Quantum Test for Higher Order Gowers Norms

Rik Westdorp*

Abstract

In this work, a quantum self-test which certifies that measurements of a quantum device have a large Gowers norm of order k is presented and analysed. The test protocol is described as a two-player quantum game, in which players provide answers based on measurements on subsystems of a maximally entangled bipartite state. The protocol makes use of $2^k + 1$ subtests. It is shown that strategies that succeed in the test with success rate $1 - \epsilon$ must have a Gowers norm larger than $1 - O(\epsilon)$. This test generalises measurement tests that certify measurements based on the second order Gowers norm.

1 Introduction

Quantum algorithms, like Shor's quantum algorithm for integer factorization [1], require a computational system that affords the advantage of employing quantum mechanical properties such as superposition, interference and entanglement. This dependence of the quantum advantage on the physical apparatus brings about a trust issue regarding the specifications of quantum devices. The means to verify quantum mechanical properties of a computational system has, accordingly, become an important issue in the field of quantum computation.

The Bell test [2] provided the first procedure that could certify quantum mechanical properties of a system. It makes use of a statistical bound, called a Bell inequality, that bounds the correlation of answers of two isolated parties to questions of a verifier. The Bell inequality holds under the assumption that the parties do not share any entanglement. As such, a violation certifies that the parties have successfully made use of entanglement. From here, the capacity of tests has developed to means of specifying more detailed features, such as the measurements employed during the test [3].

As pointed out by Vidick, there is a connection between the analysis of these measurement tests and the field of approximate representation theory. In particular, the Gowers-Hatami theorem [4] can be used to show that when measurements are tested to approximately satisfy representative group relations, the measurements essentially behave as the corresponding group. A key aspect herein is the notion of Gowers norms. Gowers norms are useful tools for quantifying structure in functions on a finite group. More specifically, matrix-valued functions with a large second order Gowers norm, or U^2 norm, correlate with a group representation. In testing applications, it is verified that the employed strategies have a large U^2 norm, so that it can be concluded that the measurements essentially behave as the corresponding group.

For scalar-valued functions, similar structural conclusions can be formulated for functions with a large Gowers norm of higher order (U^k norm, with $k \geq 3$) [5]. However, as the order increases, less structure remains and the description of the class of functions becomes more complicated. At this point, a precise structural classification of matrix-valued functions with a large U^k norm is not available. Nonetheless, while it is still unclear what structural properties are present in this class of functions, the question arises whether the property of a large U^k norm can be verified in a test.

In this work, a two-player protocol to test order k Gowers norms consisting of $2^k + 1$ subtests is introduced and analysed. It is shown that strategies that are successful in the test with success rate $1 - \epsilon$ must have a Gowers norm larger than $1 - O(\epsilon)$. The proof of this claim follows the structure of an analysis of the Blum-Luby-Rubinfeld linearity test by Vidick [6]. Each of the subtests is shown to produce a correlation between observables employed in the test, which can be combined to obtain an estimate of the Gowers norm.

The remaining part of this work proceeds as follows: Section 2 introduces notation and describes the set-up of two-player tests. In Section 3, Gowers norms for scalar functions are introduced and we discuss their generalisation to matrix-valued functions. Thereafter, in Section 4, we present the Gowers-Hatami theorem on approximate representations and examine the relation with measurement testing. Section 5 treats the protocol to test Gowers norms and its analysis. Lastly, the results are discussed in Section 6.

*This work resulted from an internship at QuSoft, CWI, under supervision of Dr. J. Briët as part of the Applied Mathematics Masters program at the Delft University of Technology.

2 Preliminaries

In what follows, the set-up of a two-player self-test is described before we discuss the topic of Gowers norms and their connection with approximate representation theory in Sections 3 and 4. We also introduce notation regarding the quantum states and measurements involved.

2.1 Two-player games

The protocols that make up quantum self-tests can be conveniently formulated in the language of two-player quantum games. In this setting, we think of two players having access to a subsystem of a quantum state, instead of speaking about two measurement devices. The end-user takes on the role of a referee, who communicates with the two players by randomly sending them instances from an agreed upon set of queries. The players, whom we will name Alice and Bob, must then respond according to an agreed upon set of answers. The testing protocol describes what queries the referee should send to the players, what answers the players can provide and which responses are accepted.

Alice and Bob are assumed to have no means of communication, except for having access to parts of the same quantum system. This ensures that the test cannot be trivially cheated, because a player does not know what query the other player receives. In order to still succeed in the test, they must make use of the non-local nature of quantum measurement by preparing an entangled state. In this work, we consider a setting in which the two players have access to a maximally entangled bipartite state $|\mathrm{EPR}\rangle_{d\times d} := \frac{1}{\sqrt{d}}\sum_{i=1}^{d} e_i \otimes e_i \in \mathbb{C}^d \otimes \mathbb{C}^d$ of dimension $d \times d$. Alice and Bob can perform projective measurements on their subsystem, and we denote the space of n-outcome projective measurement on $\mathbb{C}^d$ as $\mathrm{Proj}_n(d)$. In case the measurement is binary, we call the projective measurement an observable, and we denote the space of observables on $\mathbb{C}^d$ as $\mathrm{Obs}(d)$.

2.2 Measurement

Upon receiving a query, both players measure their subsystem with a projective measurement and submit the measurement result to the referee. Say Alice measures her subsystem with an n-outcome projective measurement $\{A_1, \ldots, A_n\}$ with outcomes $\{\lambda_1, \ldots, \lambda_n\}$, and Bob with an m-outcome projective measurement $\{B_1, \ldots, B_m\}$ with outcomes $\{\mu_1, \ldots, \mu_m\}$. Here, $A^1, \ldots, A^n$ and $B^1, \ldots, B^m$ are projectors that sum to identity. This results in the following probability distribution on $\{\lambda_1, \ldots, \lambda_n\} \times \{\mu_1, \ldots, \mu_m\}$ of measurement outcomes (a, b):

$$\begin{aligned}
\mathbb{P}[(a,b)] &= \left\| \frac{1}{\sqrt{d}} \sum_{i=1}^{d} A^a e_i \otimes B^b e_i \right\|^2 = \frac{1}{d} \left\langle \sum_{i=1}^{d} A^a e_i \otimes B^b e_i, \sum_{j=1}^{d} A^a e_j \otimes B^b e_j \right\rangle \\
&= \frac{1}{d} \sum_{i,j=1}^{d} \langle A^a e_i \otimes B^b e_i, A^a e_j \otimes B^b e_j \rangle = \frac{1}{d} \sum_{i,j=1}^{d} \langle A^a e_i, A^a e_j \rangle \langle B^b e_i, B^b e_j \rangle \\
&= \frac{1}{d} \sum_{i,j=1}^{d} e_i^* (A^a)^* A^a e_j e_i^* (B^b)^* B^b e_j = \frac{1}{d} \sum_{i,j=1}^{d} e_i^* A^a e_j e_i^* B^b e_j = \frac{1}{d} \sum_{i,j=1}^{d} (A^a)_{ij} (B^b)_{ij} \\
&= \frac{1}{d} \sum_{i,j=1}^{d} \overline{(A^a)_{ji}} (B^b)_{ij} = \frac{1}{d} \sum_{i=1}^{d} (A^a B^b)_{ii} = \frac{1}{d} \operatorname{Tr}(A^a B^b).
\end{aligned}$$

Before the start of the game, Alice and Bob should come up with a strategy on how to respond to the queries of the referee. That is, for each question that the referee can ask, Alice and Bob must select a projective measurement that will be used to produce their answer to a query. Their strategy is thus characterised by a function that maps queries of the referee to projective measurements.

3 Gowers norms

As seen in the previous section, strategies of players in a quantum game are specified by a function that sends queries to projective measurements. For quantum self-tests that are used to certify measurement behaviour, the queries of the referee are often labelled by elements of some Abelian group G. One can then associate a function $f : G \to M_d(\mathbb{C})$ with the strategy of a player that maps group elements to a $d \times d$ complex matrix. A useful tool for analysing functions on an Abelian group is the Gowers norm. Below, we define the Gowers norms first on scalar-valued functions and show that they are indeed norms. Thereafter, we introduce a matrix-valued generalisation.

3.1 Scalar-valued

Gowers uniformity norms originated in the field of additive combinatorics. The following definitions and proofs are adapted from [7].

Definition 1 (Gowers uniformity norm, scalar-valued)**.** *Let G be an Abelian group and $f : G \to \mathbb{C}$. For $k \geq 2$, the Gowers uniformity norm is defined by*

$$\|f\|_{U^k}^{2^k} := \mathop{\mathbb{E}}_{x,h_1,\ldots,h_k \in G} \prod_{\omega \in \{0,1\}^k} \mathcal{C}^{|\omega|} f(x + \omega \cdot h),$$

where $\mathcal{C}f := \overline{f}$ is the conjugation operator, $\omega := (\omega_1, \ldots, \omega_k), h := (h_1, \ldots, h_k)$, and $|\omega| := \omega_1 + \ldots + \omega_k$.

So for instance, we have for $k = 2$:

$$\|f\|_{U^2}^4 = \mathop{\mathbb{E}}_{x,h_1,h_2 \in G} f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2),$$

and for $k = 3$:

$$\begin{aligned}\|f\|_{U^3}^8 = \mathop{\mathbb{E}}_{x,h_1,h_2,h_3 \in G} & f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2)\times \\ & f(x+h_1+h_3)f(x+h_2+h_3)\overline{f(x+h_1+h_2+h_3)}.\end{aligned}$$

To see that these expressions indeed define norms, it is convenient to define a multilinear form on 2^k functions $(f_\omega)_{\omega \in \{0,1\}^k}$, which takes on the role of an inner product. This form can be used to show that the Gowers norm satisfies the triangle inequality. Homogeneity and non-negativity are clear from the definition.

Definition 2 (Gowers inner product, scalar-valued)**.** *Let G be an Abelian group, $k \geq 2$, and $f_\omega : G \to \mathbb{C}$ for all $\omega \in \{0,1\}^k$. The Gowers inner product is defined by*

$$\langle (f_\omega)_{\omega \in \{0,1\}^k} \rangle_{U^k} := \mathop{\mathbb{E}}_{x,h_1,\ldots,h_k \in G} \prod_{\omega \in \{0,1\}^k} \mathcal{C}^{|\omega|} f_\omega(x + \omega \cdot h).$$

Note that the Gowers inner product induces the Gowers norm:

$$\|f\|_{U^k}^{2^k} = \langle (f)_{\omega \in \{0,1\}^k} \rangle_{U^k}.$$

The selective conjugation of terms in the Gowers inner product ensures that the product satisfies a generalised version of conjugate symmetry. More precisely, for $1 \leq i \leq k$ we can divide the functions in the product into two subsets of equal size by the value of their label ω at the i-th position. Interchanging the groups results in conjugation of the Gowers inner product. As such, the Gowers inner product behaves as a regular inner product on these groups. This allows the use of the Cauchy-Schwarz inequality, for instance for the subdivision based on the last position of the label:

$$|\langle (f_\omega)_{\omega \in \{0,1\}^k} \rangle_{U^k}| \leq \langle (f_{\omega',0})_{\omega \in \{0,1\}^k} \rangle_{U^k}^{1/2} \langle (f_{\omega',1})_{\omega \in \{0,1\}^k} \rangle_{U^k}^{1/2},$$

where ω' denotes the first $k-1$ components of ω. By repeated application of the Cauchy-Schwarz inequality one obtains the Gowers-Cauchy-Schwarz inequality

$$|\langle (f_\omega)_{\omega \in \{0,1\}^k} \rangle_{U^k}| \leq \prod_{\tilde{\omega} \in \{0,1\}^k} |\langle (f_{\tilde{\omega}})_{\omega \in \{0,1\}^k} \rangle_{U^k}|^{1/2^d} = \prod_{\omega \in \{0,1\}^k} \|f_\omega\|_{U^k}.$$

The Gowers-Cauchy-Schwarz inequality can be used to deduce the triangle inequality as follows:

$$\begin{aligned}\|f_0 + f_1\|_{U^k}^{2^k} = \langle (f_0 + f_1), \ldots, (f_0 + f_1) \rangle_{U^k} &= \sum_{\omega \in \{0,1\}^{2^k}} \langle f_{\omega_1}, \ldots, f_{\omega_{2^k}} \rangle_{U^k} \\ &\leq \sum_{\omega \in \{0,1\}^{2^k}} \prod_{i=1}^{2^k} \|f_{\omega_i}\|_{U^k} = \prod_{\tilde{\omega} \in \{0,1\}^k} (\|f_0\|_{U^k} + \|f_1\|_{U^k}),\end{aligned}$$

and it follows that

$$\|f_0 + f_1\|_{U^k} \leq \|f_0\|_{U^k} + \|f_1\|_{U^k},$$

as desired.

3.2 Matrix-valued

Since our interest lies with matrix-valued functions, we introduce a generalisation of the Gowers norms for functions that take values in the matrices of size $n \times n$.

Definition 3 (Gowers uniformity norm, matrix-valued)**.** *Let G be an Abelian group and $F : G \to M_n(\mathbb{C})$. For $k \geq 2$, the Gowers uniformity norm is defined by*

$$\|F\|_{U^k}^{2^k} := \mathop{\mathbb{E}}_{x,h_1,\ldots,h_k \in G} \operatorname{Tr}\left[\prod_{\omega \in \{0,1\}^k} \mathcal{H}^{|\omega|} F(x + \omega \cdot h)\right],$$

where $\mathcal{H}F := F^*$ acts as the conjugate transpose.

With this expression we can also associate a generalised inner product.

Definition 4 (Gowers inner product, matrix-valued)**.** *Let G be an Abelian group, $k \geq 2$, and $F_\omega : G \to \mathbb{C}$ for all $\omega \in \{0,1\}^k$. The Gowers inner product is defined by*

$$\langle (F_\omega)_{\omega \in \{0,1\}^k} \rangle_{U^k} := \mathop{\mathbb{E}}_{x,h_1,\ldots,h_k \in G} \operatorname{Tr}\left[\prod_{\omega \in \{0,1\}^k} \mathcal{H}^{|\omega|} F_\omega(x + \omega \cdot h)\right].$$

By linearity of the trace, the matrix-valued Gowers inner product is multilinear. Furthermore, the cyclic property of the trace ensures that the product satisfies the generalised version of conjugate symmetry [4]. Therefore we can conclude that also in the matrix-valued case, the Gowers norms are indeed norms as their inner products satisfy the Gowers-Cauchy-Schwarz inequality.

4 Approximate representations

Having defined the notion of Gowers norms for both scalar-valued and matrix-valued functions on an Abelian group, we will now move on to discuss the relation of the second order Gowers norm to representations in Section 4.1. We then move on to applications in the field of measurement testing in Section 4.2, and consider what can be expected higher order Gowers norms in Section 4.3.

4.1 Gowers-Hatami theorem

In the context of matrix-valued functions on a group, the most structured examples of functions are homomorphisms from the group to the matrix group, as they preserve the group relation and thereby the group structure. It is easily verified that the homomorphisms from a group to the matrix group, or group representations, have a large U^2 norm. The Gowers-Hatami theorem provides an inverse statement. It states that functions with a large U^2 norm correlate with a group representation [4]:

Theorem 1 (Gowers-Hatami)**.** *Let G be a finite group, let $c > 0$ and let $F : G \to M_n(\mathbb{C})$ be a function such that $\|F(x)\|_{op} \leq 1$ for every $x \in G$ and $\|F\|_{U^2}^4 \geq cn$. Then there exists $m \in [cn/(2-c), (2-c)n/c]$, $n \times m$ partial unitary matrices U and V , and a unitary representation $P : G \to U(m)$ such that*

$$|\mathbb{E}_x \langle F(x), VP(x)U^* \rangle| \geq \tau(c)^4 m,$$

where $\tau(c) = \max\{(c/(2-c))^2, (c/2)^{1/2}\}$.

In the conclusion of the theorem, the expectation denotes an average over the group elements, and the inner product is the Frobenius matrix inner product. The condition $\|F(x)\|_{op} \leq 1$ for every $x \in G$ ensures that the functions do not have a large U^2 norm by trivial means. We see that the representation with which the function correlates is not necessarily of the same dimension, and the unitary matrices serve to reconcile this difference. The Gowers-Hatami theorem characterises the role of the U^2 norm as measure of structure. The larger the U^2 norm of a function, the closer it lies to a function that has perfect structure, a group representation.

4.2 Testing group relations

When brought into the context of strategies for quantum test as described in Section 2, the Gowers-Hatami theorem provides a meaningful statement about strategies that have a large U^2 norm. That is, the measurements performed during the test upon receiving a query, behave as a group representation. This conclusion can thus certify a claim that a measurement device can perform some group of measurements. Vidick and Natarajan,

for example, have formulated a self-test which verifies that a measurement device performs measurements that are homomorphic to the group of Weyl-Heisenberg operators [8]. Their protocol makes use of the concept of approximate representations, which is a sufficient condition for having a large U^2 norm. Approximate representations are functions on the group for which the homomorphism property holds approximately. For instance, one can define the approximate representations as a function $F : G \to M_n(\mathbb{C})$ that satisfies

$$\|F(x)F(y) - F(x+y)\| \leq \epsilon,$$

for all $x, y \in G$. The relation above is a suitable starting point for quantum testing. Consider for the moment that x and y are fixed. Then, one can verify the relation above by sending one player questions x and y, and the other $x + y$. The verifier accepts the answers when product of the two answers matches the answer of the other player. For such a protocol, a large success rate demonstrates that the approximate representation property is satisfied. Vidick and Natarajan extend the statement to all $x, y \in G$ by choosing a suitable group presentation, and testing that these relations hold approximately. One can then retrieve the approximate representation property by writing elements of the group in terms of the generators. With the approximate representation property established, it can be concluded from the Gowers-Hatami theorem that the measurements are close to a representation of the group.

4.3 Outlook

The work of Vidick and Natarajan provides a clear method for establishing group relations in measurement devices via the U^2 norm. There may however be instances where a device can not achieve a large enough U^2 norm to pass such a test. Nevertheless, it can be the case that a function has a small U^2 norm, but a large U^3 or higher order Gowers norm. Presently, it is unclear what one can conclude about functions with a large U^k norm, for $k \geq 3$. In the simplified case of the scalar-valued Gowers norm, inverse theorems for higher order Gowers norms do exist. They have been established in [5], and are a lot more complicated than the U^2 case. Since scalar-valued functions are a trivial example of matrix-valued functions, inverse theorems for higher order matrix-valued Gowers norms can not be expected to be any simpler. Although the nature of functions with a large U^k norm is presently unclear, having a large U^k norm is a property that can be verified in a quantum self-test. This claim is asserted in the following section.

5 Testing the Gowers norms

In the section below, a two-player protocol is introduced that can certify the use of a strategy with a large U^k norm for functions on an Abelian group Z. Section 5.1 provides a description of the testing protocol. In Section 5.2, it is shown that the protocol is a sound test for the order k Gowers norm.

5.1 Protocol

Two players, Alice and Bob, each have access to one subsystem of a maximal entangled bipartite state of dimension $d \times d$ upon which they can perform measurements. The referee assigns roles 'Player 1' and 'Player 2' to Alice and Bob at random. He selects $x, h_1, \ldots, h_k \in Z$ uniformly at random. Denote $c_\omega := x + \omega \cdot (h_1, \ldots, h_d)$ for all $\omega \in \Omega := \{0,1\}^d$ and furthermore $c_A := \{c_\omega | \omega \in A\}$ for subsets $A \subseteq \Omega$. With equal probability, the verifier performs one of the following subtests described in Table 1 below.

Table 1. In this table, the subtest used in the Gowers test are summarized. The test consist of one Parallel consistency subtest, $2^k - 1$ Linearity consistency subtests (one for each $\omega \in \Omega \setminus \overline{1}$) and a Gowers norm subtest. For each subtest, the queries sent by the verifier, the expected answers from the players and the condition for success is specified.

Subtest	Query for Player 1	Expected answer of Player 1	Query for Player 2	Expected answer of Player 2	Condition for success
Parallel consistency	x	1 bit a	x	1 bit b	$a = b$
Linearity consistency ω, for $\omega \in \Omega \setminus \overline{1}$	$c_{\Omega \setminus \overline{1}}$	$2^k - 1$ bits $a_{\Omega \setminus \overline{1}}$	c_ω	1 bit b	$a_\omega = b$
Gowers norm	$c_{\Omega \setminus \overline{1}}$	$2^k - 1$ bits $a_{\Omega \setminus \overline{1}}$	$c_{\overline{1}}$	1 bit b	$\prod_{\omega \in \Omega \setminus \overline{1}} a_\omega = b$

Alice answers 1 bit questions via a strategy $F : Z \to \mathrm{Obs}(d)$ and $2^k - 1$ bits questions via a strategy $G : Z^{\Omega \setminus \overline{1}} \to \mathrm{Proj}_{2^n}(d)$, with $n = 2^k - 1$. Here it is understood that upon receiving a query $x \in Z$, Alice measures her subsystem with observable $F(x)$, and upon receiving a $2^k - 1$-tuple query $c_{\Omega \setminus \overline{1}}$ she measures her subsystem with the $2^{2^k - 1}$-outcome projective measurement $G(c_{\Omega \setminus \overline{1}})$. We denote Bob's respective strategies as $\tilde{F}$ and $\tilde{G}$.

The Parallel consistency subtest enforces the players to use strategies that are almost identical. The linearity consistency subtests ensures that the answers to a query c_ω correlate with the bit with label ω in the 2^k-1 bits answer. Lastly, the Gowers subtest sets up a correlation between the product of bits in the 2^k-1 bits answer and the 1 bit answer. These correlations can be combined to show that the expectation of the product of answers to queries c_Ω is large. As will be explained in the following section, this implies that the strategies used have a large Gowers norm of order k.

5.2 Analysis

In this section we show that the Gowers test described in the previous section can only by passed with strategies that have a large U^k norm. The analysis follows the structure of a work by Vidick on the Blum-Luby-Rubinfeld linearity test [6]. More precisely, we prove the following theorem.

Theorem 2 (Soundness of the Gowers test)**.** *Let $k \geq 2$ be an integer, $\epsilon \geq 0$, and $F : Z \to Obs(d)$ and $G : (Z)^{\Omega\setminus\overline{1}} \to Proj_{2^n}(d)$ with $n = 2^k - 1$ a quantum strategy for the Gowers test. If players determining their answers according to this strategy succeed in the test with probability at least $1-\epsilon$, then*

$$\|F\|_{U^k}^{2^k} \geq 1 - O(\epsilon).$$

Proof: Suppose a strategy determined by $F, G, \tilde{F}, \tilde{G}$ as above is successful in the Gowers test with success rate larger than $1-\epsilon$. It follows that the success rate for each of the subtests is larger than $1-(2^k+1)\epsilon$. Note that in the Linearity consistency subtest only 1 bit of the 2^k-1 bits answer of player 1 is relevant for the subtest. As such, we introduce 2^k-1 observables associated to a projective measurement, each corresponding to a bit in the 2^k-1 bits answer. For an 2^n-outcome projective measurement $G = \sum_{j\in\{0,1\}^n} \lambda_j G^j$, where $(G^j)_{j\in\{0,1\}^n}$ are projectors that sum to identity, we define for $i = 1, \ldots, n$:

$$G_i := \sum_{j\in\{0,1\}^n} (-1)^{j\cdot u_i} G^j,$$

where u_i is the n-tuple with value 1 only at position i. Let us fix a bijection $\Omega \leftrightarrow \{1, \ldots, 2^k\}$, so that we can use both $i \in \{1, \ldots, 2^k\}$ and $\omega \in \Omega$ as labels. Note that these observables commute pairwise and that their product is

$$G_1 \cdots G_n = \sum_{j\in\{0,1\}^n} (-1)^{j\cdot\overline{1}} G^j.$$

which corresponds to a measurement of product of the 2^k-1 bits answer. The success rates of the subtests each imply a 'closeness' relation between related observables. For functions $A, B : Z^{k+1} \to M_{d\times d}(\mathbb{C})$ we define the closeness relation $A \approx_\epsilon B$, which holds if and only if

$$\mathop{\mathbb{E}}_{x,h_1,\ldots,h_k} \|A - B\|_f^2 \leq \epsilon,$$

where $\|\cdot\|_f$ denotes the Frobenius matrix norm. The relations we obtain from the subtests are the following:

- *Parallel consistency*: $F(x) \otimes I \approx_{O(\epsilon)} I \otimes \tilde{F}(x)$,
- *Linearity consistency ω*: $F(c_\omega) \otimes I \approx_{O(\epsilon)} I \otimes \tilde{G}_\omega(c_{\Omega\setminus\overline{1}})$ and $G_\omega(c_{\Omega\setminus\overline{1}}) \otimes I \approx_{O(\epsilon)} I \otimes \tilde{F}(c_\omega)$,
- *Gowers norm*: $F(c_{\overline{1}}) \otimes I \approx_{O(\epsilon)} I \otimes \tilde{G}_1(c_{\Omega\setminus\overline{1}}) \cdots \tilde{G}_n(c_{\Omega\setminus\overline{1}})$ and $G_1(c_{\Omega\setminus\overline{1}}) \cdots G_n(c_{\Omega\setminus\overline{1}}) \otimes I \approx_{O(\epsilon)} I \otimes \tilde{F}(c_{\overline{1}})$.

In the relations above, the arguments in the functions should be interpreted as a composition. For example, $F(c_\omega)$ denotes the map $(x, h_1, \ldots, h_k) \mapsto F(c_\omega)$. We derive the first relation below, the others are analogous.

$$
\begin{aligned}
\|F(x)\otimes I - I\otimes \tilde{F}(x)\|_f^2 &\leq \sum_{a=\pm 1} \|F(x)^a\otimes I - I\otimes \tilde{F}(x)^a\|_f^2 \\
&= \sum_{a=\pm 1} \|(F(x)^a\otimes I - I\otimes \tilde{F}(x)^a)\frac{1}{\sqrt{d}}\sum_{i=1}^{d} e_i\otimes e_i\|^2 \\
&= \sum_{a=\pm 1}\frac{1}{d}\sum_{i,j=1}^{d}(\langle F(x)^a e_i\otimes e_i, F(x)^a e_j\otimes e_j\rangle + \langle e_i\otimes \tilde{F}(x)^a e_i, e_j\otimes \tilde{F}(x)^a e_j\rangle \\
&- \langle F(x)^a e_i\otimes e_i, e_j\otimes \tilde{F}(x)^a e_j\rangle - \langle e_i\otimes \tilde{F}(x)^a e_i, F(x)^a e_j\otimes e_j\rangle) \\
&= \sum_{a=\pm 1}\frac{1}{d}\sum_{i=1}^{d}(e_i^* F(x)^a e_i + e_i^*\tilde{F}(x)^a e_i) \\
&- \sum_{a=\pm 1}\frac{1}{d}\sum_{i,j=1}^{d}(e_i^* F(x)^a e_j e_i^*\tilde{F}(x)^a e_j + e_i^* F(x)^a e_j e_i^*\tilde{F}(x)^a e_j) \\
&= \frac{1}{d}(\mathrm{Tr}(I)+\mathrm{Tr}(I)) - 2\sum_{a=\pm 1}\frac{1}{d}\mathrm{Tr}(F(x)^a\tilde{F}(x)^a) \\
&= 2 - 2\sum_{a=\pm 1}\frac{1}{d}\mathrm{Tr}(F(x)^a\tilde{F}(x)^a).
\end{aligned}
$$

We recognise this last sum as the probability that Alice and Bob give the same answer in the Parallel consistency subtest, given that it was played with question x. Upon taking the expectation over possible questions we obtain:

$$
\mathop{\mathbb{E}}_{x,h_1,h_2}\|F(x)\otimes I - I\otimes\tilde{F}(x)\|_f^2 \leq 2 - 2(1-(2^k+1)\epsilon) = (2^{k+1}+2)\epsilon,
$$

as desired.

To proceed, we will use that the closeness relation $\approx_{O(\epsilon)}$ is transitive via the triangle inequality. This allows us to reduce relations about observables on different subsystems (as obtained from all subtests but the Parallel consistency subtest) to relations about observables on the same subsystem by switching the players around via $F(x)\otimes I \approx_{O(\epsilon)} I\otimes\tilde{F}(x)$. In case of the Linearity consistency ω subtests, this gives:

$$
\begin{aligned}
&F(c_\omega)\otimes I \approx_{O(\epsilon)} I\otimes\tilde{F}(c_\omega) \approx_{O(\epsilon)} G_\omega(c_{\Omega\setminus\overline{1}})\otimes I \\
\implies &F(c_\omega)\otimes I \approx_{O(\epsilon)} G_\omega(c_{\Omega\setminus\overline{1}})\otimes I.
\end{aligned}
$$

Writing out the squared norm in the definition of the closeness relation then gives us

$$
\mathop{\mathbb{E}}_{x,h_1,\ldots,h_k}\langle F(c_\omega)\otimes I, G_\omega(c_{\Omega\setminus\overline{1}})\otimes I\rangle_f \geq 1 - O(\epsilon),
$$

which in turn gives us

$$
\mathop{\mathbb{E}}_{x,h_1,\ldots,h_k}\langle F(c_\omega), G_\omega(c_{\Omega\setminus\overline{1}})\rangle_f \geq 1 - O(\epsilon).
$$

Here we have used the relation obtained from the Parallel consistency subtest as $F(c_\omega)\otimes I \approx_{O(\epsilon)} I\otimes\tilde{F}(c_\omega)$ instead of $F(x)\otimes I \approx_{O(\epsilon)} I\otimes\tilde{F}(x)$. It is still valid because when $x, h_1, \ldots, h_d$ are chosen uniformly in Z, the sums c_ω are also uniformly distributed in Z. In total, we have the following correlations:

$$
\begin{aligned}
\mathop{\mathbb{E}}_{x,h_1,\ldots,h_k}\langle G_\omega(c_{\Omega\setminus\overline{1}}), F(c_\omega)\rangle_f &\geq 1 - O(\epsilon), \quad \text{for} \quad \omega\in\Omega\setminus\overline{1}, \\
\mathop{\mathbb{E}}_{x,h_1,h_2}\langle G_1(c_{\Omega\setminus\overline{1}})\cdots G_n(c_{\Omega\setminus\overline{1}}), F(c_{\overline{1}})\rangle_f &\geq 1 - O(\epsilon).
\end{aligned}
$$

Let us now fix a query and write $G_i := G_i(c_{\Omega\setminus\overline{1}})$ for $i = 1,\ldots,2^k-1$ and $F_j := F(c_j)$ for $j = 1,\ldots,2^k$. We can then use the triangle-inequality as follows:

$$
\begin{aligned}
&\|F_1\cdots F_{2^k-1} - F_{2^k}\|_f^2 \\
=&\|(F_1-G_1)F_2\cdots F_{2^k-1} + G_1(F_2-G_2)F_3\cdots F_{2^k-1} \\
&+\ldots + G_1\cdots G_{2^k-2}(F_{2^k-1}-G_{2^k-1}) + G_1\cdots G_{2^k-1} - F_{2^k}\|_f^2 \\
\leq& 2^k[\|(F_1-G_1)F_2\cdots F_{2^k-1}\|_f^2 + \|G_1(F_2-G_2)F_3\cdots F_{2^k-1}\|_f^2 \\
&+\ldots + \|G_1\cdots G_{2^k-2}(F_{2^k-1}-G_{2^k-1})\|_f^2 + \|G_1\cdots G_{2^k-1} - F_{2^k}\|_f^2].
\end{aligned}
$$

Expanding the squared norms and using that the dimension-normalized Frobenius norm of an observable is 1 and that this norm is invariant under unitary transformations, we find:

$$2 - 2\langle F_1 \cdots F_{2^k-1}, F_{2^k}\rangle_f \leq 2^{2k+1} - 2^{k+1}[\langle F_1, G_1\rangle_f + \ldots + \langle F_{2^k-1}, G_{2^k-1}\rangle_f + \langle G_1 \cdots G_{2^k-1}, F_{2^k}\rangle_f],$$

which gives:

$$\langle F_1 \cdots F_{2^k-1}, F_{2^k}\rangle_f \geq 1 - 4^k + 2^k[\langle F_1, G_1\rangle_f + \ldots + \langle F_{2^k-1}, G_{2^k-1}\rangle_f + \langle G_1 \cdots G_{2^k-1}, F_{2^k}\rangle_f].$$

Taking expectations, and applying the correlations gives the result:

$$\|F\|_{U^k}^{2^k} = \mathop{\mathbb{E}}_{x,h_1,\ldots,h_k} \left\langle \prod_{i=1}^{2^k-1} F(c_i), F(c_{2^k}) \right\rangle_f \geq 1 - O(\epsilon).$$

□

6 Discussion and conclusions

This work set out to present and analyse a quantum self-test which can certify that measurements of a quantum device employed in the test have a large U^k norm, when interpreted as a function from a group of labels to unitary measurement matrices. This Gowers test protocol was described in the setting of a two-player game, in which two isolated parties receive queries from a verifier, and are required to provide classical answers. The players are assumed to produce their answer by performing measurements on their respective subsystems of a maximally entangled bipartite state.

The protocol consists of $2^k + 1$ subtests, that the verifier executes with equal probability. The first is a Parallel consistency subtest in which both players receive the same question and are required to submit a 1 bit answer, used to ensure that the strategies of the players is nearly identical. Additionally, the test includes $2^k - 1$ Linearity consistency subtests, in which one player is expected to submit a $2^k - 1$ bits answer, and the other a 1 bit answer. This test is used to verify consistency between the 1 bit answer and components of the $2^k - 1$ bit answer. The last subtest forms the essence of the Gowers test. It ensures that the product of the $2^k - 1$ answer matches the answer of the other player, resulting in a large Frobenius inner product of the observables used in measurement.

It was established that the Gowers test protocol forms a sound test for verification of large Gowers norm strategies. Strategies with a success rate larger than $1 - \epsilon$ were shown to have a Gowers norm of at least $\|F\|_{U^k}^{2^k} \geq 1 - O(\epsilon)$. The proof makes use of a closeness relation, which states that measurements performed upon certain queries are expected to behave similarly. This implies a set of correlations between the strategies, from which it can be concluded that Gowers norm of the strategy function must satisfy a lower bound of $1 - O(\epsilon)$.

The analysis assumes a setting in which players make use of a maximally entangled bipartite state, resulting in strong correlations between strategies. This work does not consider a setting in which players make use of a more general quantum state. For such a setting, the analysis should be adapted by describing the correlation in a different inner product. The suitable inner product would then be a trace matrix inner-product specified by a positive-definite matrix that is related to the quantum state.

The Gowers test protocol presented in this work has been formulated in the setting of an Abelian group. A generalisation towards non-Abelian groups requires an adaptation of the Gowers norm, cf. [4]. This Gowers norm for functions on a non-Abelian group averages over slightly different subsets of the group, as one has to specify the order of group operations in this setting. In order to modify the test for functions on non-Abelian groups, the distribution on group elements in the test has to be changed accordingly.

It is presently unclear what further conclusions can be drawn about functions with a large U^k norm, as inverse theorems for higher order Gowers norms on matrix-valued functions are presently not available. As such, the implications of successfully passing the Gowers test remain somewhat limited. In contrast, inverse theorems for higher order Gowers norms on scalar-valued functions have recently been established. Generalising these results to the matrix-valued case would be a fruitful area for further work.

References

[1] Peter W Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM review* 41.2 (1999), pp. 303–332.

[2] John S Bell. "On the einstein podolsky rosen paradox". In: *Physics Physique Fizika* 1.3 (1964), p. 195.

[3] Dominic Mayers and Andrew Yao. "Self testing quantum apparatus". In: *arXiv preprint quant-ph/0307205* (2003).

[4] William Timothy Gowers and Omid Hatami. "Inverse and stability theorems for approximate representations of finite groups". In: *Sbornik: Mathematics* 208.12 (2017), p. 1784.

[5] Ben Green, Terence Tao, and Tamar Ziegler. "An inverse theorem for the Gowers U s+ 1 [N]-norm". In: *Annals of Mathematics* (2012), pp. 1231–1372.

[6] Thomas Vidick. unpublished. Avalailable at `http://users.cms.caltech.edu/~vidick/pauli_braiding_1.pdf`.

[7] Terence Tao and Van H Vu. *Additive combinatorics*. Vol. 105. Cambridge University Press, 2006.

[8] Anand Natarajan and Thomas Vidick. "Robust self-testing of many-qubit states". In: *arXiv preprint arXiv:1610.03574* (2016).