Electronic Colloquium on Computational Complexity, Report No. 167 (2022)

Parallel Repetition for the GHZ Game: Exponential Decay

Mark Braverman *   Subhash Khot†   Dor Minzer‡

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.

1 Introduction

1.1 Multi-player Parallel Repetition and the GHZ Game

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 $a \oplus b \oplus c = x \vee y \vee z$. It is easy to prove that the value of the GHZ game, $\mathsf{val}(\mathsf{GHZ})$, 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 $f_i(\vec{x}) \oplus g_i(\vec{y}) \oplus h_i(\vec{z}) = x_i \vee y_i \vee z_i$ for all $i = 1, \ldots, n$. What can one say about the value of the n-fold repeated game, $\mathsf{val}(\mathsf{GHZ}^{\otimes n})$? As for lower bounds, it is clearly that case that $\mathsf{val}(\mathsf{GHZ}^{\otimes n}) \geqslant (3/4)^n$ 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 managed to prove stronger parallel repetition theorems for the GHZ game [10] (subsequently simplified by [5]), and indeed as suggested by [3] this development led to a parallel repetition

*Department of Computer Science, Princeton University. Research supported in part by the NSF Alan T. Waterman Award, Grant No. 1933331, a Packard Fellowship in Science and Engineering, and the Simons Collaboration on Algorithms and Geometry.

†Courant institute of Mathematical Sciences, New York University. Supported by the NSF Award CCF-1422159, NSF Award CCF-2130816, and the Simons Investigator Award.

‡Department of Mathematics, Massachusetts Institute of Technology. Supported by a Sloan Research Fellowship.

ISSN 1433-8092

theorem for a certain class of 3-player games [6, 7], namely for the class of games with binary questions. Quantitatively, they showed that $\mathsf{val}(\mathsf{GHZ}^{\otimes n}) \leqslant 1/n^{\Omega(1)}$, and subsequently that for any 3-player game G with $\mathsf{val}(G) < 1$ whose questions are binary, one has that $\mathsf{val}(G^{\otimes n}) \leqslant 1/n^{\Omega(1)}$. 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.

1.2 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 1.1. *There is $\varepsilon > 0$ such that for all n,* $\mathsf{val}(\mathsf{GHZ}^{\otimes n}) \leqslant 2^{-\varepsilon \cdot n}$.

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.

1.3 Proof Idea

Our proof of Theorem 1.1 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 $f\colon \{0,1\}^n \to \{0,1\}^n$, $g\colon \{0,1\}^n \to \{0,1\}^n$ and $h\colon \{0,1\}^n \to \{0,1\}^n$ represent the strategies of Alice, Bob and Charlie respectively, and denote their success probability by η. Thus, we have that

$$\Pr_{(x,y,z)\in S^n}\left[f(x)\oplus g(y)\oplus h(z) = x\vee y\vee z\right] \geqslant \eta, \tag{1}$$

where the operations are coordinate-wise. Using Cauchy-Schwarz it follows that if we sample x, y, z and u, v, w conditioned on $x\vee y\vee z = u\vee v\vee w$, then $f(x)\oplus g(y)\oplus h(z) = f(u)\oplus g(v)\oplus h(w)$ with probability at least η^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 $P\colon \Sigma^3 \to \{0,1\}$ with alphabet $\Sigma = \{0,1\}^2$ defined as $P((x,u),(y,v),(z,w)) = 1$ if $x\vee y\vee z = u\vee v\vee w$, $x+y+z = 0$ and $u+v+w = 0$. A linear embedding is an Abelian group $(A,+)$ and a collection of maps $\phi\colon \Sigma\to A$, $\gamma\colon \Sigma\to A$ and $\delta\colon \Sigma\to A$ not all constant such that $\phi(x,u)+\gamma(y,v)+\delta(z,w) = 0$. There are 2 trivial linear embeddings into $(\mathbb{Z}_2,+)$: 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 and h must use these linear embeddings and thus be correlated with linear functions over $\mathbb{Z}_2$. Alas, it turns out that there is yet, another embedding which is less obvious: taking $(A,+) = (\mathbb{Z}_4,+)$, $\phi(x,u) = x+u$, $\gamma(y,v) = y+v$ and $\delta(z,w) = z+w$. This motivates us to look at the original problem and see if we can already see $(\mathbb{Z}_4,+)$ structure there.

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

$$\Pr_{(x,y,z)\in S^n}[F(x) + G(y) + H(z) = 0 \pmod 4] \geqslant \eta.$$

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 $2f(x)_1 + 2g(y)_1 + 2h(z)_1 = 0 \pmod 4$. 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 $F(x)_1 + G(y)_1 + H(z)_1 = 2-1+2-1+2+0 = 0 \pmod 4$. Else, exactly one of them is 1, say $f(x)_1 = 1$ and $g(y)_1 = h(z)_1 = 0$, and then $F(x)_1 + G(y)_1 + H(z)_1 = 2-1+0-1+0-0 = 0$. □

In words, Lemma 1.2 says that F, G, H form an approximate "cross homomorphism" from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4^n$. 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 $s \in \mathbb{Z}_4^n$ such that $F(x) \in s + \{0,2\}^n$ for at least $\eta' = \Omega(\eta^{10^4})$ 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, $x = -s \pmod 2$. Thus, $\eta' \leqslant 2^{-n}$, giving an exponential bound on η.

2 Proof of Theorem 1.1

2.1 From Testing to Additive Quadruples

We need the following definition:

Definition 2.1. *Let $(A, +), (B, +)$ be Abelian groups, and let $F\colon A^n \to B^n$. 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 $F, G, H\colon \{0,1\}^n \to B^n$ are functions such that $F(x) + G(y) + H(z) = 0$ for at least η of the triples x, y, z satisfying $x \oplus y = z$ (such as the one given in Lemma 1.2), then each one of the functions F, G and H has a substaintial amount of additive quadruples.

Lemma 2.2. *Suppose that $F, G, H\colon \{0,1\}^n \to B^n$ satisfy that*

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

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

Proof. By the premise and Cauchy-Schwarz

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

Making change of variables, we get that $\eta^2 \leqslant \mathbb{E}_{x,u,u'} \left[1_{F(x)-F(x\oplus u\oplus u')=H(u')-H(u)} \right]$. Squaring and using Cauchy-Schwarz again we get that

$$\eta^4 \leqslant \mathop{\mathbb{E}}_{x,u,u'} \left[1_{F(x)-F(x\oplus u\oplus u')=H(u')-H(u)} \right]^2 \leqslant \mathop{\mathbb{E}}_{u,u'} \left[\mathop{\mathbb{E}}_x \left[1_{F(x)-F(x\oplus u\oplus u')=H(u')-H(u)} \right]^2 \right]$$
$$\leqslant \mathop{\mathbb{E}}_{u,u'} \left[\mathop{\mathbb{E}}_{x,x'} \left[1_{F(x)-F(x\oplus u\oplus u')=F(x')-F(x'\oplus u\oplus u')} \right] \right],$$

which by another change of variables is equal to $\mathbb{E}_{x,y,u,v:x+y=u+v} \left[1_{F(x)+F(y)=F(u)+F(v)} \right]$, and the claim is proved. □

2.2 From Additive Quadruples to Linear Structure

We intend to use Lemma 2.2 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 2.3. *Let $(A,+)$ and $(B,+)$ be Abelian groups, let $n \in \mathbb{N}$ and let $\mathcal{A} \subseteq A^n$. A function $\phi\colon \mathcal{A} \to B^n$ is called a Freiman homorphism of order k if for all $a_1,\ldots,a_k \in \mathcal{A}$ and $b_1,\ldots,b_k \in \mathcal{A}$ 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 2.4. *Let $(A,+)$ be an Abelian group, let $n \in \mathbb{N}$ and let $\mathcal{A},\mathcal{B} \subseteq A^n$. We define*

$$\mathcal{A}+\mathcal{B} = \{\, a+b \mid a \in \mathcal{A}, b \in \mathcal{B} \,\}.$$

If $\mathcal{A} = \mathcal{B}$, we denote the sum-set $\mathcal{A}+\mathcal{B}$ more succinctly as $2\mathcal{A}$, and more generally $k\mathcal{A}$ denotes the k-fold sum set of $\mathcal{A}$.

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 $\mathbb{Z}_N$, 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 2.5 (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, $\left|\left\{\, (x,y,z,w) \in \Gamma^4 \;\middle|\; x+y=z+w \,\right\}\right| \geqslant \xi\,|\Gamma|^3$. Then there exists $\Gamma' \subseteq \Gamma$ of size at least $\Omega(\xi\,|\Gamma|)$ such that $|\Gamma'-\Gamma'| \leqslant O(\xi^{-4}\,|\Gamma'|)$.*

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

Theorem 2.6 (Plünnecke's inequality)**.** *Let G be an Abelian group, and suppose that $\Gamma \subseteq G$ has $|\Gamma - \Gamma| \leqslant C|\Gamma|$. Then $|m\Gamma - r\Gamma| \leqslant C^{m+r}|\Gamma|$.*

Lemma 2.7 (Corollary 7.6 in [8])**.** *Let $n \in \mathbb{N}$, and suppose that a function $\phi\colon \mathbb{Z}_2^n \to \mathbb{Z}_4^n$ has at least $\xi|\mathbb{Z}_2^n|^3$ additive quadruples. Then there exists $\mathcal{A} \subseteq \mathbb{Z}_2^n$ such that $\phi|_{\mathcal{A}}$ is a Freiman homomorphism of order 8 and $|\mathcal{A}| \geqslant \Omega(\xi^{257}|\mathbb{Z}_2^n|)$.*

Proof. Let $\Gamma = \{(x, \phi(x)) \mid x \in \mathbb{Z}_2^n\}$ be the graph of ϕ, and think of it as a set in the Abelian group $\mathbb{Z}_2^n \times \mathbb{Z}_4^n$. Then Γ contains at least $\xi|\mathbb{Z}_2^n|^3 = \xi|\Gamma|^3$ solutions to $\gamma_1 + \gamma_2 = \gamma_3 + \gamma_4$, hence by Theorem 2.5 we may find $\Gamma' \subseteq \Gamma$ such that $|\Gamma'| \geqslant \Omega(\xi|\Gamma|)$ and $|\Gamma' - \Gamma'| \leqslant O(\xi^{-4}|\Gamma'|)$. By Theorem 2.6 we get that $|16\Gamma' - 16\Gamma'| \leqslant O(\xi^{-32\cdot 4}|\Gamma'|) \leqslant C \cdot |\Gamma'|$ where $C = O(\xi^{-128})$.

Let $\mathcal{Y} = \{y \in \mathbb{Z}_4^n \mid (0, y) \in 8\Gamma' - 8\Gamma'\}$; we claim that $|\mathcal{Y}| \leqslant C$ 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 $i = 1, \dots, 15$, and range over all $|\Gamma'|$ pairs $(x, w_x) \in \Gamma'$ to get $|\Gamma'|$ elements $(x + x' - x'', w_x + w' - w'') \in 8\Gamma' - 8\Gamma'$ 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 and $y \in \mathcal{Y}$, hence $|16\Gamma' - 16\Gamma'| > C|\Gamma'|$, in contradiction. The set $\mathcal{Y}$ will be useful for us as for any $x \in \mathbb{Z}_2^n$, 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 $I_1, \dots, I_t \subseteq [n]$ independently and uniformly and consider

$$\mathcal{W} = \left\{ y \in \mathbb{Z}_4^n \mid \sum_{j \in I_i} y_j = 0 \; \forall i = 1, \dots, t \right\}.$$

We note that the 0 vector is always in $\mathcal{W}$, but any other $y \in \mathbb{Z}_4^n$ 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 $y \pmod 2$ is a non-zero vector that must satisfy t randomly chosen equations modulo 2, which happens with probability 2^{-t}. Thus, $\mathbb{E}[|\mathcal{Y} \cap \mathcal{W} \setminus \{0\}|] \leqslant 2^{-t}|\mathcal{Y}| < 1$, so we may choose $\mathcal{W}$ such that $\mathcal{Y} \cap \mathcal{W} = \{0\}$.

For an $a \in \mathbb{Z}_4^n$ we define $\Gamma'_a = \{(x, y) \in \Gamma' \mid y \in a + \mathcal{W}\}$. We claim that there is a choice for a such that (1) $|\Gamma'_a| \geqslant 4^{-t}|\Gamma'| \geqslant \Omega(\xi^{257}|\mathbb{Z}_2^n|)$, and (2) taking $\mathcal{A} = \{x \mid \exists y \text{ such that } (x, y) \in \Gamma'_a\}$, 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

$$\mathop{\mathbb{E}}_{a}\left[|\Gamma'_a|\right] = \sum_{(x,y) \in \Gamma'} \Pr_a[y \in a + \mathcal{W}] = \sum_{(x,y) \in \Gamma'} \Pr_a[y - a \in \mathcal{W}] \geqslant \sum_{(x,y) \in \Gamma'} 4^{-t} = 4^{-t}\left|\Gamma'\right|,$$

so there is an a such that $|\Gamma'_a| \geqslant 4^{-t}|\Gamma'|$, and we show that the second item holds for all a.

Suppose towards contradiction that $\phi|_{\mathcal{A}}$ is not a Freiman homomorphism of order 8. Thus we can find $x_1, \dots, x_8 \in \mathcal{A}$ and $x'_1, \dots, x'_8 \in \mathcal{A}$ that have the same sum yet $\phi(x_1) + \ldots + \phi(x_8) \neq \phi(x'_1) + \ldots + \phi(x'_8)$. Denoting $x = x_1 + \ldots + x_4 - x'_5 - \ldots - x'_8 = x'_1 + \ldots + x'_4 - x_5 - \ldots - x_8$, $y = \phi(x_1) + \ldots + \phi(x_4) - \phi(x'_5) - \ldots - \phi(x'_8)$ and $y' = \phi(x'_1) + \ldots + \phi(x'_4) - \phi(x_5) - \ldots - \phi(x_8)$ so that $y \neq y'$, we get that $(x, y), (x, y') \in 4\Gamma'_a - 4\Gamma'_a \subseteq 4\Gamma' - 4\Gamma'$, so $y, y' \in \mathcal{Y}_x$. In particular, $y - y' \in \mathcal{Y}_x - \mathcal{Y}_x \subseteq \mathcal{Y}$. On the other hand, by choice of $\mathcal{A}$ we get that $\phi(x_i), \phi(x_i') \in a + \mathcal{W}$ for all i and so $y, y' \in 4\mathcal{W} - 4\mathcal{W} = \mathcal{W}$ and so $y - y' \in \mathcal{W}$. It follows that $y - y' \in \mathcal{Y} \cap \mathcal{W}$, but by the choice of $\mathcal{W}$ this last intersection only contains the 0 vector, and contradiction. $\square$

Thus, combining Lemmas 2.2 and 2.7 we are able to conclude that F is a Freiman homomorphism of order 8 when restricted to a set $\mathcal{A} \subseteq \mathbb{Z}_2^n$ whose size is at least $\Omega(\eta^{1028}N)$. A Freiman homomorphism of order 8 is also a Freiman homomorphism of order 4, and the following lemma shows this tells that there is a shift of $\{0,2\}^n$ in which $F(x)$ lies for many x's:

Lemma 2.8. *Let $\mathcal{A} \subseteq \mathbb{Z}_2^n$ and suppose that $\phi\colon \mathcal{A} \to \mathbb{Z}_4^n$ is a Freiman homomorphism of order 4. Then there is $s \in \mathbb{Z}_4^n$ such that for all $x \in \mathcal{A}$, $\phi(x) \in s + \{0,2\}^n$.*

Proof. Choose any $a \in \mathcal{A}$ and let $s = \phi(a)$. Then for any $x \in \mathcal{A}$, applying the Freiman homomorphism condition on the tuples (x, x, a, a) and (a, a, a, a) that have the same sum over $\mathbb{Z}_2^n$, 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. $\square$

Combining the last two lemmas we get the following corollary.

Corollary 2.9. *Suppose that $F\colon \mathbb{Z}_2^n \to \mathbb{Z}_4^n$ is a function for which there are $G, H\colon \mathbb{Z}_2^n \to \mathbb{Z}_4^n$ such that $\Pr_{(x,y,z)\in S^n}[F(x) + G(y) + H(z) = 0] \geqslant \eta$. Then there is $s \in \mathbb{Z}_4^n$ such that*

$$\Pr_{x\in\mathbb{Z}_2^n}[F(x) \in \{0,2\}^n + s] \geqslant \Omega(\eta^{1028}).$$

Proof. By Lemma 2.2 we get that F has at least $\eta^4 N^3$ additive quadruples, so by Lemma 2.7 there is $\mathcal{A} \subseteq \mathbb{Z}_2^n$ of size at least $\Omega(\eta^{1028}N)$ such that $F|_{\mathcal{A}}$ is a Freiman homomorphism. Applying Lemma 2.8 we conclude that there is $s \in \mathbb{Z}_4^n$ such that $F(x) \in s + \{0,2\}^n$ for all $x \in \mathcal{A}$ and the proof is concluded. $\square$

2.3 Concluding Theorem 1.1

Let $f, g, h\colon \{0,1\}^n \to \{0,1\}^n$ be strategies that achieve value at least η in $\mathsf{GHZ}^{\otimes n}$, and define $F\colon \mathbb{Z}_2^n \to \mathbb{Z}_4^n$ by $F(x) = 2f(x) - x$ and similarly $G(y) = 2g(y) - y$ and $H(z) = 2h(z) - z$. By Lemma 1.2 we get that $\Pr_{(x,y,z)\in S^n}[F(x) + G(y) + H(z) = 0] \geqslant \eta$, hence by Corollary 2.9 there is $s \in \mathbb{Z}_4^n$ such that $\Pr_{x\in\mathbb{Z}_2^n}[F(x) \in s + \{0,2\}^n] \geqslant \eta'$ 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 modulo 2. We also have that $2f(x) - L(x) \in \{0,2\}^n$ so this vanishes modulo 2, hence we get that $x = -s \pmod 2$. In other words, there can be at most single x such that $F(x) \in s + \{0,2\}^n$ and so $\Pr_{x\in\mathbb{Z}_2^n}[F(x) \in s + \{0,2\}^n] \leqslant 2^{-n}$. Combining, we get that $\eta' \leqslant 2^{-n}$ and so $\eta \leqslant 2^{-n/1028+O(1)}$.

References

[1] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable *k*-csps: I. 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 *8th Innovations in Theoretical Computer Science Conference, ITCS 2017, January 9-11, 2017, Berkeley, CA, USA*, volume 67 of *LIPIcs*, pages 37:1–37:16.

[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 62:1–62:19.

[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.

[8] William T Gowers. A new proof of Szemerédi's theorem. *Geometric & Functional Analysis GAFA*, 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-Szemerédi-Gowers theorem. *Combinatorica*, 35(6):695–701, 2015.

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

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il