Abstract — We show that the value of the \( n \)-fold repeated GHZ game is at most \( 2^{-\Omega(n)} \), improving upon the polynomial bound established by Holmgren and Raz. Our result is established via a reduction to approximate subgroup type questions from additive combinatorics. 

Index Terms — Parallel Repetition, GHZ game, Abelian Embeddings, Analysis of Boolean functions, Additive Combinatorics

I. INTRODUCTION

The GHZ game is a 3-player game in which a verifier samples a triplet \((x, y, z)\) uniformly from \( S = \{(x, y, z) \mid x, y, z \in \{0, 1\}, x \oplus y \oplus z = 0 \pmod{2}\} \), then sends \( x \) to Alice, \( y \) to Bob and \( z \) to Charlie. The verifier receives from each one of them a bit, \( a \) from Alice, \( b \) from Bob and \( c \) from Charlie, and accepts if and only if \( a \oplus b \oplus c = x \lor y \lor z \). It is easy to prove that the value of the GHZ game, \( \text{val}(\text{GHZ}) \), defined as the maximum acceptance probability of the verifier over all strategies of the players, is \( 3/4 \). The \( n \)-fold repeated GHZ game is the game in which the verifier samples \((x_i, y_i, z_i)\) independently from \( S \) for \( i = 1, \ldots, n \), sends \( \vec{x} = (x_1, \ldots, x_n) \), \( \vec{y} = (y_1, \ldots, y_n) \) and \( \vec{z} = (z_1, \ldots, z_n) \) to Alice, Bob and Charlie respectively, receives vector answers \( f(\vec{x}) = (f_1(\vec{x}), \ldots, f_n(\vec{x})) \), \( g(\vec{y}) = (g_1(\vec{y}), \ldots, g_n(\vec{y})) \) and \( h(\vec{z}) = (h_1(\vec{z}), \ldots, h_n(\vec{z})) \) and accepts if and only if \( f_i(\vec{x}) \oplus g_i(\vec{y}) \oplus h_i(\vec{z}) = x_i \lor y_i \lor z_i \) for all \( i = 1, \ldots, n \). What can one say about the value of the \( n \)-fold repeated game, \( \text{val}(\text{GHZ}^\otimes n) \)? As for lower bounds, it is clearly that case that \( \text{val}(\text{GHZ}^\otimes n) \geq (3/4)^n \) and one expects that value of the game to be exponentially decaying with \( n \). Proving such upper bounds though is significantly more challenging.

The GHZ game is a prime example of a 3-player game for which parallel repetition is not well understood. For 2-player games, parallel repetition theorems with an exponential decay have been known for a long time [14], [9], [13], [2], [4], and in fact the state of the art parallel repetition theorems for 2-player games are essentially optimal. As for multi-player games, Verbitsky showed [18] that the value of the \( n \)-fold repeated game approaches 0, however his argument uses the density Hales-Jewett theorem and hence gives a weak rate of decay (inverse Ackermann type bounds in \( n \)). More recently, researchers have been trying to investigate multi-player games more systematically and managed to prove an exponential decay for a certain class of games known as expanding games [3]. This work also identified the GHZ game as a bottleneck for current technique, saying that, in a sense, the GHZ game exhibits the worst possible correlations between questions for which existing information-theoretic techniques are incapable of handling.

A sequence of recent works [10] (subsequently simplified by [5]) managed to prove stronger parallel repetition theorems for the GHZ game, and indeed as suggested by [3] this development led to a parallel repetition theorem for a certain class of 3-player games [6], [7], namely for the class of games with binary questions. Quantitatively, they showed that \( \text{val}(\text{GHZ}^\otimes n) \leq 1/n^{\Omega(1)} \), and subsequently that for any 3-player game \( G \) with \( \text{val}(G) < 1 \) whose questions are binary, one has that \( \text{val}(G^\otimes n) \leq 1/n^{\Omega(1)} \). The techniques utilized by these works is a combination of information theoretic techniques (as used in the case of 2-player games) and Fourier analytic techniques.

A. Our Result

The main result of this paper is an improved upper bound for the value of the \( n \)-fold repeated GHZ game, which is exponential in \( n \). More precisely:

**Theorem I.1.** There is \( \varepsilon > 0 \) such that for all \( n \), \( \text{val}(\text{GHZ}^\otimes n) \leq 2^{-\varepsilon n} \).

Such bounds cannot be achieved by the methods of [10], [5], [6], [7], and we hope that the observations made herein would be useful towards getting better parallel repetition theorems for more general classes of 3-player games.

B. Proof Idea

Our proof of Theorem I.1 follows by reducing it to approximate sub-group type questions from additive combinatorics, and our argument uses results of Gowers [8]. Similar ideas have been also explored in the TCS community (for example, by Samorodnitsky [16]).

Suppose \( f: \{0, 1\}^n \rightarrow \{0, 1\}^n \), \( g: \{0, 1\}^n \rightarrow \{0, 1\}^n \) and \( h: \{0, 1\}^n \rightarrow \{0, 1\}^n \) represent the strategies of Alice, Bob and Charlie respectively, and denote their success probability by \( \eta \). Thus, we have that

\[
\Pr_{(x,y,z) \in S^n} [f(x) \oplus g(y) \oplus h(z) = x \lor y \lor z] \geq \eta, \quad (1)
\]
where the operations are coordinate-wise. Using Cauchy-Schwarz it follows that if we sample \( x, y, z \) and \( u, v, w \) conditioned on \( x \lor y \land z = u \lor v \lor w \), then \( f(x) \oplus g(y) \oplus h(z) = f(u) \oplus g(v) \oplus h(w) \) with probability at least \( \eta^2 \), hence \( f(x) \oplus f(u) \oplus g(y) \oplus g(v) \oplus h(z) \oplus h(w) = 0 \). What functions \( f, g, h \) can satisfy this? We draw an intuition from [1], that suggested that such advantage can only be gained from linear embeddings. In this respect, we are looking at the predicate \( P: \Sigma^3 \to \{0,1\} \) with alphabet \( \Sigma = \{0,1\}^2 \) defined as \( P((x,u),(y,v),(z,w)) = 1 \) if \( x \lor y \land z = u \lor v \lor w \), \( x+y+z = 0 \) and \( u+v+w = 0 \). A linear embedding is an Abelian group \((A,+)\) and a collection of maps \( \phi: \Sigma \to A, \gamma: \Sigma \to A \) and \( \delta: \Sigma \to A \) not all constant such that \( \phi(x,u) + \gamma(y,v) + \delta(z,w) = 0 \). There are 2 trivial linear embeddings into \((\mathbb{Z}_2^3,+)\); the projection onto the first coordinate as well as the projection onto the second coordinate. Thus, one is tempted to guess that in the above scenario, the functions \( f, g, h \) must use these linear embeddings and thus be correlated with linear functions over \( \mathbb{Z}_2^3 \). Alas, it turns out that there is yet another embedding which is less obvious: taking \((A,+)=(\mathbb{Z}_4^3,+), \phi(x,u) = x+u, \gamma(y,v) = y+v \) and \( \delta(z,w) = z+w \). This motivates us to look at the original problem and see if we can already see \((\mathbb{Z}_4^3,+)\) structure there.

**a)** Approximate Homomorphisms. For \((x, y, z) \in S\), if \( x \lor y \land z = 1 \), then exactly two of the variables are 1; if \( x \lor y \land z = 0 \), then all of \( x, y, z \) are 0. Thus, one can see that the check we are making is equivalent to checking that \( 2f(x) + 2g(y) + 2h(z) = x + y + z \) (mod 4). Indeed, on a given coordinate \( i \), if \( (x_i \lor y_i \land z_i) = 1 \), then \( x_i + y_i + z_i = 2 \) and the answers need to satisfy that \( f(x_i) + g(y_i) + h(z_i) = 1 \) (mod 2) which implies \( 2f(x_i) + 2g(y_i) + 2h(z_i) = 2 \) (mod 4). Similarly, if \( (x_i \lor y_i \land z_i) = 0 \) then \( x_i + y_i + z_i = 0 \) and the constraint says that we want \( f(x_i) + g(y_i) + h(z_i) = 0 \) (mod 2) which implies that \( 2f(x_i) + 2g(y_i) + 2h(z_i) = 0 \) (mod 4). Thus, the GHZ test can be thought of as a system of equations modulo 4, as suggested by the above intuition. More precisely, defining \( F: \mathbb{Z}_4^3 \to \mathbb{Z}_4^3 \) by \( F(x_i) = 2f(x_i) - x_i \) and similarly \( G, H: \mathbb{Z}_4^3 \to \mathbb{Z}_4^3 \) by \( G(y_i) = 2g(y_i) - y_i \) and \( H(z_i) = 2h(z_i) - z_i \), we have the following lemma:

**Lemma 1.2.** For each \( x, y, z \in S^n \), \( F(x) + G(y) + H(z) = 0 \) (mod 4) if and only if \( f(x_i) \oplus g(y_i) \oplus h(z_i) = x_i \lor y_i \lor z_i \) for all \( i = 1, \ldots, n \). Consequently, \( \Pr_{(x,y,z) \in S^n} [F(x) + G(y) + H(z) = 0 \text{ (mod 4)}] \geq \eta \).

**Proof.** Without loss of generality we focus on the first coordinate. If \( (x_1, y_1, z_1) = (0,0,0) \), then by (1) we get that \( f(x_1) \oplus g(y_1) \oplus h(z_1) = 0 \), hence either all of them are 0 or exactly two of them are 1, and in any case \( 2f(x_1) + 2g(y_1) + 2h(z_1) = 0 \) (mod 4). Otherwise, without loss of generality \( (x_1, y_1, z_1) = (1,1,0) \), and then by (1) we get \( f(x_1) \oplus g(y_1) \oplus h(z_1) = 1 \), and there are two cases. If \( f(x_1) = g(y_1) = h(z_1) = 1 \), then we get that \( F(x_1) + G(y_1) + H(z_1) = 2 - 1 + 2 - 1 + 2 + 0 = 0 \) (mod 4). Else, exactly one of them is 1, say \( f(x_1) = 1 \) and \( g(y_1) = h(z_1) = 0 \), and then \( F(x_1) + G(y_1) + H(z_1) = 2 - 1 + 0 - 0 + 0 - 0 = 0 \).

In words, Lemma 1.2 says that \( F, G, H \) form an approximate “cross homomorphism” from \( \mathbb{Z}_2^3 \) to \( \mathbb{Z}_4^3 \). Once we have made this observation, the proof is concluded by a routine application of powerful tools from additive combinatorics.

More specifically, we appeal to results of Gowers and show for any \( F \) that satisfies Lemma 1.2 (for some \( G \) and \( H \)) must exhibit some weak linear behaviour. Specifically, we show that for such \( F \) there is a shift \( s \in \mathbb{Z}_4^3 \) such that \( F(x) \in s + \{0,2\}^n \) for at least \( \eta = \Omega(\eta^{10/24}) \) fraction of inputs. On the other hand, on such points \( x \) we get that \( 2f(x) - x = F(x) = s + L(x) \) for some \( L(x) \in \{0,2\}^n \), and noting that this must hold modulo 2 we get that there can only be one such point, \( x = -s \) (mod 2). Thus, \( \eta \leq 2^{-n} \), giving an exponential bound on \( \eta \).

**II. PROOF OF THEOREM 1.1**

**A. From Testing to Additive Quadruples**

We need the following definition:

**Definition 1.1.** Let \( (A,+),(B,+),(C,) \) be Abelian groups, and let \( F: A^n \to B^n \). We say \( x,y,u,v \in A^n \times A^n \times A^n \times A^n \) is an additive quadruple if \( x+y = u+v \) and \( F(x)+F(y) = F(u)+F(v) \).

In our application, we will always have \( A = \{0,1\} \). For convenience we denote \( N = 2^n \). Thus, it is clear that the number of additive quadruples is always at most \( N^3 \) (as this is the number of solutions to \( x+y = u+v \)). The following lemma asserts that if \( F,G,H: \{0,1\}^n \to B^n \) are functions such that \( F(x) + G(y) + H(z) = 0 \) for at least \( \eta \) of the triples \( x,y,z \) satisfying \( x \oplus y = z \) (as such the one given in Lemma 1.2), then each one of the functions \( F,G,H \) has a substantial amount of additive quadruples.

**Lemma 1.2.** Suppose that \( F,G,H: \{0,1\}^n \to B^n \) satisfy

\[
\Pr_{(x,y,z) \in S^n} [F(x) + G(y) + H(z) = 0] \geq \eta. 
\]

Then \( F \) has at least \( \eta^4 N^3 \) additive quadruples.

**Proof.** By the premise and Cauchy-Schwarz:

\[
\eta^2 = \mathbb{E}_y \left[ \mathbb{E}_x \left[ 1_{G(y) = -F(x) - H(x \oplus y)} \right] \right]^2 \\
\leq \mathbb{E}_y \left[ \mathbb{E}_x \left[ 1_{G(y) = -F(x) - H(x \oplus y)} \right] \right]^2 \\
= \mathbb{E}_{x,x',y} \left[ 1_{G(y) = -F(x) - H(x \oplus y)} 1_{G(y) = -F(x') - H(x' \oplus y)} \right] \\
\leq \mathbb{E}_{x,x',y} \left[ 1_{F(x) - F(x') = H(x' \oplus y) - H(x \oplus y)} \right].
\]

Making change of variables, we get that \( \eta^2 \leq \mathbb{E}_{x,u,u'} \left[ 1_{F(x) - F(x \oplus u) = H(u') - H(u)} \right] \). Squaring and
using Cauchy-Schwarz again we get that
\[
\eta^4 \leq \mathbb{E}_{x,u,u'} \left[ \frac{1}{F(x)-F(x\oplus u\oplus u')} - H(u') - H(u) \right]^2 \\
\leq \mathbb{E}_{u,u'} \left[ \frac{1}{F(x)-F(x\oplus u\oplus u')} - H(u') - H(u) \right] \\
\leq \mathbb{E}_{x,x'} \left[ \frac{1}{F(x)-F(x\oplus u\oplus u')} - F(x') - F(x'\oplus u\oplus u') \right],
\]
which by another change of variables is equal to
\[
\mathbb{E}_{x,y,u,u',x+y=x+u} \left[ \frac{1}{F(x)+F(y)=F(u)+F(v)} \right],
\]
and the claim is proved. \(\square\)

B. From Additive Quadruples to Linear Structure

We intend to use Lemma II.2 to conclude a structural result for \(F\), and towards this end we show that a function that has many additive quadruples must exhibit some linear structure. The content of this section is a straight-forward combination of well-known results in additive combinatorics, and we include it here for the sake of completeness. We need the notions of Freiman homomorphism, sum-sets and a result of Gowers [8].

We begin with two definitions:

Definition II.3. Let \((A,+)\) and \((B,+)\) be Abelian groups, let \(n \in \mathbb{N}\) and let \(A \subseteq A^n\). A function \(\phi: A \to B^n\) is called a Freiman homomorphism of order \(k\) if for all \(a_1, \ldots, a_k \in A\) and \(b_1, \ldots, b_k \in B\) such that \(a_1 + \ldots + a_k = b_1 + \ldots + b_k\) it holds that
\[
\phi(a_1) + \ldots + \phi(a_k) = \phi(b_1) + \ldots + \phi(b_k).
\]

Definition II.4. Let \((A,+)\) be an Abelian group, let \(n \in \mathbb{N}\) and let \(A, B \subseteq A^n\). We define
\[
A + B = \{a + b \mid a \in A, b \in B\}.
\]

If \(A = B\), we denote the sum-set \(A + B\) more succinctly as \(2A\), and more generally \(kA\) denotes the \(k\)-fold sum set of \(A\).

We need a result of Gowers [8] asserting that a function \(F\) with many additive quadruples can be restricted to a relatively large set and yield a Freiman homomorphism. Gowers states and proves the statement for \(Z_N\), and we adapt his proof for our setting. For the proof we need two notable results in additive combinatorics. The first of which is the Balog-Szemerédi-Gowers theorem, and we use the version from [17]:

Theorem II.5 (Balog-Szemerédi-Gowers). Let \(G\) be an Abelian group, and suppose that \(\Gamma \subseteq G\) contains at least \(\xi |\Gamma|^3\) additive quadruples, that is,
\[
\left| \{(x, y, z, w) \in \Gamma^4 \mid x + y = z + w \} \right| \geq \xi |\Gamma|^3.
\]
Then there exists \(\Gamma' \subseteq \Gamma\) of size at least \(\Omega(\xi |\Gamma|)\) such that \(|\Gamma' - \Gamma'| \leq O(\xi^{-4} |\Gamma'|)\).

The second result we need is Plünnecke’s inequality [12], [15] (see also [11]):

Theorem II.6 (Plünnecke’s inequality). Let \(G\) be an Abelian group, and suppose that \(\Gamma \subseteq G\) has \(|\Gamma - \Gamma| \leq C |\Gamma|\). Then \(|m\Gamma - r\Gamma| \leq C^{m+r} |\Gamma|\).

Lemma II.7 (Corollary 7.6 in [8]). Let \(n \in \mathbb{N}\), and suppose that a function \(\phi: Z_4^n \to Z_4^n\) has at least \(\xi |Z_4^n|^3\) additive quadruples. Then there exists \(\mathcal{A} \subseteq Z_4^n\) such that \(\phi|\mathcal{A}\) is a Freiman homomorphism of order 8 and \(|\mathcal{A}| \geq \Omega(\xi^{257} |Z_4^n|)\).

Proof. Let \(\Gamma = \{(x, \phi(x)) \mid x \in Z_4^n\}\) be the graph of \(\phi\), and think of it as a set in the Abelian group \(Z_4^n \times Z_4^n\). Then \(\Gamma\) contains at least \(\xi |Z_4^n|^3 = \xi |\Gamma|^3\) solutions to \(\gamma_1 + \gamma_2 = \gamma_3 + \gamma_4\), hence by Theorem II.5 we may find \(\Gamma' \subseteq \Gamma\) such that \(|\Gamma' - \Gamma'| \geq \Omega(\xi^{-4} |\Gamma'|)\). By Theorem II.6 we get that \(|16\Gamma - 16\Gamma'| \leq O(\xi^{-32} |\Gamma'|) \leq C \cdot |\Gamma'|\) where \(C = \Omega(\xi^{-128})\).

Let \(\mathcal{Y} = \{ y \in Z_4^n \mid (0, y) \in 8\Gamma' - 8\Gamma'\}\); we claim that \(|\mathcal{Y}| \leq C\) and towards contradiction we assume the contrary.

First, note that we may choose \(|\Gamma'|\) distinct values of \(x\) such that \((x, w_x) \in 8\Gamma' - 8\Gamma'\) for some \(w_x\). Indeed, we can fix any 15 elements \((x_i, w_i) \in \Gamma'\) for \(i = 1, \ldots, 15\), and range over all \(|\Gamma'|\) pairs \((x, w_x) \in \Gamma'\) to get \(|\Gamma'|\) elements \((x + x' - x\ominus w_x + \omega - w') \in 8\Gamma' - 8\Gamma'\) where \(x' = x_1 + \ldots + x_7, x'' = x_8 + \ldots + x_{15}\) and \(w' = w_1 + \ldots + w_7\) and \(w'' = w_8 + \ldots + w_{15}\), which have distinct first coordinate. Thus, looking at the \(|\Gamma'|\) elements \((x, w_x) \in 8\Gamma' - 8\Gamma'\) with distinct first coordinate, we get that \((x, w_x + y) \in 16\Gamma' - 16\Gamma'\) for all \(x, y \in \mathcal{Y}\), hence \(|16\Gamma' - 16\Gamma'| > C |\Gamma'|\), in contradiction. The set \(\mathcal{Y}\) will be useful for us as for any \(x \in \mathcal{Z}_4^n\), we may define \(\mathcal{Y}_x = \{ y \mid (x, y) \in 4\Gamma' - 4\Gamma'\}\) and get that \(\mathcal{Y}_x - \mathcal{Y}_x \subseteq \mathcal{Y}\).

Take \(t = \log(C) + 1\), choose \(I_1, \ldots, I_t \subseteq [n]\) independently and uniformly and consider
\[
\mathcal{W} = \left\{ y \in Z_4^n \mid \sum_{j \in I_i} y_j = 0 \forall i = 1, \ldots, t \right\}.
\]

We note that the 0 vector is always in \(\mathcal{W}\), but any other \(y \in \mathcal{Z}_4^n\) is in \(\mathcal{W}\) with probability at most \(2^{-t}\). Indeed, if \(y\)’s entries are all \(\{0, 2\}\)-valued then \(y\) can be in \(\mathcal{W}\) only if \(y/2\) satisfies \(t\) randomly chosen equations modulo 2, which happens with probability \(2^{-t}\). If there are entries of \(y\) that are either 1 or 3, then we get that \(y \mod 2\) is a non-zero vector that must satisfy \(t\) randomly chosen equations modulo 2, which happens with probability \(2^{-t}\). Thus, \(\mathbb{E} |\mathcal{Y} \cap \mathcal{W} \setminus \{0\}| \leq 2^{-t} |\mathcal{Y}| < 1\), so we may choose \(\mathcal{W}\) such that \(|\mathcal{Y} \cap \mathcal{W} = \{0\}|\).

For an \(a \in \mathcal{Z}_4^n\) we define \(\mathcal{Y}_a = \{ (x, y) \in \Gamma' \mid y \in a + \mathcal{W} \}\). We claim that there is a choice for \(a\) such that (1) \(|\mathcal{Y}_a| \geq 4^{-t} |\Gamma'\| \geq \Omega(\xi^{257} |Z_4^n|)\), and (2) taking \(\mathcal{A} = \{ x \mid \exists y \text{ such that } (x, y) \in \Gamma' \}\), the function \(\phi|\mathcal{A}\) is a Freiman homomorphism of order 8. Together, this gives the statement of the lemma.
For the first item we have
\[
E_a [\Gamma'_a] = \sum_{(x,y) \in \Gamma'} \Pr_a [y \in a + W] \\
= \sum_{(x,y) \in \Gamma'} \Pr_a [y - a \in W] \\
\geq \sum_{(x,y) \in \Gamma'} 4^{-t} \\
= 4^{-t} [\Gamma'],
\]
so there is an \(a\) such that \(\Gamma'_a \geq 4^{-t} [\Gamma']\), and we show that the second item holds for all \(a\).

Suppose towards contradiction that \(\phi|_A\) is not a Freiman homomorphism of order 8. Thus we can find \(x_1, \ldots, x_8 \in A\) and \(x'_1, \ldots, x'_8 \in A\) that have the same sum yet \(\phi(x_1) + \ldots + \phi(x_8) \neq \phi(x'_1) + \ldots + \phi(x'_8)\). Denoting \(x = x_1 + \ldots + x_8 - x'_8 = x'_1 + \ldots + x'_8 - x_8\), \(y = \phi(x_1) + \ldots + \phi(x_4) - \phi(x'_4)\), and \(y' = \phi(x'_1) + \ldots + \phi(x'_4) - \phi(x_4)\) so that \(y \neq y'\), we get that \((x,y), (x',y') \in 4\Gamma, 4\Gamma_8 \subseteq 4\Gamma - 4\Gamma, \) so \(y, y' \in Y\).

In particular, \(y - y' \in Y\). On the other hand, by choice of \(A\) we get that \(\phi(x_i), \phi(x'_i) \in a + W\) for all \(i\) and so \(y, y' \in 4W - 4W = W\) and \(y - y' \in W\). It follows that \(y - y' \in Y\). Thus we get that there is a shift of \(\{0, 2\}^n\) in which \(F(x)\) lies for many \(x\):

**Lemma II.8.** Let \(A \subseteq Z_8^n\) and suppose that \(\phi: A \rightarrow Z_8^n\) is a Freiman homomorphism of order 4. Then there is \(s \in Z_4^n\) such that for all \(x \in A\), \(\phi(x) \in s + \{0, 2\}^n\).

**Proof.** Choose any \(a \in A\) and let \(s = \phi(a)\). Then for any \(x \in A\), applying the Freiman homomorphism condition on the tuples \((x, x, a, a)\) and \((a, a, a, a)\) that have the same sum over \(Z_8^n\), we get that \(2\phi(x) + 2\phi(a) = 4\phi(a) = 0\), so \(2\phi(x) - s = 0\). This implies that \(\phi(x) - s \in \{0, 2\}^n\), and the proof is concluded.

Combining the last two lemmas we get the following corollary.

**Corollary II.9.** Suppose that \(F: Z_8^n \rightarrow Z_4^n\) is a function for which there are \(G, H: Z_8^n \rightarrow Z_4^n\) such that \(Pr_{x,y,z \in Z_8^n} [F(x) + G(y) + H(z) = 0] \geq \eta\). Then there is \(s \in Z_4^n\) such that
\[
Pr_{x \in Z_8^n} [F(x) \in \{0, 2\}^n + s] \geq \Omega(\eta^{1028} N^4).
\]

**Proof.** By Lemma II.2 we get that \(F\) has at least \(\eta^4N^3\) additive quadruples, so by Lemma II.7 there is \(A \subseteq Z_8^n\) of size at least \(\Omega(\eta^{1028} N^4)\) such that \(F|_A\) is a Freiman homomorphism. Applying Lemma II.8 we conclude that there is \(s \in Z_4^n\) such that \(F(x) \in \{0, 2\}^n\) for all \(x \in A\) and the proof is concluded.

C. Concluding Theorem 1.1

Let \(f, g, h: \{0, 1\}^n \rightarrow \{0, 1\}^n\) be strategies that achieve value at least \(\eta\) in GHZ^{\otimes n}, and define \(F: Z_8^n \rightarrow Z_4^n\) by \(F(x) = 2f(x) - x\) and similarly \(G(y) = 2g(y) - y\) and \(H(z) = 2h(z) - z\). By Lemma I.2 we get that \(Pr_{x,y,z \in Z_8^n} [F(x) + G(y) + H(z) = 0] \geq \eta\), hence by Corollary II.9 there is \(s \in Z_4^n\) such that \(Pr_{x \in Z_2^n} [F(x) \in \{0, 2\}^n + s] \geq \eta'\) for \(\eta' = \Omega(\eta^{1028})\). For any such \(x\), we get that \(2f(x) - x = F(x) = s + L(x)\) where \(L(x) \in \{0, 2\}^n\), and so \(x = s + 2f(x) - L(x)\). Note that this is equality modulo 4 hence it implies it also holds mod 2. We also have that \(2f(x) - L(x) \in \{0, 2\}^n\) so this vanishes modulo 2, hence we get that \(x = s \mod 2\). In other words, there can be at most single \(x\) such that \(F(x) \in \{0, 2\}^n\) and so \(Pr_{x \in Z_2^n} [F(x) \in \{0, 2\}^n] \leq 2^{-n}\). Combining, we get that \(\eta' \leq 2^{-n}\) and so \(\eta \leq 2^{-n/1028} + O(1)\).

Acknowledgements

Author Braverman was supported by NSF Alan T. Waterman Award, Grant No. 1933331, a Packard Fellowship in Science and Engineering, and the Simons Collaboration on Algorithms and Geometry. Author Khot was supported by NSF Award CCF-1422159, NSF Award CCF-2130816, and the Simons Investigator Award. Author Minzer was supported by a Sloan Research Fellowship, NSF CCF award 1157468 and NSF CAREER award 2239160.

References

[1] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-csp-s: 1. In STOC ’22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 – 24, 2022, pages 976–988, 2022.

[2] Mark Braverman and Ankit Garg. Small value parallel repetition for general games. In Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015, pages 335–340. ACM, 2015.

[3] Irit Dinur, Prahladh Harsha, Rakesh Venkat, and Henry Yuen. Multiplayer parallel repetition for expanding games. In 58th Innovations in Theoretical Computer Science Conference, ITCS 2017, January 9-11, 2017, Berkeley, CA, USA, volume 67 of LIPIcs, pages 37:1–37:16, 2017.

[4] Irit Dinur and David Steurer. Analytical approach to parallel repetition. In Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 – June 03, 2014, pages 624–633. ACM, 2014.

[5] Uma Girish, Justin Holmgren, Kunal Mittal, Ran Raz, and Wei Zhan. Parallel repetition for the GHZ game: A simpler proof. In Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2021, August 16–18, 2021, University of Washington, Seattle, Washington, USA (Virtual Conference), volume 207 of LIPIcs, pages 6:1–6:12, 2021.

[6] Uma Girish, Justin Holmgren, Kunal Mittal, Ran Raz, and Wei Zhan. Parallel repetition for all 3-player games over binary alphabet. In STOC ’22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 – 24, 2022, pages 998–1009. ACM, 2022.

[7] Uma Girish, Kunal Mittal, Ran Raz, and Wei Zhan. Polynomial bounds on parallel repetition for all 3-player games with binary inputs. In Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2022, September 19-21, 2022, University of Illinois, Urbana-Champaign, USA (Virtual Conference), volume 245 of LIPIcs, pages 6:1–6:17, 2022.

[8] William T Gowers. A new proof of Szemerédi’s theorem. Geometric & Functional Analysis GAF, 11(3):465–588, 2001.
[9] Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. *Theory Comput.*, 5(1):141–172, 2009.

[10] Justin Holmgren and Ran Raz. A parallel repetition theorem for the GHZ game. *CoRR*, abs/2008.05059, 2020.

[11] Giorgis Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012.

[12] Helmut Plünnecke. Eine zahlentheoretische anwendung der graphentheorie. 1970.

[13] Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM J. Comput.*, 40(6):1871–1891, 2011.

[14] Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, 1998.

[15] Imre Z Ruzsa. An application of graph theory to additive number theory. *Scientia, Ser. A.*, 3(97-109):9, 1989.

[16] Alex Samorodnitsky. Low-degree tests at large distances. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 506–515, 2007.

[17] Tomasz Schoen. New bounds in Balog-Szemeredi-Gowers theorem. *Combinatorica*, 35(6):695–701, 2015.

[18] Oleg Verbitsky. Towards the parallel repetition conjecture. *Theoretical Computer Science*, 157(2):277–282, 1996.