. Interactive proofs for BQP via self-tested graph states. Theory of Computing, 12(3):1–42, 2016.

[McK17] Matthew McKague. Self-testing in parallel with CHSH. Quantum, 1:1, Apr 2017.

[MM11] Matthew McKague and Michele Mosca. Generalized self-testing and the security of the 6-state protocol. In Wim van Dam, Vivien M. Kendon, and Simone Severini, editors, Theory of Quantum Computation, Communication, and Cryptography, pages 113–130, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[MMG09] Matthew McKague, Michele Mosca, and Nicolas Gisin. Simulating quantum systems using real hilbert spaces. Physical Review Letters, 102(2), Jan 2009.

[MNP21] Laura Mancinska, Thor Gabelgaard Nielsen, and Jitendra Prakash. Glued magic games self-test maximally entangled states. arXiv:2105.10658, 2021.

[MPS24] Laura Mančinska, Jitendra Prakash, and Christopher Schafhauser. Constant-sized robust self-tests for states and measurements of unbounded dimension. Commun. Math. Phys., 405(221), 2024.

[MW16] Ashley Montanaro and Ronald de Wolf. A Survey of Quantum Property Testing. Number 7 in Graduate Surveys. Theory of Computing Library, 2016.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. Quantum Information & Computation, 4(4):273–286, 2004.

[MYS12] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. Journal of Physics A: Mathematical and Theoretical, 45(45):455304, Oct 2012.

[NC10] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, 2010.

[NZ23] Anand Natarajan and Tina Zhang. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification. arXiv:2303.01545, 2023.

[PAB+20] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. Adv. Opt. Photon., 12(4):1012–1236, Dec 2020.

[Pau16] Vern Paulsen. Lecture notes "Entanglement and Nonlocality", 2016. Available at https://www.math.uwaterloo.ca/~vpaulsen.

[PPW23] Ekta Panwar, Palash Pandya, and Marcin Wieśniak. An elegant scheme of self-testing for multipartite Bell inequalities. npj Quantum Information, 9(1):71, 2023.

[PSZZ24] Connor Paddock, William Slofstra, Yuming Zhao, and Yangchen Zhou. An operator-algebraic formulation of self-testing. Ann. Henri Poincaré, 25:4283–4319, 2024.

[SB20] Ivan Supić and Joseph Bowles. Self-testing of quantum systems: a review. Quantum, 4:337, Sep 2020.

[SBJ+23] Shubhayan Sarkar, Jakub J. Borkała, Chellasamy Jebarathinam, Owidiusz Makuta, Debashis Saha, and Remigiusz Augusiak. Self-testing of any pure entangled state with the minimal number of measurements and optimal randomness certification in a one-sided device-independent scenario. Physical Review Applied, 19(3), Mar 2023.

[SBR+23] Ivan Supić, Joseph Bowles, Marc-Olivier Renou, Antonio Acín, and Matty J Hoban. Quantum networks self-test all entangled states. Nature Physics, 19:670–675, Feb 2023.

[SSKA21] Shubhayan Sarkar, Debashis Saha, Jędrzej Kaniewski, and Remigiusz Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. npj Quantum Information, 7(1):1–5, 2021.

[Tsi87] Boris Tsirelson. Quantum analogues of the Bell inequalities. the case of two spatially separated domains. Journal of Soviet Mathematics, 36:557–570, 1987.

[Vol22] Jurij Volčič. Personal communication. 2022.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. Physical Review Letters, 113(14), Sep 2014.

[Wat18] John Watrous. The Theory of Quantum Information. Cambridge University Press, 2018.

[WKB+20] Erik Woodhead, Jędrzej Kaniewski, Boris Bourdoncle, Alexia Salavrakos, Joseph Bowles, Antonio Acín, and Remigiusz Augusiak. Maximal randomness from partially entangled states. Phys. Rev. Research, 2:042028, Nov 2020.

[YN13] Tzyh Haur Yang and Miguel Navascue s. Robust self-testing of unknown quantum systems into any entangled two-qubit states. Physical Review A, 87(5), May 2013.