The asymptotic induced matching number of hypergraphs: balanced binary strings

Srinivasan Arunachalam*

Center for Theoretical Physics
Massachusetts Institute of Technology
Cambridge, MA, U.S.A.

arunacha@mit.edu

Péter Vrana†

Department of Geometry
Budapest University of Technology and Economics
Budapest, Hungary

MTA-BME Lendület Quantum Information Theory Research Group

vranap@math.bme.hu

Jeroen Zuiddam‡

Institute for Advanced Study
Princeton, NJ, U.S.A.

jzuiddam@ias.edu

Submitted: Sep 18, 2019; Accepted: Jun 24, 2020; Published: Jul 24, 2020

Abstract

We compute the asymptotic induced matching number of the k-partite k-uniform hypergraphs whose edges are the k-bit strings of Hamming weight $k/2$, for any large enough even number k. Our lower bound relies on the higher-order extension of the well-known Coppersmith–Winograd method from algebraic complexity theory, which was proven by Christandl, Vrana and Zuiddam. Our result is motivated by

*Supported by the MIT–IBMWatson AI Lab under the project *Machine Learning in Hilbert space*. Partially supported by QuSoft, CWI and ERC Consolidator Grant QPROGRESS.

†Supported by the National Research, Development and Innovation Fund of Hungary within the Quantum Technology National Excellence Program (Project Nr. 2017-1.2.1-NKP-2017-00001) and via the research grants K124152, KH129601.

‡Partially supported by QuSoft, CWI. This material is based upon work supported by the National Science Foundation under Grant No. DMS-1638352

the study of the power of this method as well as of the power of the Strassen support functionals (which provide upper bounds on the asymptotic induced matching number), and the connections to questions in tensor theory, quantum information theory and theoretical computer science. Our proof relies on a new combinatorial inequality that may be of independent interest. This inequality concerns how many pairs of Boolean vectors of fixed Hamming weight can have their sum in a fixed subspace.

Mathematics Subject Classifications: 05D99

1 Introduction

1.1 Asymptotic induced matchings

We study in this paper an asymptotic parameter of k-partite k-uniform hypergraphs: the asymptotic induced matching number. For $k \in \mathbb{N}$, a *k-partite k-uniform hypergraph*, or *k-graph* for short, is a tuple of finite sets $V_1, \ldots, V_k$ together with a subset Φ of their cartesian product:

$$\Phi \subseteq V_1 \times \cdots \times V_k.$$

Whenever possible we will leave the vertex sets V_i implicit and refer to the k-graph by its edge set Φ. For any $k \in \mathbb{N}$ we use the notation $[k] \coloneqq \{1, 2, \ldots, k\}$. Let Φ be a k-graph. We say a subset Ψ of Φ is *induced* if $\Psi = \Phi \cap (\Psi_1 \times \cdots \times \Psi_k)$ where for each $i \in [k]$ we define the marginal set $\Psi_i \coloneqq \{a_i : a \in \Psi\}$. We call Ψ a *matching* if any two distinct elements $a, b \in \Psi$ are distinct in all k coordinates, that is, $\forall i \in [k] : a_i \neq b_i$. The *subrank*[1] or *induced matching number* $\mathrm{Q}(\Phi)$ is defined as the size of the largest subset Ψ of Φ that is an induced matching, that is,

$$\mathrm{Q}(\Phi) \coloneqq \max\{|\Psi| : \Psi \subseteq \Phi, \Psi = \Phi \cap (\Psi_1 \times \cdots \times \Psi_k), \forall a \neq b \in \Psi \ \forall i \in [k] \ a_i \neq b_i\}.$$

For example, consider the 3-graph

$$\Phi = \{(1,1,1), (2,2,2), (3,3,3)\} \subseteq [3] \times [3] \times [3].$$

Here Φ is itself an induced matching, and so $\mathrm{Q}(\Phi) = 3$. Next, let

$$\Phi = \{(1,1,1), (2,2,2), (3,3,3), (1,2,3)\} \subseteq [3] \times [3] \times [3].$$

Now the subset $\{(1,1,1), (2,2,2)\} \subseteq \Phi$ is an induced matching and there is no larger induced matching in Φ, and so $\mathrm{Q}(\Phi) = 2$.

In order to define the asymptotic induced matching number, we define the *Kronecker product* of any two k-graphs $\Phi \subseteq V_1 \times \cdots \times V_k$ and $\Psi \subseteq W_1 \times \cdots \times W_k$ as the k-graph

$$\begin{aligned} \Phi \boxtimes \Psi &\coloneqq \big\{\big((a_1, b_1), \ldots, (a_k, b_k)\big) : a \in \Phi, b \in \Psi\big\} \\ &\subseteq (V_1 \times W_1) \times \cdots \times (V_k \times W_k), \end{aligned}$$

[1] The term subrank originates from an analogous parameter in the theory of tensors, see Section 1.4.1.

and we naturally define the power $\Phi^{\boxtimes n} = \Phi \boxtimes \cdots \boxtimes \Phi$. The *asymptotic subrank* or the *asymptotic induced matching number* of the k-graph Φ is defined as

$$\underset{\sim}{\mathrm{Q}}(\Phi) \coloneqq \lim_{n\to\infty} \mathrm{Q}(\Phi^{\boxtimes n})^{1/n}.$$

This limit exists and equals the supremum $\sup_{n\in\mathbb{N}} \mathrm{Q}(\Phi^{\boxtimes n})^{1/n}$ by Fekete's lemma [25].

We study the following basic question:

Problem 1. Given Φ what is the value of $\underset{\sim}{\mathrm{Q}}(\Phi)$?

A priori, for $\Phi \subseteq V_1 \times \cdots \times V_k$ we have the upper bound $\mathrm{Q}(\Phi) \leqslant \min_i |V_i|$ and therefore it holds that $\underset{\sim}{\mathrm{Q}}(\Phi) \leqslant \min_i |V_i|$, since $|V_i^{\times n}| = |V_i|^n$.

Problem 1 has been studied for several families of k-graphs, in several different contexts: the cap set problem [12, 33, 19, 23, 24], approaches to fast matrix multiplication [32, 4, 5, 28], arithmetic removal lemmas [21, 14], property testing [15, 17], quantum information theory [35, 36], and the general study of asymptotic properties of tensors [34, 7, 8]. We finally mention the related result of Ruzsa and Szemerédi which says that the largest subset $E \subseteq \binom{n}{2}$ such that $(E\times E\times E)\cap\{(\{a,b\},\{b,c\},\{c,a\}) : a,b,c \in [n]\}$ is a matching, has size $n^{2-o(1)} \leqslant |E| \leqslant o(n^2)$ when n goes to infinity [27], see also [2, Equation 2].

1.2 Result

We solve Problem 1 for a family of k-graphs that are structured but nontrivial. For $k \geqslant n$ let $\lambda = (\lambda_1, \ldots, \lambda_n) \vdash k$ be an integer partition of k with n nonzero parts, that is, $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n > 0$ and $\sum_{i=1}^n \lambda_i = k$. We define the k-graph

$$\Phi_\lambda \coloneqq \{s \in [n]^k : \mathrm{type}(s) = \lambda\}$$

where the expression $\mathrm{type}(s) = \lambda$ means that s is a permutation of the k-tuple

$$(\underbrace{1,\ldots,1}_{\lambda_1},\underbrace{2,\ldots,2}_{\lambda_2},\ldots,\underbrace{n,\ldots,n}_{\lambda_n}).$$

For example, the partition $\lambda = (1,1) \vdash 2$ corresponds to the 2-graph

$$\Phi_{(1,1)} = \{(2,1),(1,2)\} \subseteq [2] \times [2]$$

and the partition $\lambda = (2,2) \vdash 4$ corresponds to the 4-graph

$$\Phi_{(2,2)} = \{(2,2,1,1),(2,1,2,1),(2,1,1,2),(1,2,2,1),(1,2,1,2),(1,1,2,2)\} \subseteq [2]^{\times 4}.$$

It was shown in [7] that $\underset{\sim}{\mathrm{Q}}(\Phi_{(k-1,1)}) = 2^{H((1-1/k,1/k))}$ for every $k \in \mathbb{N}_{\geqslant 3}$ where H is the Shannon entropy in base 2. As a natural continuation of that work we study $\underset{\sim}{\mathrm{Q}}(\Phi_{(k/2,k/2)})$ for even $k \in \mathbb{N}$. Since $\Phi_{(k/2,k/2)} \subseteq [2]^{\times k}$ we have $\underset{\sim}{\mathrm{Q}}(\Phi_{(k/2,k/2)}) \leqslant 2$. Clearly, the 2-graph $\Phi_{(1,1)}$ is itself a matching, and so $\underset{\sim}{\mathrm{Q}}(\Phi_{(1,1)}) = 2$. It was shown in [7] that also $\underset{\sim}{\mathrm{Q}}(\Phi_{(2,2)}) = 2$. Our new result is the following extension:

Theorem 2. *Let $k \in \mathbb{N}_{\geqslant 2}$ be even and large enough. Then $\underset{\sim}{\mathrm{Q}}(\Phi_{(k/2,k/2)}) = 2$.*

In other words, we prove that for every large enough even $k \in \mathbb{N}_{\geqslant 2}$ there is an induced matching $\Psi \subseteq \Phi_{(k/2,k/2)}^{\boxtimes n}$ of size $|\Psi| = 2^{n-o(n)}$ when n goes to infinity.

Moreover, we numerically verified that $\underset{\sim}{\mathrm{Q}}(\Phi_{(k/2,k/2)}) = 2$ also holds for all even integers $k \leqslant 2000$. We conjecture that $\underset{\sim}{\mathrm{Q}}(\Phi_{(k/2,k/2)}) = 2$ for all even k. More generally, we conjecture (cf. [35] and [7, Question 1.3.3]) that $\log_2 \underset{\sim}{\mathrm{Q}}(\Phi_\lambda)$ equals the Shannon entropy of the probability distribution obtained by normalising the partition λ. We will discuss further motivation and background in Section 1.4.

1.3 Methods

We prove Theorem 2 by applying the higher-order Coppersmith–Winograd (CW) method from [7] to the k-graph $\Phi_{(k/2,k/2)}$. This method is an extension of the work of Coppersmith and Winograd [10] and Strassen [32] from the case $k = 3$ to the case $k \geqslant 4$. It provides a construction of large induced matchings in k-graphs via the probabilistic method, and we prove Theorem 2 by analysing the size of these induced matchings.

Theorem 3 (Higher-order CW method [7])**.** *Let $\Phi \subseteq V_1 \times \cdots \times V_k$ be a nonempty k-graph for which there exist injective maps $\alpha_i : V_i \to \mathbb{Z}$ such that for all $a \in \Phi$ the equality*

$$\alpha_1(a_1) + \cdots + \alpha_k(a_k) = 0$$

holds. For any $R \subseteq \Phi \times \Phi$ let $r(R)$ be the rank over $\mathbb{Q}$ of the $|R| \times k$ matrix with rows

$$\{\alpha(x) - \alpha(y) : (x, y) \in R\},$$

where $\alpha(x) \coloneqq (\alpha_1(x_1), \ldots, \alpha_k(x_k)) \in \mathbb{Z}^k$. Then

$$\log_2 \underset{\sim}{\mathrm{Q}}(\Phi) \geqslant \max_{P \in \mathscr{P}} \left(H(P) - (k-2) \max_{R \in \mathscr{R}} \frac{\max_{Q \in \mathscr{Q}_{R,(P_1,\ldots,P_k)}} H(Q) - H(P)}{r(R)} \right) \tag{1}$$

where the parameters P, R and Q are taken over the following domains:

- *$\mathscr{P}$ is the set of probability distributions on Φ*
- *$\mathscr{R}$ is the set of subsets of $\Phi \times \Phi$ that are not a subset of $\{(x, x) : x \in \Phi\}$ and moreover satisfy $\exists i \in [k]\, \forall (x, y) \in R \colon x_i = y_i$*
- *$\mathscr{Q}_{R,(P_1,\ldots,P_k)}$ is the set of probability distributions on $R \subseteq \Phi \times \Phi$ with marginal distributions equal to $P_1, \ldots, P_k, P_1, \ldots, P_k$ respectively.*

Here for $P \in \mathscr{P}$ we denote by $P_1, \ldots, P_k$ the marginal probability distributions of P on the components $V_1, \ldots, V_k$ respectively, and H denotes Shannon entropy.

Let $\lambda \vdash k$ be any integer partition of k with n nonzero parts. We can apply Theorem 3 to the k-graph $\Phi = \Phi_\lambda$ as follows. For every $a \in \Phi_\lambda$ the equality

$$\sum_{i=1}^{k} a_i = \sum_{j=1}^{n} j\lambda_j \tag{2}$$

holds, since the element j occurs λ_j times in a. Let $\alpha_1, \dots, \alpha_{k-1}$ be identity maps $\mathbb{Z} \to \mathbb{Z}$ and let $\alpha_k : \mathbb{Z} \to \mathbb{Z} : x \mapsto x - \sum_{j=1}^{n} j\lambda_j$. Then, because of (2), $\forall a \in \Phi_\lambda \colon \alpha_1(a_1) + \cdots + \alpha_k(a_k) = 0$. (Note that with this choice of maps $\alpha_1, \dots, \alpha_k$ we have that $\alpha(x) - \alpha(y)$ equals $x - y$ for every $(x, y) \in R$.) Therefore Theorem 3 can be applied to obtain a lower bound on $\underset{\sim}{\mathrm{Q}}(\Phi_\lambda)$ for any partition λ. The difficulty now lies in evaluating the right-hand side of (1).

Let us return to the case $\lambda = (k/2, k/2)$. To prove Theorem 2 via Theorem 3 we will show for every large enough even $k \in \mathbb{N}$ and $\Phi = \Phi_{(k/2,k/2)}$ that the right-hand side of (1) is at least 2, using the aforementioned choice of injective maps $\alpha_1, \dots, \alpha_k$. In Section 2 we prove that this follows from the following statement, which may be of interest on its own.

Theorem 4. *For any large enough even $k \in \mathbb{N}_{\geqslant 4}$ and subspace*

$$V \subseteq \{x \in \mathbb{F}_2^k : x_k = 0\} \subseteq \mathbb{F}_2^k$$

the inequality

$$\left|\left\{(x, y) \in \mathbb{F}_2^k \times \mathbb{F}_2^k : |x| = |y| = \tfrac{k}{2},\, x - y \in V\right\}\right| \leqslant \binom{k-1}{k/2}^{\frac{\dim_{\mathbb{F}_2}(V)}{k-2}+1} \tag{3}$$

holds. Here $|x|$ denotes the Hamming weight of $x \in \mathbb{F}_2^k$.

In Section 3 we prove Theorem 4 for low-dimensional V by carefully splitting the left-hand side of (3) into two parts and upper bounding these parts. In Section 4 we prove Theorem 4 for high-dimensional V using Fourier analysis, Krawchouk polynomials and an upper bound on the size of Hamming layers in subspaces. We thus prove Theorem 4 and hence Theorem 2. While in our current proof the tools for the low- and high-dimensional cases are used complementarily, it may be possible that the full Theorem 2 can be proven by cleverly using only the low-dimensional tools or only the high-dimensional tools.

1.4 Motivation and background

Our original motivation to study the asymptotic induced matching number of k-graphs comes from a connection to the study of asymptotic properties of tensors. In fact, the interplay in this connection goes both directions. The purpose of this section is to discuss the asymptotic study of tensors and the connection with the asymptotic induced matching number. Reading this section is not required to understand the rest of the paper.

1.4.1 Asymptotic rank and asymptotic subrank of tensors

The asymptotic study of tensors is a field of its own that started with the work of Strassen [30, 31, 32] in the context of fast matrix multiplication. We begin by introducing two fundamental asymptotic tensor parameters: asymptotic rank and asymptotic subrank.

Let $\mathbb{F}$ be a field. Let $a \in \mathbb{F}^{n_1} \otimes \cdots \otimes \mathbb{F}^{n_k}$ and $b \in \mathbb{F}^{m_1} \otimes \cdots \otimes \mathbb{F}^{m_k}$ be k-tensors. We write $a \leqslant b$ if there are linear maps $A_i : \mathbb{F}^{m_i} \to \mathbb{F}^{n_i}$ for $i \in [k]$ such that $a = (A_1 \otimes \cdots \otimes A_k)(b)$. For $n \in \mathbb{N}$ let $\{e_n : j \in [n]\}$ be the standard basis of $\mathbb{F}^n$. For $n \in \mathbb{N}$ define the k-tensor

$$\langle n \rangle \coloneqq \sum_{i=1}^{n} e_i \otimes \cdots \otimes e_i \in (\mathbb{F}^n)^{\otimes k}.$$

The rank of the k-tensor a is defined as $\mathrm{R}(a) \coloneqq \min\{n \in \mathbb{N} : a \leqslant \langle n \rangle\}$. The subrank of the k-tensor a is defined as

$$\mathrm{Q}(a) \coloneqq \max\{n \in \mathbb{N} : \langle n \rangle \leqslant a\}. \tag{4}$$

One can think of tensor rank as a measure of the complexity of a tensor, namely the "cost" of the tensor in terms of the diagonal tensors $\langle n \rangle$. It has been studied in several contexts, see, e.g., [6, 20]. In this language, the subrank is the "value" of the tensor in terms of $\langle n \rangle$ and as such is the natural companion to tensor rank. It has its own applications, which we will elaborate on after having discussed the asymptotic viewpoint.

Writing a and b in the standard basis as $a = \sum_i a_i\, e_{i_1} \otimes \cdots \otimes e_{i_k}$, $b = \sum_j b_j\, e_{j_1} \otimes \cdots \otimes e_{j_k}$, the tensor Kronecker product $a \boxtimes b$ is the k-tensor defined by

$$a \boxtimes b \coloneqq \sum_{i,j} a_i b_j\ (e_{i_1} \otimes e_{j_1}) \otimes \cdots \otimes (e_{i_k} \otimes e_{j_k}) \in (\mathbb{F}^{n_1} \otimes \mathbb{F}^{m_1}) \otimes \cdots \otimes (\mathbb{F}^{n_k} \otimes \mathbb{F}^{m_k}).$$

In other words, the k-tensor $a \boxtimes b$ is the image of the $2k$-tensor $a \otimes b$ under the natural regrouping map $\mathbb{F}^{n_1} \otimes \cdots \otimes \mathbb{F}^{n_k} \otimes \mathbb{F}^{m_1} \otimes \cdots \otimes \mathbb{F}^{m_k} \to (\mathbb{F}^{n_1} \otimes \mathbb{F}^{m_1}) \otimes \cdots \otimes (\mathbb{F}^{n_k} \otimes \mathbb{F}^{m_k})$. The asymptotic rank of a is defined as $\underset{\sim}{\mathrm{R}}(a) \coloneqq \lim_{n\to\infty} \mathrm{R}(a^{\boxtimes n})^{1/n}$ and the asymptotic subrank of a is defined as $\underset{\sim}{\mathrm{Q}}(a) \coloneqq \lim_{n\to\infty} \mathrm{Q}(a^{\boxtimes n})^{1/n}$. These limits exist and equal the infimum $\inf_n \mathrm{R}(a^{\boxtimes n})^{1/n}$ and the supremum $\sup_n \mathrm{Q}(a^{\boxtimes n})^{1/n}$, respectively. This follows from Fekete's lemma and the fact that $\mathrm{R}(a \boxtimes b) \leqslant \mathrm{R}(a)\,\mathrm{R}(b)$ and $\mathrm{Q}(a \boxtimes b) \geqslant \mathrm{Q}(a)\,\mathrm{Q}(b)$.

Tensor rank is known to be hard to compute [16] (the natural tensor rank decision problem is NP-hard). Not much is known about the complexity of computing subrank, asymptotic subrank and asymptotic rank. It is a long-standing open problem in algebraic complexity theory to compute the asymptotic rank of the matrix multiplication tensor. The asymptotic rank of the matrix multiplication tensor corresponds directly to the asymptotic algebraic complexity of matrix multiplication. The asymptotic subrank of 3-tensors also plays a central role in the context of matrix multiplication, for example in recent work on barriers for upper bound methods on the asymptotic rank of the matrix multiplication tensor [9, 1]. As another example, in combinatorics, the resolution of the cap set problem [12, 33] can be phrased in terms of the asymptotic subrank of a well-chosen 3-tensor, cf. [7], via the general connection to the asymptotic induced matching number that we will review now.

The subrank of k-tensors as defined in (4) and the subrank of k-graphs as defined in Section 1.1 are related as follows. For any k-tensor $a = \sum_i a_i\, e_{i_1} \otimes \cdots \otimes e_{i_k} \in \mathbb{F}^{n_1} \otimes \cdots \otimes \mathbb{F}^{n_k}$ we define the k-graph $\operatorname{supp}(a)$ as the support of a in the standard basis:

$$\operatorname{supp}(a) \coloneqq \{i \in [n_1] \times \cdots \times [n_k] : a_i \neq 0\}.$$

It is readily verified that the subrank of the k-graph $\operatorname{supp}(a)$ is at most the subrank of the k-tensor a, that is, $\mathrm{Q}(\operatorname{supp}(a)) \leqslant \mathrm{Q}(a)$. The reader may also verify directly that $\operatorname{supp}(a \boxtimes b) = \operatorname{supp}(a) \boxtimes \operatorname{supp}(b)$. Therefore, the asymptotic subrank of the support of a is at most the asymptotic subrank of the k-tensor a, that is,

$$\underset{\sim}{\mathrm{Q}}(\operatorname{supp}(a)) \leqslant \underset{\sim}{\mathrm{Q}}(a). \tag{5}$$

We can read (5) in two ways. On the one hand, given any k-tensor a we may find lower bounds on $\underset{\sim}{\mathrm{Q}}(a)$ by finding lower bounds on $\underset{\sim}{\mathrm{Q}}(\operatorname{supp}(a))$. On the other hand, given any k-graph $\Phi \subseteq [n_1] \times \cdots \times [n_k]$ the asymptotic subrank $\underset{\sim}{\mathrm{Q}}(\Phi)$ is upper bounded by $\underset{\sim}{\mathrm{Q}}(a)$ for any tensor $a \in \mathbb{F}^{n_1} \otimes \cdots \otimes \mathbb{F}^{n_k}$ (over any field $\mathbb{F}$) with support equal to Φ, that is,

$$\underset{\sim}{\mathrm{Q}}(\Phi) \leqslant \min_{\text{field } \mathbb{F}} \min_{\substack{a \in \mathbb{F}^{n_1} \otimes \cdots \otimes \mathbb{F}^{n_k} : \\ \operatorname{supp}(a) = \Phi}} \underset{\sim}{\mathrm{Q}}(a). \tag{6}$$

We do not know whether the inequality in (6) can be strict. We will discuss these two directions in the following two sections.

1.4.2 Upper bounds on asymptotic subrank of k-tensors

Let us focus on the task of finding upper bounds on the asymptotic subrank of k-tensors. One natural strategy is to construct maps $\phi : \{k\text{-tensors over } \mathbb{F}\} \to \mathbb{R}_{\geqslant 0}$ that are submultiplicative under the tensor Kronecker product $\boxtimes$, normalised on $\langle n \rangle$ to n, and monotone under $\leqslant$, that is, for any k-tensors a and b and for any $n \in \mathbb{N}$:

$$\phi(a \boxtimes b) \leqslant \phi(a)\phi(b) \tag{7}$$

$$\phi(\langle n \rangle) = n \tag{8}$$

$$a \leqslant b \Rightarrow \phi(a) \leqslant \phi(b). \tag{9}$$

The reader verifies directly that for any such map ϕ the inequality $\underset{\sim}{\mathrm{Q}}(a) \leqslant \phi(a)$ holds.

Strassen in [32], motivated by the study of the algebraic complexity of matrix multiplication, introduced an infinite family of maps

$$\zeta^\theta : \{k\text{-tensors over } \mathbb{F}\} \to \mathbb{R}_{\geqslant 0}$$

parametrised by probability vectors $\theta \in \mathbb{R}^k_{\geqslant 0}$, $\sum_{i=1}^k \theta_i = 1$. The maps ζ^θ are called the upper support functionals. We will not define them here. Strassen proved that each map ζ^θ satisfies conditions (7), (8) and (9). Thus

$$\underset{\sim}{\mathrm{Q}}(a) \leqslant \min_\theta \zeta^\theta(a). \tag{10}$$

Tao, motivated by the study of the cap set problem, proved in [33] that subrank is upper bounded by a parameter called slice rank, that is, $\mathrm{Q}(a) \leqslant \mathrm{slicerank}(a)$. We do not define slice rank here. While slice rank is easily seen to be normalised on $\langle n \rangle$ and monotone under $\leqslant$, slice rank is not sub-multiplicative (see, e.g., [8]). However, it still holds that

$$\underset{\sim}{\mathrm{Q}}(a) \leqslant \liminf_{n\to\infty} \mathrm{slicerank}(a^{\boxtimes n})^{1/n}.$$

It turns out [34, 8] that

$$\limsup_{n\to\infty} \mathrm{slicerank}(a^{\boxtimes n})^{1/n} \leqslant \min_{\theta} \zeta^{\theta}(a).$$

No examples are known for which this inequality is strict. It is known that for so-called oblique tensors holds $\limsup_{n\to\infty} \mathrm{slicerank}(a^{\boxtimes n})^{1/n} = \min_{\theta} \zeta^{\theta}(a)$ [8].

1.4.3 Lower bounds on asymptotic subrank of k-graphs

We now consider the task of finding lower bounds on the asymptotic subrank of k-graphs. For $k = 3$ the CW method introduced by Coppersmith and Winograd [10] and extended by Strassen [32] gives the following. Let $\Phi \subseteq V_1 \times V_2 \times V_3$ be a 3-graph for which there exist injective maps $\alpha_i : V_i \to \mathbb{Z}$ such that $\forall a \in \Phi \colon \alpha_1(a_1) + \alpha_2(a_2) + \alpha_3(a_3) = 0$. Then

$$\log_2 \underset{\sim}{\mathrm{Q}}(\Phi) \geqslant \max_{P\in\mathscr{P}} \min_{i\in[3]} H(P_i) \tag{11}$$

where $\mathscr{P}$ is the set of probability distributions on Φ. The inequality

$$\log_2 \underset{\sim}{\mathrm{Q}}(\Phi) \leqslant \max_{P\in\mathscr{P}} \min_{i} H(P_i),$$

follows from using (5) and using the support functionals as upper bound on the asymptotic subrank of tensors. Thus, the CW method is optimal whenever it can be applied.

Theorem 3 extends the CW method from $k = 3$ to higher-order tensors, that is, $k \geqslant 4$. Contrary to the situation for $k = 3$, the lower bound produced by Theorem 3 is not known to be tight.

1.4.4 Type tensors

As an investigation of the power of the higher-order CW method (Theorem 3) and of the power of the support functionals (Section 1.4.2) we study the asymptotic subrank of the following family of tensors and their support. While we do not have any immediate "application" for these tensors, we feel that they provide enough structure to make progress while still showing interesting behaviour.

Let $\lambda \vdash k$ be an integer partition of k with n nonzero parts. Recall the definition of the k-graph Φ_λ from Section 1.1. We define the tensor T_λ as the k-tensor with support Φ_λ and all nonzero coefficients equal to 1, that is,

$$T_\lambda \coloneqq \sum_{s\in\Phi_\lambda} e_{s_1} \otimes \cdots \otimes e_{s_k} \in (\mathbb{F}^n)^{\otimes k}.$$

In general, it follows from (5) and evaluating the right-hand side of (10) for $a = T_\lambda$ and the uniform $\theta = (1/k, \dots, 1/k)$ that

$$\underset{\sim}{\mathrm{Q}}(\Phi_\lambda) \leqslant \underset{\sim}{\mathrm{Q}}(T_\lambda) \leqslant 2^{H(\lambda/k)}.$$

It was shown in [7] that

$$\underset{\sim}{\mathrm{Q}}(\Phi_{(k-1,1)}) = \underset{\sim}{\mathrm{Q}}(T_{(k-1,1)}) = 2^{H((1-1/k,1/k))}$$

for every $k \in \mathbb{N}_{\geqslant 3}$ using Theorem 3. (The same result was essentially obtained in [17].) In [7] it was moreover shown that

$$\underset{\sim}{\mathrm{Q}}(\Phi_{(2,2)}) = \underset{\sim}{\mathrm{Q}}(T_{(2,2)}) = 2$$

using Theorem 3. As mentioned before, our main result (Theorem 2) is that for any large enough even $k \in \mathbb{N}_{\geqslant 2}$ it holds that

$$\underset{\sim}{\mathrm{Q}}(\Phi_{(k/2,k/2)}) = \underset{\sim}{\mathrm{Q}}(T_{(k/2,k/2)}) = 2. \tag{12}$$

We conjecture that (12) holds for all even $k \in \mathbb{N}$. We numerically verified this up to $k \leqslant 2000$ by verifying the statement of Theorem 4 for $k \leqslant 2000$. Unfortunately, with our current analysis it seems infeasible to numerically verify the statement of Theorem 4 up to the value of k from which our proof works.

More generally we conjecture that $\underset{\sim}{\mathrm{Q}}(\Phi_\lambda) = \underset{\sim}{\mathrm{Q}}(T_\lambda) = 2^{H(\lambda/k)}$ holds for all partitions $\lambda \vdash k$, where H denotes the Shannon entropy and λ/k denotes the probability vector $(\lambda_1/k, \dots, \lambda_n/k)$. The strong connection between Theorem 4 and Theorem 2 that makes our proof work relies on the fact that $(k/2, k/2)$ is uniform. For larger uniform partitions $(k/p, \dots, k/p)$ the bottleneck in extending our current proof is our use of Boolean Fourier analysis.

In quantum information theory, the tensors $T_{(m,n)}$, when normalized, correspond to so-called Dicke states (see [11, 29, 35], and, e.g., [3]). Namely, in quantum information language, Dicke states are $(m+n)$-partite pure quantum states given by

$$D_{(m,n)} \coloneqq \frac{1}{\sqrt{\binom{m+n}{m}}} T_{(m,n)} = \frac{1}{\sqrt{(m+n)!}} \sum_{\pi \in S_{m+n}} \pi\big(|0\rangle^{\otimes m} \otimes |1\rangle^{\otimes n}\big)$$

where the sum is over all permutations π of the $k = m + n$ parties. Roughly speaking, our result, Theorem 2, amounts to an asymptotically optimal k-party stochastic local operations and classical communication (SLOCC) protocol for the problem of distilling GHZ-type entanglement from a subfamily of the Dicke states. More precisely, letting $\mathrm{GHZ} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + |1\rangle^{\otimes k})$ be the k-party GHZ state, Theorem 2 says that for k large enough the maximal rate β such that n copies of $D_{(k/2,k/2)}$ can be transformed via SLOCC to $\beta n - o(n)$ copies of GHZ equals 1 when n goes to infinity, that is,

$$(D_{(k/2,k/2)})^{\otimes n} \xrightarrow{\text{SLOCC}} \mathrm{GHZ}^{\otimes n - o(n)}$$

and this rate is optimal.

2 Reduction to counting

We now begin working towards the proof of Theorem 2. The goal of this section is to reduce Theorem 2 to Theorem 4 by applying Theorem 3.

Lemma 5. *Theorem 4 implies Theorem 2.*

Proof. We will use the higher-order CW method Theorem 3 to show that Theorem 4 implies Theorem 2. Let $\Phi = \Phi_{(k/2,k/2)} = \{x \in \{0,1\}^k : |x| = k/2\}$. Let $\alpha_1, \ldots, \alpha_{k-1}$ be the identity map $\mathbb{Z} \to \mathbb{Z}$ and let $\alpha_k : \mathbb{Z} \to \mathbb{Z} : x \mapsto x - k/2$. With this definition of α we have for all $a \in \Phi$ satisfied the condition $\sum_i \alpha_i(a_i) = 0$ from Theorem 3. As in the statement of Theorem 3, for $R \in \mathscr{R}$ let $r(R)$ be the dimension of the $\mathbb{Q}$-vector space

$$\mathrm{Span}_{\mathbb{Q}}\{\alpha(x) - \alpha(y) : (x,y) \in R\} = \mathrm{Span}_{\mathbb{Q}}\{x - y : (x,y) \in R\}.$$

Let P be the uniform distribution on Φ. Then Theorem 3 gives

$$\begin{aligned}\log_2 \underset{\sim}{\mathrm{Q}}(\Phi) &\geqslant H(P) - (k-2)\max_{R\in\mathscr{R}} \frac{\max_{Q\in\mathscr{Q}_{R,(P_1,\ldots,P_k)}} H(Q) - H(P)}{r(R)} \\ &= \log_2 \binom{k}{k/2} - (k-2)\max_{R\in\mathscr{R}} \frac{\max_{Q\in\mathscr{Q}_{R,(P_1,\ldots,P_k)}} H(Q) - \log_2 \binom{k}{k/2}}{r(R)},\end{aligned}$$

For any $Q \in \mathscr{Q}_{R,(P_1,\ldots,P_k)}$ we have that $H(Q)$ is at most the Shannon entropy of the uniform distribution on R. We thus obtain

$$\log_2 \underset{\sim}{\mathrm{Q}}(\Phi) \geqslant \log_2 \binom{k}{k/2} - (k-2)\max_{R\in\mathscr{R}} \frac{\log_2 |R| - \log_2 \binom{k}{k/2}}{r(R)}. \tag{13}$$

It remains to upper bound the maximisation over $R \in \mathscr{R}$ in (13). We define the set

$$\Phi' = \{x \in \{0,1\}^{k-1} : |x| = k/2 - 1\}.$$

For $R \in \mathscr{R}$ let $r_2(R)$ be the dimension of the $\mathbb{F}_2$-vector space

$$\mathrm{Span}_{\mathbb{F}_2}\{\alpha(x) - \alpha(y) : (x,y) \in R\} = \mathrm{Span}_{\mathbb{F}_2}\{x - y : (x,y) \in R\}.$$

By assumption Theorem 4 is true. This means

$$\begin{aligned}\forall R' \subseteq \Phi'^{\times 2} \quad \log_2 |R'| &\leqslant \Big(\frac{r_2(R')}{k-2} + 1\Big)\log_2 \binom{k-1}{k/2-1} \\ &= \frac{r_2(R')}{k-2}\log_2 \binom{k-1}{k/2-1} + \log_2 \binom{k-1}{k/2-1} \\ &= \frac{r_2(R')}{k-2}\log_2 \binom{k-1}{k/2-1} + \log_2 \tfrac{1}{2}\binom{k}{k/2}\end{aligned}$$

that is

$$\forall R' \subseteq \Phi'^{\times 2} \quad \log_2(2\,|R'|) \leqslant \frac{r_2(R')}{k-2} \log_2 \binom{k-1}{k/2-1} + \log_2 \binom{k}{k/2}. \tag{14}$$

For any $R \in \mathscr{R}$ there is a subset $R' \subseteq \Phi'^{\times 2}$ with $|R| \leqslant 2\,|R'|$ and $r_2(R) = r_2(R')$. Namely, one constructs R' as follows. Without loss of generality $\forall (x,y) \in R\colon x_1 = y_1$. For every $(x,y) \in R$, if $x_1 = y_1 = 1$, then add $((x_2,\dots,x_k),(y_2,\dots,y_k))$ to R', and if $x_1 = y_1 = 0$, then add the negated tuple $((1,\dots,1)-(x_2,\dots,x_k),(1,\dots,1)-(y_2,\dots,y_k))$ to R'. Therefore, (14) implies

$$\begin{aligned}\forall R \in \mathscr{R} \quad \log_2 |R| &\leqslant \frac{r_2(R)}{k-2} \log_2 \binom{k-1}{k/2-1} + \log_2 \binom{k}{k/2} \\ &= \frac{r_2(R)}{k-2} \Big(\log_2 2 \binom{k-1}{k/2-1}^2 - \log_2 \binom{k}{k/2} \Big) + \log_2 \binom{k}{k/2}\end{aligned}$$

that is

$$\forall R \in \mathscr{R} \quad \log_2 |R| - \log_2 \binom{k}{k/2} \leqslant \frac{r_2(R)}{k-2} \Big(\log_2 2 \binom{k-1}{k/2-1}^2 - \log_2 \binom{k}{k/2} \Big)$$

that is

$$\forall R \in \mathscr{R} \quad \frac{\log_2 |R| - \log_2 \binom{k}{k/2}}{r_2(R)} \leqslant \frac{\log_2 2\binom{k-1}{k/2-1}^2 - \log_2 \binom{k}{k/2}}{k-2}. \tag{15}$$

Combining (15) with (13) and using $r_2(R) \leqslant r(R)$ gives

$$\begin{aligned}\log_2 \underset{\sim}{\mathrm{Q}}(\phi) &\geqslant \log_2 \binom{k}{k/2} - \left(\log_2 2 \binom{k-1}{k/2-1}^2 - \log_2 \binom{k}{k/2} \right) \\ &= \log_2 2 \binom{k-1}{k/2-1} - \log_2 2 \binom{k-1}{k/2-1}^2 + \log_2 2 \binom{k-1}{k/2-1} \\ &= \log_2 \binom{k-1}{k/2-1} - 2 \log_2 \binom{k-1}{k/2-1} + \log_2 \binom{k-1}{k/2-1} + 1 \\ &= 1.\end{aligned}$$

This proves the lemma. □

3 Case: low dimension

To prove Theorem 2 it remains to prove Theorem 4. Our proof of Theorem 4 is divided into two cases. In this section we prove the low-dimensional case.

Theorem 6. *For any large enough even $k \in \mathbb{N}$ and subspace $V \subseteq \{x \in \mathbb{F}_2^k : x_k = 0\} \subseteq \mathbb{F}_2^k$ such that $\dim_{\mathbb{F}_2}(V) \leqslant 11k/12$, the inequality*

$$\big|\big\{(x,y) \in \mathbb{F}_2^k \times \mathbb{F}_2^k : |x| = |y| = \tfrac{k}{2},\, x - y \in V\big\}\big| \leqslant \binom{k-1}{k/2}^{\frac{\dim_{\mathbb{F}_2}(V)}{k-2}+1}$$

holds.

We set up some notation. Let $k \in 2\mathbb{N}$ and $\Phi = \{x \in \mathbb{F}_2^k \mid |x| = k/2\}$. We will think of $\mathbb{F}_2^{k-1}$ as the subspace where the last component is 0. We want to prove: for any $V \leqslant \mathbb{F}_2^{k-1} \leqslant \mathbb{F}_2^k$ the inequality

$$|R| \leqslant \binom{k-1}{k/2}^{\frac{r}{k-2}+1} \tag{16}$$

holds for all $r \leqslant \frac{11k}{12}$, where $R = \{(x,y) \in \Phi^2 \mid x - y \in V,\, x_k = y_k = 0\}$ and $r = \dim_{\mathbb{F}_2} V$. The proof of (16) is divided into three claims that deal with different ranges for r, namely, $r = 0$, $r \in \{2, \ldots, \frac{k}{2\log k}\}$ and $r \in \{\frac{k}{2\log k}, \ldots, 11k/12\}$. The first claim is trivial:

Claim 7. *Inequality* (16) *holds when* $r = 0$.

Proof. One verifies directly that (16) becomes an equality when $r = 0$. □

We prepare to deal with $r \geqslant 2$. Without loss of generality, we may assume that every vector in V has even weight. To upper bound $|R|$ we introduce the function

$$f(k,m) = \begin{cases} \binom{m}{m/2}\binom{k-m-1}{(k-m)/2} & \text{if } m \text{ is even and } 0 \leqslant m \leqslant k-2 \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

which counts the number of pairs $(x,y) \in \Phi^2$ such that $x - y$ is an arbitrary but fixed vector with Hamming weight m. This function has the following properties.

Proposition 8.

1. *For any even* $0 < m < k$ *it holds that* $f(k,m) = f(k,k-m)$.
2. $f(k,m)$ *strictly decreases in* m *for even* $0 \leqslant m \leqslant k/2$.
3. $f(k,0) = \binom{k-1}{k/2-1} = \binom{k-1}{k/2}$.
4. $f(k,0) \geqslant f(k,k-2) = f(k,2) \geqslant f(k,k-4) = f(k,4) \geqslant \cdots$.

Proof. Claim (3) one verifies directly. For (1) we verify that

$$\begin{aligned} f(k,k-m) &= \binom{k-m}{(k-m)/2}\binom{m-1}{m/2-1} \\ &= 2\binom{k-m-1}{(k-m)/2-1}\frac{1}{2}\binom{m}{m/2} \\ &= f(k,m). \end{aligned}$$

For (2) we verify that

$$\frac{f(k,m)}{f(k,m+2)} = \frac{\binom{m}{m/2}\binom{k-m}{(k-m)/2}}{\binom{m+2}{(m+2)/2}\binom{k-m-2}{(k-m-2)/2}}$$

$$= \frac{m!}{(\frac{m}{2}!)^2}\frac{(k-m)!}{(\frac{k-m}{2}!)^2}\Bigg/\frac{(m+2)!}{(\frac{m+2}{2}!)^2}\frac{(k-m-2)!}{(\frac{k-m-2}{2}!)^2}$$
$$= \frac{(k-m)(k-m-1)}{(m+1)(m+2)}\frac{(\frac{m}{2}+1)^2}{(\frac{k-m}{2})^2}$$
$$= \frac{m+2}{m+1}\frac{k-m-1}{k-m},$$

which is > 1 when $(m+2)(k-m-1) > (m+1)(k-m)$, that is, when $k/2-2 \geqslant m$. Claim (4) follows from (1) and (2). □

Using the definition of $f(k,m)$, we can write $|R|$ in (16) as follows: suppose V has a_m vectors of weight m, then

$$|R| = \sum_{m=0}^{k-1} a_m f(k,m). \tag{18}$$

To get an upper bound on $|R|$, we fix some even $s \in \{2,\dots,k/2\}$ and in the terms with $f(k,m) > f(k,s)$ we replace a_m by $\binom{k-1}{m}$, while in the remaining terms we replace $f(k,m)$ by $f(k,s)$. This gives, using Proposition 8 (4),

$$\begin{aligned}
|R| &\leqslant f(k,0) + \sum_{\substack{m=2\\ m \text{ even}}}^{s-2}\left[\binom{k-1}{k-m}+\binom{k-1}{m}\right]f(k,m) + f(k,s)\sum_{m=s}^{k-s} a_m \\
&\leqslant f(k,0) + \sum_{\substack{m=2\\ m \text{ even}}}^{s-2}\left[\binom{k-1}{m-1}+\binom{k-1}{m}\right]f(k,m) + 2^r f(k,s) \qquad (19)\\
&= \sum_{\substack{m=0\\ m \text{ even}}}^{s-2}\binom{k}{m} f(k,m) + 2^r f(k,s).
\end{aligned}$$

Now our goal is to understand for which values of k, r, s the inequality

$$\sum_{\substack{m=0\\ m \text{ even}}}^{s-2}\binom{k}{m} f(k,m) + 2^r f(k,s) \leqslant \binom{k-1}{k/2}^{\frac{r}{k-2}+1} \tag{20}$$

holds. In particular, if for every k and $r \leqslant 11k/12$, there exists such an s, then (16) and hence Theorem 6 holds.

First we replace (20) by a stronger but simpler inequality. Divide both sides of (20) by $\binom{k-1}{k/2-1}$ and bound the right-hand side from below as follows using Stirling's formula

$$2^r\left(\frac{\pi(k+1)}{2}\right)^{-\frac{r}{2(k-2)}} \leqslant \left(\frac{2^{k-1}}{\sqrt{\pi(k+1)/2}}\right)^{\frac{r}{k-2}} \leqslant \binom{k-1}{k/2-1}^{\frac{r}{k-2}}. \tag{21}$$

Thus (20) is implied by

$$\sum_{\substack{m=0\\ m \text{ even}}}^{s-2} \frac{\binom{k}{m} f(k,m)}{\binom{k-1}{k/2-1}} + \frac{2^r f(k,s)}{\binom{k-1}{k/2-1}} \leqslant 2^r \left(\frac{\pi(k+1)}{2}\right)^{-\frac{r}{2(k-2)}} \tag{22}$$

Claim 9. *Inequality* (16) *holds for every* $k \geqslant 27$*, and* $r \in \{2, \dots, \frac{k}{2\log k}\}$.

Proof. Let $s = 2$. The left-hand side of (22) equals

$$1 + 2^r \cdot 2 \frac{\binom{k-3}{(k-2)/2}}{\binom{k-1}{k/2}} = 1 + 2^r \frac{1}{2} \frac{k}{k-1}. \tag{23}$$

Since $2^{-r} \leqslant \frac{1}{4}$, we see that (22) is implied by

$$\frac{1}{4} + \frac{1}{2}\frac{k}{k-1} \leqslant \left(\frac{\pi(k+1)}{2}\right)^{-\frac{r}{2(k-2)}}. \tag{24}$$

This is equivalent to

$$r \leqslant 2(k-2) \frac{\log\left(\frac{1}{1/4 + k/(2(k-1))}\right)}{\log(\pi/2 \cdot (k+1))}. \tag{25}$$

We use that for k large enough it holds that $\frac{1}{1/4+k/(2(k-1))} \geqslant 13/10$, $2(k-2) \geqslant \frac{5}{3}k$, and

$$\log(\pi/2 \cdot (k+1)) \cdot \frac{3}{5} \cdot \frac{1}{\log(13/10)} \leqslant 2\log(k)$$

to see that the right-hand side of (25) is at least $k/(2\log k)$. □

Claim 10. *Inequality* (16) *holds for* k *large enough and every* $r \in \{\frac{k}{2\log k}, \dots, 11k/12\}$.

To prepare for the proof of Claim 10 we now further simplify the left-hand side of (22) via

$$\begin{aligned}
\frac{\binom{k}{m} f(k,m)}{\binom{k-1}{k/2-1}} &= \frac{\binom{k}{m}\binom{m}{m/2}\binom{k-m-1}{(k-m)/2}}{\binom{k-1}{k/2-1}} \\
&= \frac{k!m!(k-m-1)!(k/2-1)!(k/2)!}{m!(k-m)!\left(\frac{m}{2}!\right)^2 \frac{k-m}{2}!\left(\frac{k-m}{2}-1\right)!(k-1)!} \\
&= \frac{k(k/2-1)!}{(k-m)\frac{m}{2}!\left(\frac{k-m}{2}-1\right)!}\binom{k/2}{m/2} \\
&= \frac{\frac{k}{2}(k/2-1)!}{\frac{k-m}{2}\frac{m}{2}!\left(\frac{k-m}{2}-1\right)!}\binom{k/2}{m/2} = \binom{k/2}{m/2}^2
\end{aligned} \tag{26}$$

and

$$\begin{aligned}\frac{f(k,s)}{\binom{k-1}{k/2-1}} &= \binom{s}{s/2}\frac{\binom{k-s-1}{(k-s)/2}}{\binom{k-1}{k/2-1}}\\ &= \binom{s}{s/2}\frac{(k-s-1)!\left(\frac{k}{2}-1\right)!\frac{k}{2}!}{\frac{k-s}{2}!\left(\frac{k-s}{2}-1\right)!(k-1)!}\\ &= 2^{-s}\binom{s}{s/2}\frac{2^{s/2}\frac{\frac{k}{2}!}{\frac{k-s}{2}!}}{2^{-s/2}\frac{(k-1)!}{(k-s-1)!}\frac{\left(\frac{k-s}{2}-1\right)!}{\left(\frac{k}{2}-1\right)!}}\\ &= 2^{-s}\binom{s}{s/2}\prod_{i=0}^{s/2-1}\frac{k-2i}{k-2i-1} = 2^{-s}\binom{s}{s/2}\prod_{i=0}^{s/2-1}\left(1+\frac{1}{k-2i-1}\right).\end{aligned} \tag{27}$$

We have the upper bound $\binom{s}{s/2} \leqslant 2^s\sqrt{\frac{2}{\pi s}}$. In the product of $s/2$ terms, each term is at least 1 and the largest term is the last one. Since $s \leqslant k/2$, we can use $k-s-1 \geqslant k/2-1$ to get

$$1 \leqslant \prod_{i=0}^{s/2-1}\left(1+\frac{1}{k-2i-1}\right) \leqslant \left(1+\frac{1}{k-s-1}\right)^{s/2} \leqslant \left(1+\frac{1}{k/2-1}\right)^{k/4} \leqslant 2 \tag{28}$$

for all $k \geqslant 4$. Plugging in (26),(27) into (22), we see that (20) is implied by

$$\sum_{\substack{m=0\\ m \text{ even}}}^{s-2}\binom{k/2}{m/2}^2 + 2^r\sqrt{\frac{8}{\pi s}} \leqslant 2^r\left(\frac{\pi(k+1)}{2}\right)^{-\frac{r}{2(k-2)}}, \tag{29}$$

that is, (20) is implied by

$$2^{-r}\sum_{\substack{m=0\\ m \text{ even}}}^{s-2}\binom{k/2}{m/2}^2 + \sqrt{\frac{8}{\pi s}} \leqslant \left(\frac{\pi(k+1)}{2}\right)^{-\frac{r}{2(k-2)}}. \tag{30}$$

To further upper bound the left-hand side of (30) we use the following lemma, which we will prove later.

Lemma 11. *For any even k and $2 \leqslant s \leqslant k/2$ the following inequality holds:*

$$\frac{\sum_{\substack{m=0\\ m \text{ even}}}^{s}\binom{k/2}{m/2}^2}{\sum_{\substack{m=0\\ m \text{ even}}}^{s}\binom{k}{m}} \leqslant \frac{4}{\sqrt{\pi}}\cdot\sqrt{\frac{k}{s(k-s)}} \tag{31}$$

Remark 12. Numerics suggest that the optimal constant in the above inequality is $\sqrt{2/\pi}$ instead of $4/\sqrt{\pi}$.

Assuming that r satisfies

$$\sum_{\substack{m=0\\ m \text{ even}}}^{s-2} \binom{k}{m} \leqslant 2^r \tag{32}$$

we have

$$\begin{aligned} 2^{-r} \sum_{\substack{m=0\\ m \text{ even}}}^{s-2} \binom{k/2}{m/2}^2 + \sqrt{\frac{8}{\pi s}} &\leqslant 2^{-r} \frac{4}{\sqrt{\pi}} \cdot \sqrt{\frac{k}{s(k-s)}} \sum_{\substack{m=0\\ m \text{ even}}}^{s} \binom{k}{m} + \sqrt{\frac{8}{\pi s}} \\ &\leqslant \frac{4}{\sqrt{\pi}} \cdot \sqrt{\frac{k}{s(k-s)}} + \sqrt{\frac{8}{\pi s}} \\ &\leqslant \frac{4}{\sqrt{\pi}} \cdot \sqrt{\frac{2}{s}} + \sqrt{\frac{8}{\pi s}} = 3\sqrt{\frac{8}{\pi s}}, \end{aligned} \tag{33}$$

where the first inequality used Lemma 11, the second inequality used (32), and the third inequality used $\frac{k}{k-s} \leqslant 2$ (which holds, since $s \leqslant k/2$). Thus, assuming (32), we have that (30) is implied by

$$3\sqrt{\frac{8}{\pi s}} \leqslant \left(\frac{\pi(k+1)}{2}\right)^{-\frac{r}{2(k-2)}}. \tag{34}$$

In other words, if there is an $s \geqslant 24 \geqslant \frac{72}{\pi} = 22.9183\ldots$ such that

$$\log \sum_{\substack{m=0\\ m \text{ even}}}^{s-2} \binom{k}{m} \leqslant r \leqslant (k-2)\frac{\log s - \log \frac{72}{\pi}}{\log(k+1) + \log \frac{\pi}{2}}, \tag{35}$$

then (30) holds. We further upper bound the left-hand side of (35) by

$$\log \sum_{\substack{m=0\\ m \text{ even}}}^{s-2} \binom{k}{m} \leqslant \log \sum_{m=0}^{s-2} \binom{k}{m} \leqslant kh\Big(\frac{s}{k}\Big). \tag{36}$$

Here $h(p) \coloneqq -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function. Hence the bound in (35) is implied by

$$kh\Big(\frac{s}{k}\Big) \leqslant r \leqslant (k-2)\frac{\log s - \log \frac{72}{\pi}}{\log(k+1) + \log \frac{\pi}{2}}. \tag{37}$$

Proof of Claim 10. Use the bound of (37) with $s = 2\lfloor k^\beta/2 \rfloor$ to get that inequality (16) holds for $\beta \in (0,1)$, $k \geqslant \max\{24^{1/\beta}, 2^{1/(1-\beta)}\}$, and

$$kh(k^{\beta-1}) \leqslant r \leqslant (k-2)\frac{\log(k^\beta - 2) - \log \frac{72}{\pi}}{\log(k+1) + \log \frac{\pi}{2}}. \tag{38}$$

Fix $\beta = 1 - \frac{2\log\log k}{\log k}$. For this choice of β, we have $k \geqslant 24^{1/\beta}$ for every $k \geqslant 3500$ and clearly $k \geqslant 2^{1/(1-\beta)}$ for every $k \geqslant 3$, thereby satisfying the requirements for (38). Now observe that

$$kh(k^{\beta-1}) = kh\Big(\frac{1}{\log^2 k}\Big) \leqslant \frac{4k}{\log^2 k}\log\log k \leqslant \frac{k}{2\log k}, \tag{39}$$

where the first inequality uses the fact that for every $x \in (0, 1/2]$ it holds that $h(x) \leqslant 2x\log\frac{1}{x}$, and the second inequality holds for every $k \geqslant 13\cdot 10^{12}$. Next, for k large enough

$$\begin{aligned}(k-2)\frac{\log(k^\beta-2)-\log\frac{72}{\pi}}{\log(k+1)+\log\frac{\pi}{2}} &\geqslant (k-2)\frac{\log(k^\beta-2)-\log\frac{72}{\pi}}{\log(2k)} \geqslant (k-2)\frac{\log(k^\beta-2)-5}{\log(2k)}\\ &\geqslant (k-2)\frac{\log k^\beta - 6}{\log(2k)}.\end{aligned} \tag{40}$$

For very large k, observe that

$$(k-2)\frac{\log k^\beta - 6}{\log(2k)} \geqslant \frac{11k}{12}, \tag{41}$$

since the left-hand side divided by k goes to 1 when k goes to infinity. Putting together equations (41) and (39) along with (38), we prove the claim. □

Proof of Lemma 11. We will make use of the following variant of Stirling's formula (due to Robbins [26]), valid for all positive integers n:

$$\sqrt{2\pi n}\frac{n^n}{e^n}e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\frac{n^n}{e^n}e^{\frac{1}{12n}}. \tag{42}$$

First we bound the ratio of the individual terms (assuming $m \neq 0$) as

$$\begin{aligned}\frac{\binom{k/2}{m/2}^2}{\binom{k}{m}} &= \frac{\frac{k}{2}!^2 m!(k-m)!}{\frac{m}{2}!^2\frac{k-m}{2}!^2 k!}\\ &\leqslant \frac{1}{\sqrt{2\pi}}\sqrt{\frac{\frac{k^2}{4}m(k-m)}{\frac{m^2}{4}\frac{(k-m)^2}{4}k}}\frac{\left(\frac{k}{2}\right)^k m^m(k-m)^{k-m}}{\left(\frac{m}{2}\right)^m\left(\frac{k-m}{2}\right)^{k-m}k^k}\\ &\cdot\exp\left\{\frac{1}{3k}+\frac{1}{12m}+\frac{1}{12(k-m)}-\frac{2}{6m+1}-\frac{2}{6(k-m)+1}-\frac{1}{12k+1}\right\}\\ &\leqslant \sqrt{\frac{2}{\pi}}\sqrt{\frac{k}{m(k-m)}},\end{aligned} \tag{43}$$

since the third factor is 1 and the argument of the exponential is negative if $2 \leqslant m \leqslant \frac{k}{2}$.

Now let us turn to the ratio of the sums. Let $0 < c_1 < 2c_1 < c_2 < \frac{1}{2}$ be fixed constants. Assume first that $2 \leqslant s \leqslant c_2 k$. The denominator can be bounded from below by its last term, while the numerator can be bounded from above as

$$\begin{aligned}\sum_{\substack{m=0\\ m \text{ even}}}^{s} \binom{k/2}{m/2}^2 = \sum_{i=0}^{s/2} \binom{k/2}{i}^2 = \sum_{j=0}^{s/2} \binom{k/2}{s/2-j}^2 &\leqslant \sum_{j=0}^{s/2} \binom{k/2}{s/2}^2 \left(\frac{s}{k-s}\right)^{2j} \\ &\leqslant \sum_{j=0}^{\infty} \binom{k/2}{s/2}^2 \left(\frac{s}{k-s}\right)^{2j} \\ &= \binom{k/2}{s/2}^2 \frac{(k-s)^2}{k(k-2s)} \\ &\leqslant \binom{k/2}{s/2}^2 \frac{(1-c_2)^2}{1-2c_2},\end{aligned} \tag{44}$$

where in the first inequality we have used

$$\frac{\binom{k/2}{n}}{\binom{k/2}{n+1}} = \frac{n+1}{\frac{k}{2}-n} \leqslant \frac{\frac{s}{2}-1+1}{\frac{k}{2}-\frac{s}{2}+1} \leqslant \frac{s}{k-s} \tag{45}$$

for $n+1 \leqslant s/2$. Combining with (43) we arrive at the estimate

$$\frac{\sum_{\substack{m=0\\ m \text{ even}}}^{s} \binom{k/2}{m/2}^2}{\sum_{\substack{m=0\\ m \text{ even}}}^{s} \binom{k}{m}} \leqslant \frac{1-c_2}{1-2c_2} \frac{\binom{k/2}{s/2}^2}{\binom{k}{s}} \leqslant \frac{1-c_2}{1-2c_2} \sqrt{\frac{2}{\pi}} \sqrt{\frac{k}{s(k-s)}}. \tag{46}$$

Now we turn to the case when $c_2 k \leqslant s \leqslant k/2$. Split the sum in the numerator into two at $m \approx c_1 k$. For $m \leqslant \lfloor c_1 k \rfloor$ we use the simple bound $\binom{k/2}{m/2}^2 \leqslant \binom{k}{m}$, while for $m \geqslant \lfloor c_1 k \rfloor + 1 \geqslant c_1 k$ we use (43) to get

$$\frac{\binom{k/2}{m/2}^2}{\binom{k}{m}} \leqslant \sqrt{\frac{2}{\pi}} \sqrt{\frac{k}{m(k-m)}} \leqslant \sqrt{\frac{2}{\pi}} \frac{1}{\sqrt{k}} \frac{1}{\sqrt{c_1(1-c_1)}}. \tag{47}$$

Introducing

$$A = \sum_{\substack{m=0\\ m \text{ even}}}^{2\lfloor c_1 k/2 \rfloor} \binom{k}{m}, \qquad B = \sum_{\substack{m=2\lfloor c_1 k/2 \rfloor + 2\\ m \text{ even}}}^{s} \binom{k}{m}. \tag{48}$$

The estimate

$$\frac{\sum\limits_{\substack{m=0\\ m \text{ even}}}^{s} \binom{k/2}{m/2}^2}{\sum\limits_{\substack{m=0\\ m \text{ even}}}^{s} \binom{k}{m}} \leqslant \frac{A + \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{k}}\frac{1}{\sqrt{c_1(1-c_1)}}B}{A+B} = \frac{\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{k}}\frac{1}{\sqrt{c_1(1-c_1)}} + \frac{A}{B}}{1+\frac{A}{B}} \leqslant \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{k}}\frac{1}{\sqrt{c_1(1-c_1)}} + \frac{A}{B} \tag{49}$$

follows. The ratio

$$\frac{\binom{k}{n}}{\binom{k}{n-1}} = \frac{k-n+1}{n} = \frac{k+1}{n} - 1 \tag{50}$$

is monotonically decreasing in n, therefore, by induction

$$\frac{\binom{k}{b-t}}{\binom{k}{a-t}} \geqslant \frac{\binom{k}{b}}{\binom{k}{a}} \tag{51}$$

whenever $a \leqslant b$. Apply this with $a = 2\lfloor c_1 k/2 \rfloor$, $b = s$ and $t = 2\lfloor c_1 k/2 \rfloor - m$ to get

$$\begin{aligned} A = \sum_{\substack{m=0\\ m \text{ even}}}^{2\lfloor c_1 k/2 \rfloor} \binom{k}{m} &= \sum_{\substack{m=0\\ m \text{ even}}}^{2\lfloor c_1 k/2 \rfloor} \binom{k}{m+s-2\lfloor c_1 k/2 \rfloor} \frac{\binom{k}{m}}{\binom{k}{m+s-2\lfloor c_1 k/2 \rfloor}} \\ &\leqslant \sum_{\substack{m=0\\ m \text{ even}}}^{2\lfloor c_1 k/2 \rfloor} \binom{k}{m+s-2\lfloor c_1 k/2 \rfloor} \frac{\binom{k}{2\lfloor c_1 k/2 \rfloor}}{\binom{k}{s}} \\ &= \frac{\binom{k}{2\lfloor c_1 k/2 \rfloor}}{\binom{k}{s}} \sum_{\substack{m=s-2\lfloor c_1 k/2 \rfloor\\ m \text{ even}}}^{s} \binom{k}{m} \leqslant \frac{\binom{k}{2\lfloor c_1 k/2 \rfloor}}{\binom{k}{s}} B, \end{aligned} \tag{52}$$

that is,

$$\frac{A}{B} \leqslant \frac{\binom{k}{2\lfloor c_1 k/2 \rfloor}}{\binom{k}{s}} \leqslant 2^{k(h(c_1)-h(s/k))}\sqrt{8k\frac{s}{k}\left(1-\frac{s}{k}\right)} \leqslant 2^{k(h(c_1)-h(c_2))}\sqrt{2k}. \tag{53}$$

We now look for a constant C that satisfies

$$\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{k}}\frac{1}{\sqrt{c_1(1-c_1)}} + 2^{k(h(c_1)-h(c_2))}\sqrt{2k} \leqslant C \cdot \sqrt{\frac{k}{s(k-s)}} \tag{54}$$

when $c_2 k \leqslant s \leqslant k/2$. Equivalently, we need

$$\sqrt{\frac{2}{\pi}}\sqrt{\frac{s}{k}\left(1-\frac{s}{k}\right)}\frac{1}{\sqrt{c_1(1-c_1)}} + \sqrt{2}\cdot 2^{k(h(c_1)-h(c_2))}k\sqrt{\frac{s}{k}\left(1-\frac{s}{k}\right)} \leqslant C. \tag{55}$$

Using $\sqrt{\frac{s}{k}\left(1-\frac{s}{k}\right)} \leqslant \frac{1}{2}$ and that $2^{k(h(c_1)-h(c_2))}k$ has a global maximum at $k = \frac{1}{\ln 2}\frac{1}{h(c_2)-h(c_1)}$, an upper bound on the left-hand side is

$$\frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{c_1(1-c_1)}} + \frac{1}{\sqrt{2e\ln 2}}\frac{1}{h(c_2)-h(c_1)}. \tag{56}$$

In particular, with $c_1 = 0.09711\ldots$ and $c_2 = 0.39252\ldots$ we get $C = 2.25503\ldots < \frac{4}{\sqrt{\pi}}$. □

4 Case: high dimension

Finally, in this section we consider the remaining high-dimensional case.

Theorem 13. *For any large enough even $k \in \mathbb{N}_{\geqslant 4}$ and subspace*

$$V \subseteq \{x \in \mathbb{F}_2^k : x_k = 0\} \subseteq \mathbb{F}_2^k$$

such that $\dim_{\mathbb{F}_2}(V) \geqslant 11(k-1)/12$, the inequality

$$\left|\left\{(x,y) \in \mathbb{F}_2^k \times \mathbb{F}_2^k : |x| = |y| = \tfrac{k}{2},\, x-y \in V\right\}\right| \leqslant \binom{k-1}{k/2}^{\frac{\dim_{\mathbb{F}_2}(V)}{k-2}+1}$$

holds. Here $|x|$ denotes the Hamming weight of $x \in \mathbb{F}_2^k$.

4.1 Preliminaries

Our proof of Theorem 13 uses Fourier analysis on the Boolean cube $\mathbb{F}_2^n = \{0,1\}^n$, the Krawchouk polynomials, an upper bound on the size of Hamming layers in subspaces and some elementary bounds for expressions involving binomial coefficients.

4.1.1 Fourier transform

For $z \in \{0,1\}^n$ define the function $\chi_z : \{0,1\}^n \to \mathbb{R}$ by $\chi_z(x) = (-1)^{z\cdot x}$ where we use the notation $z \cdot x = \sum_i z_i x_i$. These so-called *characters* form an orthonormal basis for the space of functions $\{0,1\}^n \to \mathbb{R}$ for the inner product $\langle f, g\rangle = \frac{1}{2^n}\sum_x f(x)g(x)$. For a function $f : \{0,1\}^n \to \mathbb{R}$ define $\widehat{f} : \{0,1\}^n \to \mathbb{R}$ by $\widehat{f}(z) = \langle f, \chi_z\rangle = \frac{1}{2^n}\sum_x f(x)\chi_z(x)$. The function $\widehat{f}$ is the *Fourier transform of f*. Then $f(x) = \sum_z \widehat{f}(z)\chi_z(x)$, which is called the *Fourier expansion* of f. One verifies that for any functions $f, g : \{0,1\}^n \to \mathbb{R}$ we have the identity

$$\sum_{x,y} f(x)f(y)g(x+y) = 2^{2n}\sum_z \widehat{f}(z)^2\widehat{g}(z) \tag{57}$$

with sums over $x, y \in \{0,1\}^n$ and $z \in \{0,1\}^n$, and where we recall that the addition in $\{0,1\}^n$ is modulo 2. Indeed, by taking the Fourier expansion of f and g, then using $\chi_U(x+y) = \chi_U(x)\chi_U(y)$, and then using the orthonormality of the characters, we find

$$\begin{aligned}
\sum_{x,y} f(x)f(y)g(x+y) &= \sum_{x,y} \sum_{S,T,U} \widehat{f}(S)\,\widehat{f}(T)\,\widehat{g}(U)\,\chi_S(x)\,\chi_T(y)\,\chi_U(x+y) \\
&= \sum_{S,T,U} \widehat{f}(S)\,\widehat{f}(T)\,\widehat{g}(U)\,2^n\langle\chi_S(x),\chi_U(x)\rangle\,2^n\langle\chi_T(y),\chi_U(y)\rangle \\
&= 2^{2n} \sum_{S,T,U} \widehat{f}(S)\,\widehat{f}(T)\,\widehat{g}(U)\,[S=U]\,[T=U] \\
&= 2^{2n} \sum_{S} \widehat{f}(S)\,\widehat{f}(S)\,\widehat{g}(S).
\end{aligned}$$

Here $[S = U]$ is the indicator function that is 1 when $S = U$ and 0 otherwise.

4.1.2 Krawchouk polynomials

For $0 \leqslant k \leqslant n$ define the function

$$K_k^n : \{0,1\}^n \to \mathbb{R}$$

as the sum of the characters χ_z with $z \in \{0,1\}^n$ and $|z| = k$, that is

$$K_k^n(x) = \sum_{|z|=k} \chi_z(x).$$

The function $K_k^n(x)$ depends only on the Hamming weight $|x|$ and can thus be interpreted as a function on integers $0 \leqslant t \leqslant n$. This function may be written as $K_k^n(t) = \sum_{j=0}^{k} (-1)^j \binom{t}{j}\binom{n-t}{k-j}$ and this defines a real polynomial of degree k, called the *kth Krawchouk polynomial*. We will use the following expression for the "middle" Krawchouk polynomial for odd n.

Lemma 14 (Proposition 4.4 in [13])**.** *Let n be odd and $t \in \{0,\ldots,n\}$. Then*

$$K^n_{\frac{n-1}{2}}(t) = (-1)^{\lfloor t/2 \rfloor} \binom{n}{(n-1)/2} \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}}{\binom{n}{t}}.$$

We will encounter the Krawchouk polynomials in the following way. For any $0 \leqslant k \leqslant n$ define the function $w_k^n : \{0,1\}^n \to \{0,1\}$ by $w_k^n(z) = [|z| = k]$. Then

$$\widehat{w_k^n}(z) = \frac{1}{2^n} \sum_x w_k^n(x)(-1)^{x\cdot z} = \frac{1}{2^n} K_k^n(|z|). \tag{58}$$

We will use the following observation later. Let $A \subseteq \{0,1\}^n$. The *characteristic function* $f : \{0,1\}^n \to \{0,1\}$ of A is defined by $f(x) = [x \in A]$. Now suppose A is a linear subspace. Let $A^\perp \coloneqq \{y \in \{0,1\}^n : y \cdot x = 0 \text{ for all } x \in A\}$ be the orthogonal complement of A. The Fourier transform of f is given by

$$\widehat{f}(z) = \frac{[z \in A^\perp]}{|A^\perp|}. \tag{59}$$

Indeed, $\widehat{f}(z) = \frac{1}{2^n}\sum_{x\in A}(-1)^{x\cdot z}$ and, if $z \in A^\perp$, then this sum equals $\frac{1}{2^n}|A|$. On the other hand, if $z \notin A^\perp$, say $x_0 \cdot z = 1$, then $\sum_{x\in A}(-1)^{x\cdot z} = \sum_{x\in A}(-1)^{(x+x_0)z} = (-1)\sum_{x\in A}(-1)^{x\cdot z}$ so the sum equals zero.

4.1.3 Size of Hamming layers

Given a subspace $V \subseteq \{0,1\}^n$ of dimension d and an integer $0 \leqslant t \leqslant n$, let $V_t \subseteq V$ be the elements with (Hamming) weight t, let $V_{\leqslant t} \subseteq V$ be the elements with weight at most t and let $V_{\geqslant t} \subseteq V$ be the elements with weight at least t. We want to upper bound the size of V_t and the size of V_{n-t}.

In the first version of this paper that appeared on the arXiv we used a consequence of the KKL inequality [18] from [22] to get the upper bound $|V_t| \leqslant (2e\ln(2)d/t)^t$ for $1 \leqslant t \leqslant \ln(2)d$. The following slightly better upper bound that we learned from Swastik Kopparty simplifies the proofs that follow, and it has a short proof.

Lemma 15. *Let $V \subseteq \{0,1\}^n$ be a subspace of dimension d. Then*

$$|V_t| \leqslant |V_{\leqslant t}| \leqslant \sum_{i=0}^{t}\binom{d}{i} \quad \textit{and} \quad |V_{n-t}| \leqslant |V_{\geqslant n-t}| \leqslant \sum_{i=n-t}^{n}\binom{d}{i} = \sum_{i=0}^{t}\binom{d}{i}.$$

If $1 \leqslant t \leqslant d$, then

$$\sum_{i=0}^{t}\binom{d}{t} \leqslant \frac{(ed)^t}{t^t}.$$

Proof. We pick a basis of V and write the basis elements as columns of an $n \times d$ matrix M. We may assume (after column operations and row permutations) that the bottom $d \times d$ block of this matrix is the identity matrix. The top $(n-d) \times d$ block is arbitrary.

We will upper bound $|V_{\leqslant t}|$. The bottom d coefficients of each column of M have exactly 1 one. The bottom d coefficients of any sum of k columns of M have exactly k ones (and potentially also ones in the top $n-d$ coefficients). Thus for this sum to have weight at most t we require $k \leqslant t$. There are $\sum_{i=0}^{t}\binom{d}{i}$ ways to choose those vectors, and so $|V_{\leqslant t}| \leqslant \sum_{i=0}^{t}\binom{d}{i}$.

We want to upper bound $|V_{\geqslant n-t}|$, the number of vectors in V with at least $n-t$ ones. That is, we want to upper bound the number of vectors in V with at most t zeros. The bottom d coefficients of each column of M have exactly $d-1$ zeros. The bottom d coefficients of any sum of k columns of M have exactly $d-k$ zeros (and potentially also

zeros in the top $n-d$ coefficients). Thus for this sum to have at most t zeros, we require $d-k \leqslant t$, that is, $k \geqslant d-t$. There are $\sum_{i=d-t}^{d} \binom{d}{i}$ ways to choose those vectors, and thus $|V_{\geqslant n-t}| \leqslant \sum_{i=d-t}^{d} \binom{d}{i} = \sum_{i=0}^{t} \binom{d}{t}$.

The sum of binomial coefficients we upper bound as follows:

$$\sum_{i=0}^{t} \binom{d}{i} \leqslant \sum_{i=0}^{t} \frac{d^i}{i!} = \sum_{i=0}^{t} \frac{d^i}{t^i} \frac{t^i}{i!} \leqslant \frac{d^t}{t^t} \sum_{i=0}^{\infty} \frac{t^i}{i!} \leqslant \frac{d^t}{t^t} e^t,$$

using that $d/t \geqslant 1$. □

4.1.4 Bounds involving binomial coefficients

Lemma 16. *Let n be even.*

(i) *If $0 \leqslant m \leqslant n/3$, then*

$$\frac{\binom{n/2}{m}}{\binom{n+1}{2m+1}} \leqslant 2\left(\frac{2m+1}{2(n-m+1)}\right)^{m+1}.$$

(ii) *If $1 \leqslant m \leqslant (n+1)/3$, then*

$$\frac{\binom{n/2}{m}}{\binom{n+1}{2m}} \leqslant \left(\frac{m}{n-m+1}\right)^{m}.$$

Proof. We expand the binomial coefficients as fractions of factorials:

$$\begin{aligned}
\frac{\binom{n/2}{m}}{\binom{n+1}{2m+1}} &= \frac{(n/2)!(2m+1)!(n-2m)!}{m!(n/2-m)!(n+1)!} \\
&= \frac{(n/2)\cdots(n/2-m+1)}{(n+1)\cdots(n-m+2)} \cdot \frac{(2m+1)\cdots(m+1)}{(n-m+1)\cdots(n-2m+1)} \\
&\leqslant 2\left(\frac{2m+1}{2(n-m+1)}\right)^{m+1}
\end{aligned}$$

where in the last inequality we upper bounded each of the first m terms by $1/2$ and each of the last $m+1$ terms by $(2m+1)/(n-m+1)$ using the assumption $m \leqslant n/3$. We do the same for the other inequality:

$$\begin{aligned}
\frac{\binom{n/2}{m}}{\binom{n+1}{2m}} &= \frac{(n/2)!(2m)!(n+1-2m)!}{m!(n/2-m)!(n+1)!} \\
&= \frac{(n/2)\cdots(n/2-m+1)}{(n+1)\cdots(n-m+2)} \cdot \frac{(2m)\cdots(m+1)}{(n-m+1)\cdots(n-2m+2)} \\
&\leqslant \left(\frac{m}{n-m+1}\right)^{m}
\end{aligned}$$

where in the last inequality we upper bounded each of the first m terms by $1/2$ and each of the last m terms by $(2m)/(n-m+1)$ using the assumption $1 \leqslant m \leqslant (n+1)/3$. □

4.2 Proof of Theorem 13

Proof of Theorem 13. Let $n \in \mathbb{N}$ be large enough. Let $V \subseteq \{0,1\}^n$ be a subspace of dimension at least $11n/12$. We will prove that

$$\left|\left\{(x,y) \in (\{0,1\}^n)^{\times 2} : |x| = |y| = \tfrac{n-1}{2}, x+y \in V\right\}\right| \leqslant \binom{n}{\frac{n-1}{2}}^{1+\frac{\dim_{\mathbb{F}_2}(V)}{n-1}}. \tag{60}$$

This proves the theorem. To see this, in the theorem statement, set $k = n+1$, ignore the $(n+1)$th coordinate, and note that the size of $\left\{(x,y) \in (\{0,1\}^n)^{\times 2} : |x| = |y| = \frac{n-1}{2}, x+y \in V\right\}$ equals the size of $\left\{(x,y) \in (\{0,1\}^n)^{\times 2} : |x| = |y| = \frac{n+1}{2}, x+y \in V\right\}$ via the bijection that flips the bits of x and y.

Let $f : \{0,1\}^n \to \{0,1\}$ be the characteristic function of V, that is, $f(x) = [x \in V]$. Recall that we defined the function $w_k^n : \{0,1\}^n \to \{0,1\}$ by $w_k^n(x) = [|x| = k]$. Using equation (57) the left-hand side of (60) can be rewritten as

$$\begin{aligned}
&\left|\left\{(x,y) \in (\{0,1\}^n)^{\times 2} : |x| = |y| = \tfrac{n-1}{2}, x+y \in V\right\}\right| \\
&= \sum_{x,y} w^n_{\frac{n-1}{2}}(x) w^n_{\frac{n-1}{2}}(y) f(x+y) \\
&= 2^{2n} \sum_z \widehat{w}^n_{\frac{n-1}{2}}(z)^2 \widehat{f}(z)
\end{aligned}$$

with sums over $x, y \in \{0,1\}^n$ and $z \in \{0,1\}^n$. Since $\widehat{w}_k^n(z) = \frac{1}{2^n} K_k^n(|z|)$ (see (58)) and $\widehat{f}(z) = \frac{1}{2^n}|V| \cdot [z \in V^\perp]$ (see (59)) we have

$$2^{2n} \sum_z \widehat{w}^n_{\frac{n-1}{2}}(z)^2 \widehat{f}(z) = \frac{|V|}{2^n} \sum_z K^n_{\frac{n-1}{2}}(|z|)^2 [z \in V^\perp]. \tag{61}$$

Recall that $(V^\perp)_t$ denotes the subset of $V^\perp$ consisting of vectors with Hamming weight t. We rewrite the right-hand side of (61) as a sum over the Hamming weight $t = |z| \in \{0, \ldots, n\}$.

$$\frac{|V|}{2^n} \sum_z K^n_{\frac{n-1}{2}}(|z|)^2 [z \in V^\perp] = \frac{|V|}{2^n} \sum_t K^n_{\frac{n-1}{2}}(t)^2 \left|(V^\perp)_t\right|. \tag{62}$$

By Lemma 14 we have

$$K^n_{\frac{n-1}{2}}(t)^2 = \binom{n}{(n-1)/2}^2 \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2}{\binom{n}{t}^2}$$

which we use to rewrite (62) as

$$\frac{|V|}{2^n}\left(\sum_t K^n_{\frac{n-1}{2}}(t)^2\left|(V^\perp)_t\right|\right) = \frac{|V|}{2^n}\binom{n}{\frac{n-1}{2}}^2\left(\sum_t \frac{\binom{(n-1)/2}{\lfloor t/2\rfloor}^2}{\binom{n}{t}^2}\left|(V^\perp)_t\right|\right)$$
$$= \frac{|V|}{2^n}\binom{n}{\frac{n-1}{2}}^2\left(1+[1^n\in V^\perp]+\sum_{1\leqslant t\leqslant n-1}\frac{\binom{(n-1)/2}{\lfloor t/2\rfloor}^2}{\binom{n}{t}^2}\left|(V^\perp)_t\right|\right). \tag{63}$$

We assumed that $\dim(V)\geqslant 11n/12$. Since the statement of the theorem is directly verified to be true when $\dim(V)=n-1$ we may in addition assume that $\dim(V)<n-1$. We define $c=n-\dim(V)$. Then $2\leqslant c\leqslant n/12$. Let

$$f(n,c) \coloneqq 40\frac{c^2}{n^2}+\left(\frac{2c}{n}\right)^c.$$

In Lemma 17 and Lemma 18 below we will prove the inequalities

$$\sum_{1\leqslant t\leqslant n-1}\frac{\binom{(n-1)/2}{\lfloor t/2\rfloor}^2}{\binom{n}{t}^2}\left|(V^\perp)_t\right| \leqslant f(n,c) \tag{64}$$

$$2+f(n,c)\leqslant 2^c\binom{n}{\frac{n-1}{2}}^{\frac{1-c}{n-1}}. \tag{65}$$

These inequalities show that (63) is upper bounded as follows:

$$\begin{aligned}
&\frac{|V|}{2^n}\binom{n}{\frac{n-1}{2}}^2\left(1+[1^n\in V^\perp]+\sum_{1\leqslant t\leqslant n-1}\frac{\binom{(n-1)/2}{\lfloor t/2\rfloor}^2}{\binom{n}{t}^2}\left|(V^\perp)_t\right|\right)\\
&\leqslant \frac{|V|}{2^n}\binom{n}{\frac{n-1}{2}}^2\big(2+f(n,c)\big)\\
&\leqslant \frac{|V|}{2^n}\binom{n}{\frac{n-1}{2}}^2 2^c\binom{n}{\frac{n-1}{2}}^{\frac{1-c}{n-1}}\\
&= \binom{n}{\frac{n-1}{2}}^{1+\frac{\dim(V)}{n-1}}
\end{aligned}$$

which proves the theorem. □

Lemma 17. *Let n be odd. For $2\leqslant c\leqslant n/12$ such that $\dim(V)=n-c$ we have*

$$\sum_{1\leqslant t\leqslant n-1}\frac{\binom{(n-1)/2}{\lfloor t/2\rfloor}^2}{\binom{n}{t}^2}\left|(V^\perp)_t\right| \leqslant f(n,c).$$

with

$$f(n,c) \coloneqq 40\frac{c^2}{n^2}+\left(\frac{2c}{n}\right)^c.$$

Proof of Lemma 17. We first upper bound the sum over $t \in [1, c-1] \cup [n-c+1, n-1]$ and afterwards the sum over the remaining t's. We use $\binom{(n-1)/2}{\lfloor t/2 \rfloor} = \binom{(n-1)/2}{\lfloor (n-t)/2 \rfloor}$ and then apply Lemma 15 to get

$$\begin{aligned}
&\sum_{t=1}^{c} \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2}{\binom{n}{t}^2} \left|(V^\perp)_t\right| + \sum_{t=n-c}^{n-1} \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2}{\binom{n}{t}^2} \left|(V^\perp)_t\right| \\
&= \sum_{t=1}^{c} \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2}{\binom{n}{t}^2} \Big(\left|(V^\perp)_t\right| + \left|(V^\perp)_{n-t}\right| \Big) \\
&\leqslant 2 \sum_{t=1}^{c} \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2}{\binom{n}{t}^2} \left(\frac{ec}{t}\right)^t . \qquad (66)
\end{aligned}$$

Because of the floor in (66), we upper bound the sum over even t and the sum over odd t separately. For the even part we use Lemma 16 (ii) and replace t by $2t$ to get

$$\begin{aligned}
\sum_{\substack{t=1 \\ \text{even}}}^{c} \frac{\binom{(n-1)/2}{t/2}^2}{\binom{n}{t}^2} \left(\frac{ec}{t}\right)^t &\leqslant \sum_{\substack{t=1 \\ \text{even}}}^{c} \left(\frac{t}{2n-t}\right)^t \left(\frac{ec}{t}\right)^t \\
&= \sum_{\substack{t=1 \\ \text{even}}}^{c} \left(\frac{ec}{2n-t}\right)^t .
\end{aligned}$$

For the odd part we use Lemma 16 (i), use $4(\frac{t}{2n-t+1}) \leqslant 1$, shift t by 1, and use $ec \leqslant 2n-t$ to get

$$\begin{aligned}
\sum_{\substack{t=1 \\ \text{odd}}}^{c-1} \frac{\binom{(n-1)/2}{(t-1)/2}^2}{\binom{n}{t}^2} \left(\frac{ec}{t}\right)^t &\leqslant \sum_{\substack{t=1 \\ \text{odd}}}^{c-1} 4 \left(\frac{t}{2n-t+1}\right)^{t+1} \left(\frac{ec}{t}\right)^t \\
&\leqslant \sum_{\substack{t=1 \\ \text{odd}}}^{c-1} \left(\frac{t}{2n-t+1}\right)^t \left(\frac{ec}{t}\right)^t \\
&= \sum_{\substack{t=1 \\ \text{odd}}}^{c-1} \left(\frac{ec}{2n-t+1}\right)^t \\
&= \sum_{\substack{t=1 \\ \text{even}}}^{c} \left(\frac{ec}{2n-t}\right)^{t+1} \\
&\leqslant \sum_{\substack{t=1 \\ \text{even}}}^{c} \left(\frac{ec}{2n-t}\right)^t .
\end{aligned}$$

We upper bound both the even and the odd part as follows, replacing t by $2t$ and using $t \leqslant c/2$ and $c \leqslant n/12$:

$$\sum_{\substack{t=1 \\ \text{even}}}^{c} \left(\frac{ec}{2n-t}\right)^t = \sum_{t=1}^{c/2} \left(\frac{ec}{n-2t}\right)^{2t} \leqslant \sum_{t=1}^{\infty} \left(\frac{ec}{n-2t}\right)^{2t} \leqslant \frac{c^2e^2}{c^2\left(1-e^2\right)-2cn+n^2} \leqslant 10\frac{c^2}{n^2}. \tag{67}$$

We conclude that (66) is upper bounded by $40c^2/n^2$.

Finally, to upper bound the sum over the remaining ts we use the basic inequalities $\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2 \leqslant \binom{n}{t}$ and $(\frac{n}{k})^k \leqslant \binom{n}{k}$ to get

$$\sum_{t=c}^{n-c} \frac{\binom{(n-1)/2}{\lfloor t/2 \rfloor}^2}{\binom{n}{t}^2} \left|(V^\perp)_t\right| \leqslant \sum_{t=c}^{n-c} \frac{\left|(V^\perp)_t\right|}{\binom{n}{t}} \leqslant \frac{1}{\binom{n}{c}} \sum_{t=c}^{n-c} \left|(V^\perp)_t\right| \leqslant \frac{1}{\binom{n}{c}} \left|V^\perp\right| \leqslant \left(\frac{c}{n}\right)^c 2^c.$$

This finishes the proof. □

Lemma 18. *For large enough odd n and $2 \leqslant c \leqslant n/12$ we have*

$$2 + f(n,c) \leqslant 2^c \binom{n}{\frac{n-1}{2}}^{\frac{1-c}{n-1}}.$$

where

$$f(n,c) \coloneqq 40\frac{c^2}{n^2} + \left(\frac{2c}{n}\right)^c.$$

Proof of Lemma 18. For odd n we have $2^n/\sqrt{n} \geqslant \binom{n}{(n-1)/2}$ and thus

$$2^{1+\frac{1-c}{n-1}} \sqrt{n}^{\frac{c-1}{n-1}} = 2^c \left(\frac{2^n}{\sqrt{n}}\right)^{\frac{1-c}{n-1}} \leqslant 2^c \binom{n}{\frac{n-1}{2}}^{\frac{1-c}{n-1}}.$$

It is thus sufficient to show that for large enough n and $2 \leqslant c \leqslant n/12$ we have the inequality $2 + f(n,c) \leqslant 2(\sqrt{n}/2)^{\frac{c-1}{n-1}}$. One verifies that $2 + f(n,2) \leqslant 2(\sqrt{n}/2)^{\frac{2-1}{n-1}}$ holds for, say, every $n \geqslant 70$. To see that for large enough n the function $f_n(c) = 2(\sqrt{n}/2)^{\frac{c-1}{n-1}} - (2 + f(n,c))$ is increasing in c for $2 \leqslant c \leqslant n/12$, we compute the derivative

$$\frac{\mathrm{d}}{\mathrm{d}c} f_n(c) = (\sqrt{n}/2)^{\frac{c-1}{n-1}} \frac{\ln(n/4)}{n-1} - \frac{80c}{n^2} - (2c/n)^c \ln(2ce/n)$$

Using $c \leqslant n/12$ and for n large enough one verifies that $\frac{\mathrm{d}}{\mathrm{d}c} f_n(c) \geqslant 0$, which proves the lemma. □

Acknowledgements

Jeroen Zuiddam thanks Florian Speelman, Pjotr Buys, Avi Wigderson and Swastik Kopparty for helpful discussions.

References

[1] Josh Alman. Limits on the Universal Method for Matrix Multiplication. In Amir Shpilka, editor, *34th Computational Complexity Conference (CCC 2019)*, volume 137, pages 12:1–12:24, 2019. arXiv:1812.08731, doi:10.4230/LIPIcs.CCC.2019.12.

[2] Noga Alon and Asaf Shapira. On an extremal hypergraph problem of Brown, Erdős and Sós. *Combinatorica*, 26(6):627–645, 2006.

[3] Andreas Bärtschi and Stephan Eidenbenz. Deterministic preparation of Dicke states. Fundamentals of Computation Theory (FCT 2019). Lecture Notes in Computer Science, volume 11651, Springer. doi:10.1007/978-3-030-25027-0_9, arXiv:1904.07358.

[4] Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin, and Chris Umans. On cap sets and the group-theoretic approach to matrix multiplication. *Discrete Anal.*, 2017. arXiv:1605.06702, doi:10.19086/da.1245.

[5] Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A Grochow, and Chris Umans. Which groups are amenable to proving exponent two for matrix multiplication? *arXiv*, 2017. arXiv:1712.02302.

[6] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren Math. Wiss.* Springer-Verlag, Berlin, 1997. doi:10.1007/978-3-662-03338-8.

[7] Matthias Christandl, Péter Vrana, and Jeroen Zuiddam. Asymptotic tensor rank of graph tensors: beyond matrix multiplication. *Comput. Complexity*, 2018. arXiv:1609.07476, doi:10.1007/s00037-018-0172-8.

[8] Matthias Christandl, Péter Vrana, and Jeroen Zuiddam. Universal points in the asymptotic spectrum of tensors. In *Proceedings of 50th Annual ACM SIGACT Symposium on the Theory of Computing (STOC 2018)*. ACM, New York, 2018. arXiv:1709.07851, doi:10.1145/3188745.3188766.

[9] Matthias Christandl, Péter Vrana, and Jeroen Zuiddam. Barriers for Fast Matrix Multiplication from Irreversibility. In Amir Shpilka, editor, *34th Computational Complexity Conference (CCC 2019)*, volume 137, pages 26:1–26:17, Dagstuhl, Germany, 2019. arXiv:1812.06952, doi:10.4230/LIPIcs.CCC.2019.26.

[10] Don Coppersmith and Shmuel Winograd. Matrix multiplication via arithmetic progressions. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 1–6. ACM, 1987.

[11] Robert H. Dicke. Coherence in spontaneous radiation processes. *Phys. Rev.*, 93(1):99, 1954. doi:10.1103/PhysRev.93.99.

[12] Jordan S. Ellenberg and Dion Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Ann. of Math. (2)*, 185(1):339–343, 2017. doi:10.4007/annals.2017.185.1.8.

[13] Philip Feinsilver. Sums of squares of Krawtchouk polynomials, Catalan numbers, and some algebras over the Boolean lattice. *Int. J. Math. Comput. Sci.*, 12(1):65–83, 2017. arXiv:1603.07023.

[14] Jacob Fox, László Miklós Lovász, and Lisa Sauermann. A polynomial bound for the arithmetic k-cycle removal lemma in vector spaces. *J. Combin. Theory Ser. A*, 160:186–201, 2018. doi:10.1016/j.jcta.2018.06.004

[15] Hu Fu and Robert Kleinberg. Improved Lower Bounds for Testing Triangle-freeness in Boolean Functions via Fast Matrix Multiplication. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2014)*, pages 669–676, 2014. doi:10.4230/LIPIcs.APPROX-RANDOM.2014.669.

[16] Johan Håstad. Tensor rank is NP-complete. *J. Algorithms*, 11(4):644–654, 1990. doi:10.1016/0196-6774(90)90014-6.

[17] Ishay Haviv and Ning Xie. Sunflowers and testing triangle-freeness of functions. *Comput. Complexity*, 26(2):497–530, 2017. doi:10.1007/s00037-016-0138-7.

[18] Jeff Kahn, Gil Kalai, and Nathan Linial. The influence of variables on Boolean functions. In *29th Annual Symposium on Foundations of Computer Science (FOCS) 1988*, pages 68–80. IEEE, 1988. doi:10.1109/SFCS.1988.21923.

[19] Robert Kleinberg, William F. Sawin, and David E. Speyer. The growth rate of tri-colored sum-free sets. *Discrete Anal.*, 2018. doi:10.19086/da.3734, arXiv:1607.00047.

[20] Joseph M. Landsberg. *Tensors: geometry and applications*, volume 128 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2012.

[21] László Miklós Lovász and Lisa Sauermann. A lower bound for the k-multicolored sum-free problem in $\mathbb{Z}_m^n$. *Proc. London Math. Soc.*, 2018. doi:10.1112/plms.12223, arXiv:1804.08837.

[22] Ashley Montanaro. A new exponential separation between quantum and classical one-way communication complexity. *Quantum Inf. Comput.*, 11(7-8):574–591, 2011. http://dl.acm.org/citation.cfm?id=2230916.2230919, arXiv:1007.3587.

[23] Sergey Norin. A distribution on triples with maximum entropy marginal. *Forum Math. Sigma*, volume 7, Cambridge University Press, 2019. doi:10.1017/fms.2019.47, arXiv:1608.00243.

[24] Luke Pebody. Proof of a conjecture of Kleinberg–Sawin–Speyer. *Discrete Anal.*, 2018. doi:10.19086/da.3733, arXiv:1608.05740.

[25] Michael Fekete. Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten. *Math. Z.*, 17(1):228–249, 1923. doi:10.1007/BF01504345.

[26] Herbert Robbins. A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29, 1955. doi:10.2307/2308012.

[27] Imre Z. Ruzsa and Endre Szemerédi. Triple systems with no six points carrying three triangles. *Combinatorics (Keszthely, 1976), Coll. Math. Soc. J. Bolyai*, 18:939–945, 1978.

[28] Will Sawin. Bounds for matchings in nonabelian groups. *Electron. J. Combin.*, P4.23, 2018. https://doi.org/10.37236/7520, arXiv:1702.00905.

[29] John K. Stockton, J. M. Geremia, Andrew C. Doherty, and Hideo Mabuchi. Characterizing the entanglement of symmetric many-particle spin-1/2 systems. *Phys. Rev. A*, 67(2):022112, 2003. https://doi.org/10.1103/PhysRevA.67.022112

[30] Volker Strassen. Relative bilinear complexity and matrix multiplication. *J. Reine Angew. Math.*, 375/376:406–443, 1987. https://doi.org/10.1515/crll.1987.375-376.406

[31] Volker Strassen. The asymptotic spectrum of tensors. *J. Reine Angew. Math.*, 384:102–152, 1988. https://doi.org/10.1515/crll.1988.384.102

[32] Volker Strassen. Degeneration and complexity of bilinear maps: some asymptotic spectra. *J. Reine Angew. Math.*, 413:127–180, 1991. https://doi.org/10.1515/crll.1991.413.127

[33] Terence Tao. A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound, 2016. blog-post.

[34] Terence Tao and Will Sawin. Notes on the "slice rank" of tensors, 2016. https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors/.

[35] Péter Vrana and Matthias Christandl. Asymptotic entanglement transformation between W and GHZ states. *J. Math. Phys.*, 56(2):022204, 12, 2015. https://doi.org/10.1063/1.4908106, arXiv:arXiv:1310.3244.

[36] Péter Vrana and Matthias Christandl. Entanglement distillation from Greenberger–Horne–Zeilinger shares. *Comm. Math. Phys.*, 352(2):621–627, 2017. arXiv:1603.03964, doi:10.1007/s00220-017-2861-6.