Electronic Colloquium on Computational Complexity, Report No. 16 (2018)

On $\ell_4 : \ell_2$ ratio of functions with restricted Fourier support

Noami Kirshner and Alex Samorodnitsky

Abstract

Given a subset $A \subseteq \{0,1\}^n$, let $\mu(A)$ be the maximal ratio between ℓ_4 and ℓ_2 norms of a function whose Fourier support is a subset of A.[1] We make some simple observations about the connections between $\mu(A)$ and the additive properties of A on one hand, and between $\mu(A)$ and the uncertainty principle for A on the other hand. One application obtained by combining these observations with results in additive number theory is a stability result for the uncertainty principle on the discrete cube.

Our more technical contribution is determining $\mu(A)$ rather precisely, when A is a Hamming sphere $S(n,k)$ for all $0 \le k \le n$.

1 Introduction

Let A be a subset of the discrete cube $\{0,1\}^n$. Consider the subspace $V = V(A)$ of functions on $\{0,1\}^n$ whose Fourier support is a subset of A. That is, for any function $f \in V$, the expansion of f in terms of the Walsh-Fourier characters $f = \sum_\alpha \widehat{f}(\alpha) W_\alpha$ is supported on $\alpha \in A$. Let

$$\mu(A) \quad = \quad \max_{f \in V, f \neq 0} \left(\frac{\|f\|_4}{\|f\|_2}\right)^4 \quad = \quad \max_{f \in V, f \neq 0} \frac{\mathbb{E} f^4}{\mathbb{E}^2 f^2},$$

where the expectation on the RHS is w.r.t. the uniform measure on $\{0,1\}^n$.

The quantity $\mu(A)$ is well-investigated, especially when A is a Hamming ball or a Hamming sphere, since in this case it is closely related to the hypercontractive property of the noise operator on the discrete cube. In particular, it is know that for a Hamming ball of radius k, we have $\mu(A) \le 9^k$ [1], and for a Hamming sphere of radius k, for a constant (or slowly growing) k, we have $\mu(A) = \Theta\left(9^k/\sqrt{k}\right)$ [9].

We make several simple observations, connecting between $\mu(A)$ and the additive properties of A on one hand, and between $\mu(A)$ and the uncertainty principle for functions in $V(A)$ on the other hand. Connections of this kind have already been explored in [6, 10] (between $\mu(A)$, or closely related quantities, to the uncertainty principle), and by [5] (between $\mu(A)$ and the additive properties of A).

Additive structure of A: For $x \in A + A$, let $M_x = \{(a,b) \in A \times A : a + b = x\}$. Let $m(A) = 1 + \max_{x \neq 0} |M_x|$. Thus $m(A)$ is the maximal multiplicity of a non-zero element in

[1] Strictly speaking, we consider the fourth power of this ratio, since it is easier to work with.

ISSN 1433-8092

$A+A$ (plus one). Let $E_2(A,A)$ be the *additive energy* of A [13]. This is the number of 4-cycles in A:

$$E_2(A,A) \quad = \quad \left|\{(a,b,c,d) \in A^4 : a+b+c+d=0\}\right|$$

We observe that

Proposition 1.1: *For any subset $A \subseteq \{0,1\}^n$ holds*

1. $\mu(A) \ \leq \ |A|$
2. $\mu(A) \ \leq \ m(A)$
3. $\max_{B\subseteq A} \frac{E_2(B,B)}{|B|^2} \ \leq \ \mu(A) \ \leq \ O\left(\log^3(|A|)\right) \cdot \max_{B\subseteq A} \frac{E_2(B,B)}{|B|^2}$

Let us describe one application of this proposition. The following result has been proved in [4]. Let A be a Hamming ball of radius k, and let B and C be subsets of A. Then $|B+C| \geq \frac{|B||C|}{9^k}$. We rederive this result as follows. Recall that $\mu(A) \leq 9^k$. Hence we have

$$|B+C| \ \geq \ \frac{|B|^2|C|^2}{\sqrt{E_2(B,B)}\sqrt{E_2(C,C)}} \ = \ \frac{|B||C|}{\sqrt{\frac{E_2(B,B)}{|B|^2}}\sqrt{\frac{E_2(C,C)}{|C|^2}}} \ \geq \ \frac{|B||C|}{\mu(A)} \ \geq \ \frac{|B||C|}{9^k}. \qquad (1)$$

For the first inequality (which follows by a simple application of the Cauchy-Schwarz inequality) see e.g., [13]. The second inequality follows from the third claim of the proposition.

Remark 1.2: Another way to obtain $\mu(A)$ is as the maximal eigenvalue of a certain symmetric $|A|\times|A|$ matrix. Such matrices and their relevance to the additive structure of A were considered in [12]. Specifically, denoting by $\lambda(M)$ the maximal eigenvalue of a matrix M, it is not hard to see that

$$\mu(A) \quad = \quad \max_{y:A\rightarrow\mathbb{R},\|y\|_2=1} \lambda\left(T_A^{y\circ y}\right),$$

where (in the notation of [12]) $T = T_A^{y\circ y}$ is the $A\times A$ matrix with rows and columns indexed by the elements of A, such that $T\left(a_1,a_2\right) = \sum_{(b_1,b_2)\in M_{a_1+a_2}} y\left(a_1\right)\cdot y\left(a_2\right)$. ▮

Uncertainty principle: The uncertainty principle for the discrete cube (see e.g., [2]) states that for a non-zero function f on $\{0,1\}^n$ holds:

$$|supp(f)| \quad \geq \quad \frac{2^n}{|supp\left(\widehat{f}\right)|} \qquad (2)$$

The following claim is an immediate consequence of the Cauchy-Schwarz inequality.

Lemma 1.3: *For a non-zero function f on $\{0,1\}^n$, let let $A = supp\left(\widehat{f}\right)$. Then*

$$|supp(f)| \quad \geq \quad \frac{2^n}{\mu(A)}$$

This strengthens (2), by the first claim of Proposition 1.1.

A quantitative version of (2) was proved in [10]. For any $0 < \delta < 1$, there exists an $\epsilon > 0$ depending on δ, such that for any two subsets A, B of $\{0,1\}^n$ with $|A| \cdot |B| \leq 2^{(1-\delta)n}$ holds: if f is a non-zero function with $\widehat{f}$ supported on A, then $\frac{1}{2^n}\sum_{b \in B} f^2(b) \leq (1-\epsilon) \cdot \|f\|_2^2$.

The following claim is a strengthening of this result.

Lemma 1.4: *Let $0 < \delta < 1$. Then for any two subsets A, B of $\{0,1\}^n$ with $\mu(A) \cdot |B| \leq 2^{(1-\delta)n}$ holds: if f is a non-zero function with $\widehat{f}$ supported on A, then*

$$\frac{1}{2^n}\sum_{b \in B} f^2(b) \quad \leq \quad 2^{-\frac{\delta n}{2}} \cdot \|f\|_2^2$$

Combining Lemma 1.3 with Proposition 1.1 gives the following corollary.

Corollary 1.5: *For a non-zero function f on $\{0,1\}^n$, let $A = supp\left(\widehat{f}\right)$. Then*

$$|supp(f)| \quad \geq \quad \frac{2^n}{m(A)} \quad and \quad |supp(f)| \quad \geq \quad \Omega\left(\frac{1}{\log^3(|A|)}\right) \cdot \frac{2^n}{\max_{B \subseteq A} \frac{E_2(B,B)}{|B|^2}}$$

Up to negligible factors, both inequalities strengthen (2), since $m(A) \leq |A|+1$, and $E_2(B) \leq |B|^3$.

Combining the second inequality in Corollary 1.5 with results from additive number theory describing the structure of sets with large energy and small doubling ([3], [11]) leads to a stability version of (2). It is known that (2) holds with equality if and only if $\widehat{f}$ is a characteristic function of an affine subspace of $\{0,1\}^n$. We show that even if equality is replaced with 'near equality', the support of $\widehat{f}$ will be similar to a linear subspace, in the appropriate sense. *Notation*: let $\langle B \rangle$ denote the linear span of a subset $B \subseteq \{0,1\}^n$.

Proposition 1.6: *Let f be a non-zero function on $\{0,1\}^n$ with $|supp(f)| \cdot |supp\left(\widehat{f}\right)| \leq C \cdot 2^n$. Let $A = supp\left(\widehat{f}\right)$. Let $C' = C \cdot \log(|A|)$. There exists a subset $A' \subseteq A$ such that:*

- $$|A'| \quad \geq \quad C'^{-O\left(\log^3 C'\right)} \cdot |A|$$

  and

- $$|\langle A' \rangle| \quad \leq \quad |A|,$$

with asymptotic notation hiding absolute constants.

The third claim of Proposition 1.1 leads to the following natural question: which sets $A \subseteq \{0,1\}^n$ have the 'hereditary' property $\frac{E_2(A,A)}{|A|^2} \geq \frac{E_2(B,B)}{|B|^2}$, for all subsets $B \subseteq A$. It is easy to see that this holds if A is a subspace. We show that, up to lower order terms, this is also true for a Hamming sphere. We distinguish between two cases: the radius of the sphere is small compared to n, or the radius of the sphere is allowed to grow arbitrarily in n. For the first case, we have the following proposition:

Proposition 1.7: *Let $A = S(n,k)$ be a Hamming sphere of radius k, for $k = o(\sqrt{n})$. Then*

$$\mu(A) \quad \leq \quad \Big(1 + o_n(1)\Big) \cdot \frac{E_2(A,A)}{|A|^2}$$

For general k we have the following result, which is the most technical part of this paper.

Theorem 1.8: *Let $A = S(n,k)$ be a Hamming sphere of radius k, for $0 \leq k \leq n/2$. Let $r(x) = \frac{3-\sqrt{1+8(1-2x)^2}}{8}$, and let ψ be a function on $\left[0, \frac{1}{2}\right]$ defined by*

$$\psi(x) \quad = \quad H\big(2r(x)\big) + 4r(x) + 2\big(1 - 2r(x)\big) \cdot H\left(\frac{x - r(x)}{1 - 2r(x)}\right) - 2H(x).$$

Then

1.
$$\mu(A) \quad \leq \quad 2^{n\psi\left(\frac{k}{n}\right)}$$

2.
$$2^{n\psi\left(\frac{k}{n}\right)} \quad \leq \quad O\left(k^{3/2}\right) \cdot \frac{E_2(A,A)}{|A|^2}$$

In the light of these results it is natural to make the following conjecture.

Conjecture 1.9: Let $A = S(n,k)$ be a Hamming sphere of radius k, for $1 \leq k \leq n/2$. Then

$$\mu(A) \quad = \quad \frac{E_2(A,A)}{|A|^2}$$

▮

Remark 1.10: Proposition 1.7 and Theorem 1.8 show that among all homogeneous polynomials f of degree k the maximum of the ratio $\frac{\|f\|_4}{\|f\|_2}$ is (essentially) attained for the sum of all weight k monomials (the k^{th} *Krawchouk polynomial*). We refer to [8] (and references therein) and to Sections 4.2 and 4.3 in [10] for other results in this direction. ▮

Theorem 1.8 can be applied to extend the result of [4] (whose alternative derivation was given in (1)) to larger values of k. We start with observing that a simple modification of the proof of the theorem shows its bound to hold for Hamming balls as well.

Corollary 1.11: *Let $A = B(n, k)$ be a Hamming ball of radius k, for $0 \leq k \leq n/2$. Then:*

1. $\mu(A) \ \leq \ 2^{n\psi\left(\frac{k}{n}\right)}$.
2. $2^{n\psi\left(\frac{k}{n}\right)} \ \leq \ \min\left\{9^k, 2^n\right\}$,
   with equality only at $k = 0$, where the LHS is 1 and at $k = n/2$, where the LHS is 2^n.

The second claim of the corollary shows it to extend the bound $\mu(A) \leq 9^k$ ([1]). Using its first claim in (1) leads to the following result (which we state slightly more generally).

Corollary 1.12: *Let B be a subset of a Hamming ball of radius k_1, and let C be a subset of a Hamming ball of radius k_2. Then*

$$|B + C| \quad \geq \quad \frac{|B||C|}{2^{\frac{n}{2}\cdot\left(\psi\left(\frac{k_1}{n}\right)+\psi\left(\frac{k_2}{n}\right)\right)}}.$$

This paper is organized as follows. We prove Proposition 1.7 in Section 3, and Theorem 1.8 with Corollary 1.11 in Section 4. All the remaining claims are proved in Section 2.

2 Simple proofs

In this section we prove all the observations stated in the introduction, except for Proposition 1.7 and Theorem 1.8.

Our starting point is the following characterization of $\mu(A)$. Let $\mathbb{S} = \mathbb{S}^{|A|-1}$ denote the Euclidean sphere of dimension $|A| - 1$. We will assume the vectors in $\mathbb{S}$ to be indexed by elements of A (in other words, a vector $y \in \mathbb{S}$ is a function from A to $\mathbb{R}$, with unit ℓ_2 norm). Then $\mu(A)$ is the maximal value of the following real valued function on $\mathbb{S}$ (recall that $M_x = \{(a, b) \in A \times A : a + b = x\}$):

$$\mu(A) \quad = \quad \max_{y \in \mathbb{S}} F(y), \quad \text{where} \quad F(y) \quad = \quad \sum_{x \in A+A} \left(\sum_{(a,b) \in M_x} y_a y_b \right)^2. \tag{3}$$

To see this, note that each $y \in \mathbb{S}$ represents a Fourier expansion of a function $f = \sum_{a \in A} y_a W_a$ of ℓ_2 norm 1, and $F(y) = \mathbb{E}\, f^4 = \|f\|_4^4$.

Proof of Proposition 1.1

We start with the first claim of the proposition. Applying the Cauchy-Schwarz inequality, for any $y \in S^{|A|-1}$ holds

$$F(y) \quad = \quad \sum_{x \in A+A} \left(\sum_{(a,b) \in M_x} y_a y_b \right)^2 \quad \leq \quad \sum_{x \in A+A} |M_x| \cdot \sum_{(a,b) \in M_x} y_a^2 y_b^2 \quad \leq$$

$$\left(\max_{x \in A+A} |M_x| \right) \cdot \sum_{x \in A+A} \sum_{(a,b) \in M_x} y_a^2 y_b^2 \quad = \quad \max_{x \in A+A} |M_x| \quad = \quad |M_0| \quad = \quad |A|,$$

completing the proof.

The second claim is proved similarly. For any $y \in \mathbb{S}$ holds

$$F(y) \quad = \quad \sum_{x \in A+A} \left(\sum_{(a,b) \in M_x} y_a y_b \right)^2 \quad \leq \quad 1 + \sum_{x \in A+A \setminus \{0\}} |M_x| \cdot \sum_{(a,b) \in M_x} y_a^2 y_b^2 \quad \leq$$

$$1 + \left(\max_{x \in A+A \setminus \{0\}} |M_x| \right) \cdot \sum_{x \in A+A} \sum_{(a,b) \in M_x} y_a^2 y_b^2 \quad = \quad 1 + \max_{x \in A+A \setminus \{0\}} |M_x|,$$

We continue to the third claim, starting with the lower bound. Note that for any subset $B \subseteq A$ holds $F\left(\frac{1_B}{\sqrt{|B|}}\right) = \frac{E_2(B,B)}{|B|^2}$. Hence, by (3),

$$\mu(A) \quad \geq \quad \max_{B \subseteq A} F\left(\frac{1_B}{\sqrt{|B|}}\right) \quad = \quad \max_{B \subseteq A} \frac{E_2(B,B)}{|B|^2}.$$

We pass to the upper bound on $\mu(A)$. Let $y^* \in \mathbb{S}$ such that $F(y^*) = \mu(A)$. We may assume, w.l.o.g, that the vector y^* is nonnegative. Let $f = \sum_{a \in A} y_a^* W_a$. Then $\mathbb{E} f^4 = \mu(A)$.

We introduce some notation: For $i \geq 1$, let $A_i = \left\{ a \in A : 2^{-i} < y_a^* \leq 2^{-(i-1)} \right\}$. Let $f_i = \sum_{a \in A_i} y_a^* W_a$. Let $h_i = \sum_{a \in A_i} W_a$. Finally, let $N = \lceil \frac{1}{2} \log_2(|A|) \rceil + 2$.

We have $f = \sum_{i=1}^{\infty} f_i$, where the summation on the RHS is, of course, finite. Let $k = \sum_{i=N+1}^{\infty} f_i$. Then $k = \sum_{a \in A} z_a W_a$, with $|z_a| \leq 2^{-(N-1)} \leq \frac{1}{2\sqrt{|A|}}$ for all $a \in A$. Hence $\sum_{a \in A} z_a^2 \leq \frac{1}{4}$ and therefore, by the 4-homogeneity of F, we get $\mathbb{E} k^4 = F(z) \leq \frac{\mu(A)}{16}$.

Let $t = f - k = \sum_{i=1}^{N} f_i$. By the convexity of the function x^4 and by Jensen's inequality, we have $\mathbb{E} f^4 = \mathbb{E}(k+t)^4 \leq 8 \cdot \left(\mathbb{E} k^4 + \mathbb{E} t^4 \right)$. It follows that $\mathbb{E} t^4 \geq \frac{1}{8} \cdot \mathbb{E} f^4 - \frac{\mu(A)}{16} \geq \frac{1}{16} \cdot \mathbb{E} f^4$. So, to prove the claim it suffices to upperbound $\mathbb{E} t^4$, which we proceed to do.

By Jensen's inequality, $\mathbb{E} t^4 = \mathbb{E} \left(\sum_{i=1}^{N} f_i \right)^4 \leq N^3 \cdot \sum_{i=1}^{N} \mathbb{E} f_i^4$. For $1 \leq i \leq N$, let $y^{(i)} = 1_{A_i} \cdot y^*$. Then $\mathbb{E} f_i^4 = F\left(y^{(i)} \right) \leq 2^{-4(i-1)} \cdot F\left(1_{A_i}\right) = 2^{-4(i-1)} \cdot \mathbb{E} h_i^4$. Hence,

$$\mathbb{E} t^4 \quad \leq \quad N^3 \cdot \sum_{i=1}^{N} 2^{-4(i-1)} \mathbb{E} h_i^4 \quad = \quad 16 N^3 \cdot \sum_{i=1}^{N} 2^{-4i} \mathbb{E} h_i^4$$

Next, observe that the functions $\{f_i\}_{i=1}^N$ are orthogonal, and hence

$$\sum_{i=1}^N 2^{-2i}|A_i| \quad = \quad \sum_{i=1}^N 2^{-2i}\,\mathbb{E}\,h_i^2 \quad \le \quad \sum_{i=1}^N \mathbb{E}\,f_i^2 \quad = \quad \mathbb{E}\,t^2 \quad \le \quad 1.$$

It follows that

$$\sum_{i=1}^N 2^{-4i}\,\mathbb{E}\,h_i^4 \quad = \quad \sum_{i=1}^N 2^{-4i} E_2\left(A_i, A_i\right) \quad = \quad \sum_{i=1}^N \left(2^{-4i}|A_i|^2\right) \cdot \frac{E_2\left(A_i, A_i\right)}{|A_i|^2} \quad \le$$

$$\max_{1 \le i \le N} \frac{E_2\left(A_i, A_i\right)}{|A_i|^2} \cdot \sum_{i=1}^N 2^{-4i}|A_i|^2 \quad \le \quad \max_{1 \le i \le N} \frac{E_2\left(A_i, A_i\right)}{|A_i|^2} \cdot \sum_{i=1}^N 2^{-2i}|A_i| \quad \le \quad \max_{1 \le i \le N} \frac{E_2\left(A_i, A_i\right)}{|A_i|^2}$$

And hence, recalling that $N = O(\log|A|)$,

$$\mathbb{E}\,t^4 \quad \le \quad 16N^3 \cdot \sum_{i=1}^N 2^{-4i}\,\mathbb{E}\,h_i^4 \quad \le \quad O\left(\log^3(|A|)\right) \cdot \max_{B \subseteq A} \frac{E_2(B,B)}{|B|^2},$$

concluding the proof of the upper bound and of the proposition.

■

Proof of Lemma 1.3

Let f be a non-zero function on $\{0,1\}^n$, with $A = \mathit{supp}\left(\widehat{f}\right)$. Let $B = \mathit{supp}(f)$. Then, by the Cauchy-Schwarz inequality,

$$\mathbb{E}^2 f^2 \quad = \quad \mathbb{E}^2 f^2 \cdot 1_B \quad \le \quad \mathbb{E}\,f^4 \cdot \mathbb{E}\,1_B.$$

Hence, by the definition of $\mu(A)$,

$$|B| \quad = \quad 2^n \cdot \mathbb{E}\,1_B \quad \ge \quad 2^n \cdot \frac{\mathbb{E}^2\,f^2}{\mathbb{E}\,f^4} \quad \ge \quad \frac{2^n}{\mu(A)}.$$

■

Proof of Lemma 1.4

Let f be a non-zero function on $\{0,1\}^n$, with $A = \mathit{supp}\left(\widehat{f}\right)$. Let $B \subseteq \{0,1\}^n$ satisfy $|A| \cdot |B| = 2^{(1-\delta)n}$. Let $\frac{1}{2^n}\sum_{b \in B} f^2(b) = c \cdot \|f\|_2^2 = c \cdot \mathbb{E}\,f^2$. Then, by the Cauchy-Schwarz inequality,

$$c^2 \cdot \mathbb{E}^2 f^2 \quad = \quad \left(\frac{1}{2^n}\sum_{b \in B} f^2(b)\right)^2 \quad = \quad \mathbb{E}^2 f^2 \cdot 1_B \quad \le \quad \mathbb{E}\,f^4 \cdot \mathbb{E}\,1_B.$$

Hence, by the definition of $\mu(A)$,

$$c^2 \quad \le \quad \frac{\mathbb{E}\,f^4}{\mathbb{E}^2\,f^2} \cdot \frac{|B|}{2^n} \quad \le \quad \frac{\mu(A) \cdot |B|}{2^n} \quad = \quad 2^{-\delta n}.$$

■

Proof of Proposition 1.6

Let f be a non-zero function on $\{0,1\}^n$ with $|supp(f)| \cdot |supp\left(\widehat{f}\right)| \le C \cdot 2^n$. Let $A = supp\left(\widehat{f}\right)$, and let $B \subseteq A$ be the subset of A for which the ratio $\frac{E_2(B,B)}{|B|^2}$ is maximal. By the third claim of Proposition 1.1, we have

$$\frac{C \cdot 2^n}{|A|} \quad \ge \quad |supp(f)| \quad \ge \quad \Omega\left(\frac{1}{\log^3(|A|)}\right) \cdot \frac{2^n}{\frac{E_2(B,B)}{|B|^2}}.$$

Rearranging, this gives $\frac{E_2(B,B)}{|B|^2} \ge \frac{1}{C} \cdot \Omega\left(\frac{|A|}{\log^3(|A|)}\right)$. Since $E_2(B,B) \le |B|^3$, this implies $|B| \ge \frac{1}{C} \cdot \Omega\left(\frac{|A|}{\log^3(|A|)}\right)$. Hence

$$E_2(A,A) \quad \ge \quad E_2(B,B) \quad \ge \quad \frac{1}{C} \cdot \Omega\left(\frac{|A||B|^2}{\log^3(|A|)}\right) \quad \ge \quad \frac{1}{C^3} \cdot \Omega\left(\frac{|A|^3}{\log^9(|A|)}\right) \tag{4}$$

We quote two results from additive number theory (without stating the best known values of various constants):

- [3]: Let $A \subseteq \{0,1\}^n$ with $E_2(A,A) \ge c \cdot |A|^3$. Then there is a subset $A_1 \subseteq A$ with $|A_1| \ge \Omega\left(c^{\Theta(1)}\right) \cdot |A|$ and $|A_1 + A_1| \le O\left(c^{-\Theta(1)}\right) \cdot |A_1|$.
- [11]: Let $A_1 \subseteq \{0,1\}^n$ with $|A_1 + A_1| \le c_1 \cdot |A_1|$. Then there is a subset $A' \subseteq A_1$ with $|A'| \ge c_1^{-O\left(\log^3 c_1\right)} \cdot |A_1|$ and $|\langle A' \rangle| \le |A_1|$.

The claim of the proposition follows by combining these two results with (4).

▮

3 Proof of Proposition 1.7

Let $A = S(n,k)$. Then $A + A = S(n,0) \cup S(n,2) \cup ... \cup S(n,2k)$. We partition the function F in (3) as $F = \sum_{t=0}^{k} F_t$, where

$$F_t \quad = \quad \sum_{x \in S(n,2t)} \left(\sum_{(a,b) \in M_x} y_a y_b\right)^2.$$

Clearly $F_0 \equiv 1$. We claim that for any $1 \le t \le k$ and for any $y \in \mathbb{S}$ holds

$$F_t(y) \quad \le \quad \binom{2t}{t} \cdot \binom{k}{t}^2 \tag{5}$$

To see this, let $1 \le t \le k$ and let $x \in S(n,2t)$. Consider a representation $x = u + v$ with $u, v \in S(n,k)$. Note that each such representation corresponds to a partition of x into two parts x_1 and x_2 of weight t each, and a choice of an additional vector w of weight $k-t$ disjoint from x, such that, slightly informally, $u = x_1w$ and $v = x_2w$ (that is u is a concatenation of x_1 and w and similarly for v).

Let us denote the set of the $\binom{2t}{t}$ partitions of x into two halves x_1 and x_2 by $P(x)$. Each partition $\alpha = (x_1, x_2) \in P(x)$ defines a subsum $s_\alpha = \sum_w y_{x_1w}y_{x_2w}$ of $s_x := \sum_{(a,b)\in M_x} y_a y_b$. Clearly $s_x = \sum_{\alpha\in P(x)} s_\alpha$. By the Cauchy-Schwarz inequality, $s_x^2 \leq |P(x)| \cdot \sum_{\alpha\in P(x)} s_\alpha^2 = \binom{2t}{t} \cdot \sum_{\alpha\in P(x)} s_\alpha^2$. Summing up, we have

$$F_t(y) \quad = \quad \sum_{x\in S(n,2t)} s_x^2 \quad \leq \quad \binom{2t}{t} \cdot \sum_{x\in S(n,2t)} \sum_{\alpha\in P(x)} s_\alpha^2.$$

Hence, (5) will be implied by the following lemma.

Lemma 3.1: *For any $y \in \mathbb{S}$ holds*

$$\sum_{x\in S(n,2t)} \sum_{\alpha\in P(x)} s_\alpha^2(y) \quad \leq \quad \binom{k}{t}^2.$$

Proof: (Of the lemma)

We apply the Cauchy-Schwarz inequality to bound each of the summands. For $x \in S(n, 2t)$ and $\alpha = (x_1, x_2) \in P(x)$ we have

$$s_\alpha^2(y) \quad = \quad \left(\sum_w y_{x_1w}y_{x_2w}\right)^2 \quad \leq \quad \left(\sum_w y_{x_1w}^2\right) \cdot \left(\sum_w y_{x_2w}^2\right) \quad = \quad \sum_{w_1,w_2} y_{x_1w_1}^2 \cdot y_{x_2w_2}^2$$

That is,

$$\sum_{x\in S(n,2t)} \sum_{\alpha\in P(x)} S_\alpha^2(y) \quad \leq \quad \sum_{x\in S(n,2t)} \quad \sum_{(x_1,x_2)\in P(x)} \quad \sum_{w_1,w_2} y_{x_1w_1}^2 \cdot y_{x_2w_2}^2,$$

where the inner sum goes over all $(k-t)$-bit strings w_1, w_2 disjoint with x.

We will argue that for any two elements a and b of $S(n, k)$, the product $y_a^2 y_b^2$ appears on the RHS at most $\binom{k}{t}^2$ times, and hence the RHS is bounded from above by $\binom{k}{t}^2 \cdot \sum_{a,b\in S(n,k)} y_a^2 y_b^2 = \binom{k}{t}^2 \cdot \left(\sum_{a\in S(n,k)} y_a^2\right)^2 = \binom{k}{t}^2$.

In fact, given a and b, there are at most $\binom{k}{t}$ ways to choose a t-subset $x_1 \subseteq a$ of a, and at most $\binom{k}{t}$ ways to choose a t-subset $x_2 \subseteq b$ of b. After choosing $\{x_i\}$, their complements $\{w_j\}$ are determined uniquely by $\{x_i\}$, a and b. ▮

This completes the proof of (5). Summing up over t, we get

$$\mu(A) \quad \leq \quad \sum_{t=0}^{k} \max_{y\in\mathbb{S}} F_t(y) \quad \leq \quad \sum_{t=0}^{k} \binom{2t}{t} \cdot \binom{k}{t}^2.$$

We proceed to compare this bound to $\frac{E_2(A,A)}{|A|^2}$. We have

$$\frac{E_2(A,A)}{|A|^2} = \frac{1}{|A|^2} \cdot \sum_{x \in A+A} |M_x|^2 = \frac{1}{\binom{n}{k}^2} \cdot \sum_{t=0}^{k} \sum_{x \in S(n,2t)} |M_x|^2 = \frac{1}{\binom{n}{k}^2} \cdot \sum_{t=0}^{k} \binom{n}{2t} \left(\binom{2t}{t} \cdot \binom{n-2t}{k-t} \right)^2$$

It is easy to see that for $r = o(n)$ holds $(1 - o_n(1)) \cdot e^{-r^2/n} \cdot n^r \leq \frac{n!}{(n-r)!} \leq n^r$. This implies (following a simple calculation) that for $k = o(n)$ we can lowerbound $\frac{E_2(A,A)}{|A|^2}$ by :

$$(1 - o_n(1))\, e^{\frac{-2k^2}{n}} \cdot \frac{(k!)^2}{n^{2k}} \cdot \sum_{t=0}^{k} \frac{n^{2t}}{(2t)!} \cdot \binom{2t}{t}^2 \cdot \frac{n^{2k-2t}}{((k-t)!)^2} \quad = \quad (1 - o_n(1))\, e^{\frac{-2k^2}{n}} \cdot \sum_{t=0}^{k} \binom{2t}{t} \cdot \binom{k}{t}^2 \tag{6}$$

Taking $k = o(\sqrt{n})$, this implies $\mu(A) \leq (1 + o_n(1)) \cdot \frac{E_2(A,A)}{|A|^2}$, completing the proof of the proposition.

4 Proof of Theorem 1.8

Let $A = S(n,k)$. It will be convenient to use a notation which makes explicit the dependence of $\mu(A)$ and $\frac{E_2(A,A)}{|A|^2}$ on the parameters n and k. We let $R(n,k) = \mu(A)$ and $r(n,k) = \frac{E_2(A,A)}{|A|^2}$. Recall (see Section 3) that

$$r(n,k) \quad = \quad \frac{1}{\binom{n}{k}^2} \cdot \sum_{t=0}^{k} \binom{n}{2t} \left(\binom{2t}{t} \cdot \binom{n-2t}{k-t} \right)^2$$

We also let $s_t(n,k) = \frac{1}{\binom{n}{k}^2} \cdot \binom{n}{2t} \left(\binom{2t}{t} \cdot \binom{n-2t}{k-t} \right)^2$. Thus $r(n,k) = \sum_{t=0}^{k} s_t(n,k)$.

We start with the first (and main) claim of Theorem 1.8 and rewrite it in this notation.

$$R(n,k) \quad \leq \quad 2^{n\psi\left(\frac{k}{n}\right)}. \tag{7}$$

The main step in the proof of (7) is the following somewhat weaker claim.

Proposition 4.1: *There exists an absolute constant $C > 0$ so that for all $1 \leq k \leq n/2$ holds*

$$R(n,k) \quad \leq \quad C \cdot 2^{5n/\log(n)} \cdot r(n,k).$$

We will also need the following technical lemma. From now on, all logarithms are to base 2. Let $t_1(n,k) = \frac{3n - \sqrt{n^2 + 8(n-k)^2}}{8}$.

Lemma 4.2: *Let n be sufficiently large, and let $\frac{n}{\log n} \leq k \leq \frac{n}{2} - \frac{n}{\log n}$. Then*

$$\max_{0 \leq t \leq k} s_t(n,k) \quad = \quad \max_{t \in t_1(n,k) \pm \sqrt{n \log n}} s_t(n,k).$$

We will prove Proposition 4.1 and Lemma 4.2 below. First we show how they imply (7). It will be convenient to work with the following modification of the function ψ. It Let ϕ be a function on $\left[0, \frac{k}{n}\right]$ defined by $\phi(y) = H(2y) + 4y + 2(1-2y) \cdot H\left(\frac{k/n-y}{1-2y}\right) - 2H\left(\frac{k}{n}\right)$. Observe that $\phi\left(\frac{t_1(n,k)}{n}\right) = \psi\left(\frac{k}{n}\right)$.

Let f be a function on $\{0,1\}^n$ with $supp\left(\widehat{f}\right) \subseteq S(n,k)$, such that $R(n,k) = \frac{\mathbb{E} f^4}{\mathbb{E}^2 f^2}$. For an integer $m \geq 1$, consider a function F_m on nm boolean variables defined for $x_1, ..., x_m \in \{0,1\}^n$ by $F_m(x_1,...,x_m) = \prod_{i=1}^m f(x_i)$. Observe that for any $\alpha_1, ..., \alpha_m \in \{0,1\}^n$ holds $\widehat{F_m}(\alpha_1,...,\alpha_m) = \prod_{i=1}^m \widehat{f}(\alpha_i)$, and hence $supp\left(\widehat{F_m}\right) \subseteq S(nm, km)$. We also have $\mathbb{E} F_m^p = (\mathbb{E} f^p)^m$, for any p, and hence $\frac{\mathbb{E} F_m^4}{\mathbb{E}^2 F_m^2} = \left(\frac{\mathbb{E} f^4}{\mathbb{E}^2 f^2}\right)^m$. Denoting $N = nm$ and $K = km$, we have that

$$R(n,k) \quad = \quad \frac{\mathbb{E} f^4}{\mathbb{E}^2 f^2} \quad = \quad \left(\frac{\mathbb{E} F_m^4}{\mathbb{E}^2 F_m^2}\right)^{\frac{1}{m}} \quad \leq \quad R(N,K)^{\frac{1}{m}} \quad \leq \quad \left(C \cdot 2^{\frac{5N}{\log N}} \cdot r(N,K)\right)^{\frac{1}{m}}.$$

Taking m to infinity, we have $R(n,k) \leq \liminf_{m\to\infty} \left(r(N,K)\right)^{\frac{1}{m}}$. For a sufficiently large m we have $\frac{N}{\log N} \ll K \ll \frac{N}{2} - \frac{N}{\log N}$, and hence, by Lemma 4.2,

$$\liminf_{m\to\infty} \left(r(N,K)\right)^{\frac{1}{m}} \quad = \quad \liminf_{m\to\infty} \left(\max_t s_t(N,K)\right)^{\frac{1}{m}} \quad = \quad \liminf_{m\to\infty} \left(\max_{t \in t_1(N,K) \pm \sqrt{N \log N}} s_t(N,K)\right)^{\frac{1}{m}}$$

where $t_1(N,K) = \frac{3N - \sqrt{N^2 + 8(N-2K)^2}}{8}$. Recalling that $s_t(N,K) = \frac{1}{\binom{N}{K}^2} \cdot \binom{N}{2t} \left(\binom{2t}{t}\binom{N-2t}{K-t}\right)^2$, and using the bound $\binom{b}{a} \leq 2^{bH(a/b)}$ ([7]), we get, for $t \in t_1(N,K) \pm \sqrt{N \log N}$, that

$$\frac{1}{n} \cdot \log_2 s_t^{\frac{1}{m}}(N,K) \quad \leq \quad H\left(\frac{2t}{N}\right) + 4\frac{t}{N} + 2\left(1 - 2\frac{t}{N}\right) H\left(\frac{k/n - t/N}{1 - 2t/N}\right) - 2H\left(\frac{k}{n}\right) \quad = \quad \phi\left(\frac{t}{N}\right),$$

where t/N is in $t_1(N,K)/N \pm \sqrt{\frac{\log N}{N}} = t_1(n,k)/n \pm \sqrt{\frac{\log N}{N}}$. Fixing n and k and taking m to infinity, we get that

$$\liminf_{m\to\infty} \frac{1}{n} \cdot \log_2 \left(\left(\max_{t \in t_1 \pm \sqrt{N \log N}} s_t(N,K)\right)^{\frac{1}{m}}\right) \quad \leq \quad \phi\left(\frac{t_1(n,k)}{n}\right) \quad = \quad \psi\left(\frac{k}{n}\right),$$

completing the proof of (7).

The remainder of this section is organized as follows. We prove Proposition 4.1 in the next subsection. Lemma 4.2 is proved as one of the steps in that proof. We prove the second inequality of Theorem 1.8, namely that

$$2^{n\psi\left(\frac{k}{n}\right)} \quad \leq \quad O\left(k^{3/2}\right) \cdot r(n,k) \tag{8}$$

in Subsection 4.2. Corollary 1.11 is proved in Subsection 4.3.

4.1 Proof of Proposition 4.1

We start with observing that by choosing the constant C in the claim of the proposition to be sufficiently large, we may assume that the claim holds for all $n \leq n_0$ for any fixed n_0 of our choice. Indeed, let n_0 be chosen, and set $C = 2^{n_0}$. Then, by the first claim of Proposition 1.1, for any $n \leq n_0$ and $1 \leq k \leq n/2$ holds

$$R(n,k) \quad \leq \quad \binom{n}{k} \quad < \quad 2^n \quad \leq \quad C \quad \leq \quad C \cdot 2^{5n/\log(n)} \cdot r(n,k)$$

From now on we fix n_0 to be sufficiently large for all asymptotically valid claims below to hold for $n \geq n_0$, and set $C = 2^{n_0}$.

Next, we observe that the claim of the proposition holds when k is very small compared to n or when k is very close to $n/2$. This is done in the next two lemmas.

Lemma 4.3: *There exists a sufficiently large constant n_0 such that Proposition 4.1 holds for all $n \geq n_0$ and $k \leq \frac{n}{\log n}$.*

Proof: By (6) we have that

$$R(n,k) \quad \leq \quad O\left(e^{\frac{2k^2}{n}}\right) \cdot r(n,k) \quad \leq \quad O\left(e^{\frac{2n}{\log^2 n}}\right) \cdot r(n,k) \quad \leq \quad 2^{5\frac{n}{\log n}} \cdot r(n,k),$$

for all sufficiently large n.

$\blacksquare$

Lemma 4.4: *There exists a sufficiently large constant n_0 such that Proposition 4.1 holds for all $n \geq n_0$ and $k \geq \frac{n}{2} - \frac{n}{\log n}$.*

Proof: Assume, w.l.o.g., that k is even. Then, using the inequality $\binom{k}{k/2} \geq \Omega\left(\frac{2^k}{\sqrt{k}}\right)$, we get

$$r(n,k) \quad \geq \quad s_{k/2}(n,k) \quad = \quad \frac{\binom{n}{k} \cdot \left(\binom{k}{k/2}\binom{n-k}{k/2}\right)^2}{\binom{n}{k}^2} \quad > \quad \frac{\binom{k}{k/2}^4}{2^n} \quad \geq \quad \Omega\left(\frac{2^{4k-n}}{n^2}\right) \quad \geq$$

$$\Omega\left(2^{n-4\frac{n}{\log n}-2\log_2 n}\right) \quad \geq \quad 2^{n-5\frac{n}{\log n}},$$

where the last inequality holds for a sufficiently large n. Therefore, $R(n,k) \ < \ 2^n \ \leq \ 2^{5\frac{n}{\log n}} \cdot r(n,k)$.
$\blacksquare$

Hence from now on we may assume that n is sufficiently large and that $\frac{n}{\log n} \leq k \leq \frac{n}{2} - \frac{n}{\log n}$. The proof of Proposition 4.1 will rely on the following two claims.

Proposition 4.5: *Let $F(x,y) = \frac{8xy}{4\sqrt{xy}-\left(\sqrt{x}-\sqrt{y}\right)^2}$. Then*

1. *The function F is increasing in both x and y in the domain $0 < x/9 < y < 9x$ and is 1-homogeneous.*

2. *For any $1 \leq k \leq n/2$ the following inductive relation holds: There exist positive numbers R_0 and R_1 such that $R_0 \leq R(n-1,k)$ and $R_1 \leq R(n-1,k-1)$ and such that*

$$R(n,k) \quad \leq \quad \begin{cases} R_0 & \text{if} \quad R_0 \geq 9R_1 \\ R_1 & \text{if} \quad R_1 \geq 9R_0 \\ F\left(R_0, R_1\right) & \text{otherwise} \end{cases}$$

And

Proposition 4.6: *There exists a sufficiently large constant n_0 such that for all $n \geq n_0$ and for all $\frac{n}{\log n} \leq k \leq \frac{n}{2} - \frac{n}{\log n}$ holds*

1.

$$\frac{r(n-1,k-1)}{9} \quad < \quad r(n-1,k) \quad < \quad 9 \cdot r(n-1,k-1)$$

2.

$$r(n,k) \quad \in \quad \left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot F\Big(r(n-1,k-1), r(n-1,k)\Big)$$

We first show how to deduce Proposition 4.1 from these two claims and then prove the claims.

Assume Proposition 4.5 and Proposition 4.6 to hold. Let n_0 and $C = 2^{n_0}$ be as defined above. We will argue by induction on n that for all $1 \leq k \leq n/2$ holds $R(n,k) \leq C \cdot 2^{5\frac{n}{\log n}} \cdot r(n,k)$. Clearly, by the choice of C, this holds for $n \leq n_0$, which takes care of the base step. We pass to the induction step. Let $1 \leq k \leq n/2$ be given. We may and will assume that $n \geq n_0$. By Lemmas 4.3 and 4.4 the claim holds for $k \leq \frac{n}{\log n}$ and for $k \geq \frac{n}{2} - \frac{n}{\log n}$. So we may assume $\frac{n}{\log n} < k < \frac{n}{2} - \frac{n}{\log n}$.

Let R_0 and R_1 be the two numbers given by the second claim of Proposition 4.5. Consider first the case $R_0 \leq \frac{R_1}{9}$. Then, by Proposition 4.5 and by the induction hypothesis we have

$$R(n,k) \;\leq\; R_1 \;\leq\; R(n-1,k-1) \;\leq\; C \cdot 2^{5\frac{n-1}{\log(n-1)}} \cdot r(n-1,k-1) \;\leq\; C \cdot 2^{5\frac{n}{\log(n)}} \cdot r(n,k).$$

Let us explain the last inequality. First, $\frac{n-1}{\log(n-1)} \leq \frac{n}{\log(n)}$, since the function $\frac{x}{\log x}$ is increasing for $x \geq e$. Second, $r(n-1,k-1) \leq r(n,k)$ since $S(n,k)$ contains an 'isomorphic copy' of $S(n-1,k-1)$, given by the k-tuples in $S(n,k)$ containing (any) fixed element, say 1.

The case $R_1 \leq \frac{R_0}{9}$ is treated similarly.

It remains to deal with the case $\frac{R_0}{9} < R_1 < 9R_0$. In this case, we have $R(n,k) \leq F\left(R_0, R_1\right)$. Let $\rho = \max\left\{\frac{R_0}{r(n-1,k)}, \frac{R_1}{r(n-1,k-1)}\right\}$. Note that by the induction hypothesis $\rho \leq C \cdot 2^{5\frac{n-1}{\log(n-1)}}$.

By Proposition 4.6 the point $\Big(r(n-1,k), r(n-1,k-1)\Big)$ lies in the domain $\{(x,y) : 0 < x/9 < y < 9x\}$ and hence so is the point $\rho \cdot \Big(r(n-1,k), r(n-1,k-1)\Big)$. By the monotonicity of F in this domain and by its 1-homogeneity, we have

$$F\left(R_0, R_1\right) \;\leq\; F\Big(\rho \cdot r(n-1,k), \rho \cdot r(n-1,k-1)\Big) \;=\; \rho \cdot F\Big(r(n-1,k), r(n-1,k-1)\Big) \;\leq\; C \cdot 2^{5\frac{n-1}{\log(n-1)}} \cdot F\Big(r(n-1,k), r(n-1,k-1)\Big)$$

By Proposition 4.6, the last expression is at most $C \cdot 2^{5\frac{n-1}{\log(n-1)}} \cdot \left(1 + c \cdot \frac{\log^{3/2} n}{\sqrt{n}}\right) \cdot r(n,k)$, for some absolute constant c. Since for large x we have $\left(\frac{x}{\log x}\right)' \sim \frac{1}{\log^2 x}$, for a sufficiently large n holds

$$2^{5\frac{n-1}{\log(n-1)}} \cdot \left(1 + c \cdot \frac{\log^{3/2} n}{\sqrt{n}}\right) \quad \leq \quad 2^{5\frac{n-1}{\log(n-1)} + \frac{c}{\ln 2} \cdot \frac{\log^{3/2} n}{\sqrt{n}}} \quad \leq \quad 2^{5\frac{n}{\log(n)}},$$

completing the proof of Proposition 4.1.

4.1.1 Proof of Proposition 4.5

We start with the first claim of the proposition. The function $F(x,y) = F(x,y) = \frac{8xy}{4\sqrt{xy} - \left(\sqrt{x} - \sqrt{y}\right)^2}$ is clearly 1-homogeneous. It's easy to see that it is defined on the domain $0 < x/9 < y < 9x$. A simple computation shows that $\frac{\partial F}{\partial x}$ is proportional to $3\sqrt{x} - \sqrt{y}$ and therefore is positive in this domain. Hence F increases in x. A similar argument shows that F increases in y as well. This completes the proof of the first claim.

We pass to the second claim of the proposition.

Let f be a function on $\{0,1\}^n$ with $supp\left(\widehat{f}\right) \subseteq S(n,k)$, such that $\frac{\mathbb{E} f^4}{\mathbb{E}^2 f^2} = R(n,k)$. Given a function h on $\{0,1\}^n$, we can view it as a pair of functions on the two $(n-1)$-dimensional cubes $\{x \in \{0,1\}^n, x_n = 0\}$ and $\{x \in \{0,1\}^n, x_n = 1\}$. We write this as $h \leftrightarrow (h_0, h_1)$. Let $\widehat{f} \leftrightarrow \left(\widehat{f_0}, \widehat{f_1}\right)$, and let g_0, g_1 be functions on the $(n-1)$-dimensional cube such that $g_i = \sum_\beta \widehat{f_i}(\beta) W_\beta$. It is easy to see that $f \leftrightarrow (g_0 + g_1, g_0 - g_1)$. Note that $supp\left(\widehat{g_0}\right) \subseteq S(n-1,k)$ and $supp\left(\widehat{g_1}\right) \subseteq S(n-1,k-1)$. We can now define the parameters R_0 and R_1. Let $R_0 = \frac{\mathbb{E} g_0^4}{\mathbb{E}^2 g_0^2}$. Then $R_0 \leq R(n-1,k)$. Similarly, let $R_1 = \frac{\mathbb{E} g_1^4}{\mathbb{E}^2 g_1^2}$. Then $R_1 \leq R(n-1,k-1)$.

A simple calculation and an application of the Cauchy-Schwarz inequality gives

$$R(n,k) \quad = \quad \frac{\mathbb{E} f^4}{\mathbb{E}^2 f^2} \quad = \quad \frac{\mathbb{E} g_0^4 + 6\,\mathbb{E} g_0^2 g_1^2 + \mathbb{E} g_1^4}{\mathbb{E}^2 g_0^2 + 2\,\mathbb{E} g_0^2\, \mathbb{E} g_1^2 + \mathbb{E}^2 g_1^2} \quad \leq \quad \frac{\mathbb{E} g_0^4 + 6\sqrt{\mathbb{E} g_0^4\, \mathbb{E} g_1^4} + \mathbb{E} g_1^4}{\mathbb{E}^2 g_0^2 + 2\,\mathbb{E} g_0^2\, \mathbb{E} g_1^2 + \mathbb{E}^2 g_1^2}$$

Let $m\left(g_0, g_1\right)$ be the supremum of the RHS over a 1-parameter family of expressions, where we replace g_1 with $\theta \cdot g_1$, for a real parameter θ. Clearly $R(n,k) \leq m\left(g_0, g_1\right)$. We will show that

$$m\left(g_0, g_1\right) \quad = \quad \begin{cases} R_0 & \text{if} \quad R_0 > 9R_1 \\ R_1 & \text{if} \quad R_1 > 9R_0 \\ F\left(R_0, R_1\right) & \text{otherwise,} \end{cases}$$

and this will complete the proof of the proposition.

Consider the following function of a nonnegative parameter $x = \theta^2$:

$$G(x) \quad = \quad \frac{\mathbb{E}\, g_1^4 \cdot x^2 + 6\sqrt{\mathbb{E}\, g_0^4\, \mathbb{E}\, g_1^4} \cdot x + \mathbb{E}\, g_0^4}{\mathbb{E}^2\, g_1^2 \cdot x^2 + 2\, \mathbb{E}\, g_0^2\, \mathbb{E}\, g_1^2 \cdot x + \mathbb{E}^2\, g_0^2} \quad =: \quad \frac{Ax^2 + Bx + C}{ax^2 + bx + c}$$

By definition $m\left(g_0, g_1\right) = \sup_{x \geq 0} G(x)$. It is easy to see that the derivative G' equals, up to a positive factor, to

$$Q(x) \quad = \quad \Big(Ab - aB\Big) \cdot x^2 + 2\Big(Ac - aC\Big) \cdot x + \Big(Bc - bC\Big),$$

where $Ab - aB = 2\sqrt{\mathbb{E}\, g_1^4}\, \mathbb{E}\, g_0^2 \mathbb{E}^2 g_1^2 \cdot \left(\sqrt{R_1} - 3\sqrt{R_0}\right)$, $Ac - aC = \mathbb{E}^2 g_0^2 \mathbb{E}^2 g_1^2 \cdot \left(R_1 - R_0\right)$, and $Bc - bC = 2\sqrt{\mathbb{E}\, g_0^4} \mathbb{E}^2 g_0^2\, \mathbb{E}\, g_1^2 \cdot \left(3\sqrt{R_1} - \sqrt{R_0}\right)$.

There are three cases to consider. If $R_0 \geq 9R_1$, then the leading coefficient of Q is non-positive, and the only nonnegative root it can have is at 0 (if $R_0 = 9R_1$). This means G is decreasing on $(0, \infty)$, and $m\left(g_0, g_1\right) = G(0) = R_0$. Similarly, if $R_1 \geq 9R_0$, then G increases on $(0, \infty)$, and $m\left(g_0, g_1\right) = G(\infty) = R_1$.

The interesting case is when $1/9R_1 < R_0 < 9R_1$, and then it is easy to see that the unique maximum of G is attained at the unique positive root of the quadratic inequality $Q = 0$, that is at

$$x \quad = \quad \frac{\Big(aC - Ac\Big) \; - \; \sqrt{\Big(Ac - aC\Big)^2 - \Big(Ab - aB\Big)\Big(Bc - bC\Big)}}{Ab - aB},$$

A rather tedious simplification gives

$$x \quad = \quad \frac{\mathbb{E}\, g_0^2}{2\sqrt{\mathbb{E}\, g_1^4}} \cdot T\left(R_0, R_1\right), \quad \text{where} \quad T(u, w) \quad = \quad \frac{6\sqrt{uw} - 2u}{3\sqrt{u} - \sqrt{w}}$$

Substituting this value of x, using the fact that $Q(x) = 0$, and simplifying, we get that

$$G(x) \quad = \quad \frac{Ax^2 + Bx + C}{ax^2 + bx + c} \quad = \quad \frac{2Ax + B}{2ax + b} \quad = \quad \frac{8R_0R_1}{4\sqrt{R_0R_1} - \left(\sqrt{R_0} - \sqrt{R_1}\right)^2} \quad = \quad F\left(R_0, R_1\right),$$

completing the proof of the proposition.

4.1.2 Proof of Proposition 4.6

From now on we assume (in this subsection) that the assumptions of the proposition hold, that is that n is sufficiently large and that $\frac{n}{\log n} \leq k \leq \frac{n}{2} - \frac{n}{\log n}$.

Recall that $r(n, k) = \frac{1}{\binom{n}{k}^2} \cdot \sum_{t=0}^{k} \binom{n}{2t} \left(\binom{2t}{t} \cdot \binom{n-2t}{k-t}\right)^2 = \sum_{t=0}^{k} s_t(n, k)$, where $s_t(n, k) = \frac{1}{\binom{n}{k}^2} \cdot \binom{n}{2t} \left(\binom{2t}{t} \cdot \binom{n-2t}{k-t}\right)^2$. We start with the following claim.

Lemma 4.7: *Let* $t_1(n,k) = \frac{3n-\sqrt{n^2+8(n-2k)^2}}{8}$. *Then*

1. $\frac{k}{3} \le t_1(n,k) \le \frac{11k}{12}$.
2. *Let* $3 \le \Delta < t_1(n,k)$. *Then for* $1 \le t \le t_1(n,k) - \Delta$ *holds*
$$\frac{s_{t+1}}{s_t} \quad \ge \quad 1 + \frac{\Delta}{t}$$
3. *Let* $\log n \le \Delta < k - t_1(n,k)$. *Then for* $t_1(n,k) + \Delta \le t \le k-1$ *holds*
$$\frac{s_{t+1}}{s_t} \quad \le \quad 1 - \frac{\Delta}{t}$$

We record two immediate corollaries of this lemma. Choosing $\Delta = \sqrt{n\log n}$, we obtain

$$\max_{0\le t\le k} s_t(n,k) \quad = \quad \max_{t\in t_1(n,k)\pm\sqrt{n\log n}} s_t(n,k),$$

which is the claim of Lemma 4.2. Another immediate corollary is that

Corollary 4.8: *There is an interval of length* $L = L(n) = O\left(\sqrt{n\log n}\right)$ *such that*

$$r(n,k) \quad \le \quad \left(1+\frac{1}{n}\right)\cdot \sum_{t_1-L\le t\le t_1+L} s_t$$

Proof: (of Lemma 4.7)

We start with the first claim of the lemma. We have that

$$t_1(n,k) \;=\; \frac{3n-\sqrt{n^2+8(n-2k)^2}}{8} \;=\; \frac{32k(n-k)}{8\cdot(3n+\sqrt{n^2+8(n-2k)^2})} \;\ge\; \frac{4k(n-k)}{6n} \;\ge\; \frac{k}{3},$$

where the last inequality holds since $k \le n/2$.

On the other hand, $k - t_1(n,k) = \frac{\sqrt{n^2+8(n-2k)^2}-(3n-8k)}{8}$. If $k \ge 3n/8$, this is at least $\frac{\sqrt{n^2+8(n-2k)^2}}{8} \ge \frac{n}{8} \ge \frac{k}{4}$. Otherwise, if $k < 3n/8$, this equals

$$\frac{n^2+8(n-2k)^2-(3n-8k)^2}{8\cdot\left(\sqrt{n^2+8(n-2k)^2}+(3n-8k)\right)} \;=\; \frac{2k(n-2k)}{\sqrt{n^2+8(n-2k)^2}+(3n-8k)} \;>\; \frac{2k\cdot n/4}{6n} \;\ge\; \frac{k}{12}.$$

We proceed to the second and the third claims. Consider the ratio s_{t+1}/s_t. After some simplifying, this ratio is

$$\frac{\binom{n}{2t+2}\left(\binom{2t+2}{t+1}\binom{n-2t-2}{k-t-1}\right)^2}{\binom{n}{2t}\left(\binom{2t}{t}\binom{n-2t}{k-t}\right)^2} \quad = \quad \frac{2(2t+1)}{(t+1)^3}\cdot\frac{(k-t)^2(n-k-t)^2}{(n-2t)(n-2t-1)} \quad =$$

$$\left(\frac{2(k-t)(n-k-t)}{t(n-2t)}\right)^2 \cdot \Big(1+\epsilon(n,t)\Big), \quad \text{where} \quad 1+\epsilon(n,t) \;=\; \frac{(2t+1)t^2}{2(t+1)^3} \cdot \frac{n-2t}{n-2t-1}$$

It is easy to see that, in our assumptions for k and n, we have $-\frac{3}{t} \leq \epsilon(n,t) \leq \frac{1}{n-2t}$. We introduce some notation. Let $r(t) = \frac{2(k-t)(n-k-t)}{t(n-2t)}$, and let $q(t) = 4t^2 - 3nt + 2k(n-k)$. Then $\frac{s_{t+1}}{s_t} = r^2(t) \cdot \big(1+\epsilon(n,t)\big)$, and $r(t) = 1 + \frac{q(t)}{t(n-2t)}$.

The roots of the quadratic $q(t)$ are $t_{1,2}(n,k) = \frac{3n \pm \sqrt{n^2+8(n-2k)^2}}{8}$. (From now on till the end of this subsection we write t_1, t_2 for $t_1(n,k)$ and $t_2(n,k)$.) We know that $t_1 < k$ and it is easy to see that $t_2 > n/2 > k$. Hence, for $t \leq t_1 - \Delta$ we have:

$$r(t) \quad = \quad 1 + \frac{q(t)}{t(n-2t)} \quad = \quad 1 + \frac{4\,(t-t_1)\,(t-t_2)}{t(n-2t)} \quad \geq \quad 1 + \frac{4\Delta \cdot (t_2 - t_1)}{t(n-2t)} \quad =$$

$$\frac{\Delta \cdot \sqrt{n^2+8(n-2k)^2}}{t(n-2t)} \quad \geq \quad 1 + \frac{\Delta n}{t(n-2t)} \quad \geq \quad 1 + \frac{\Delta}{t}$$

Therefore, $\frac{s_{t+1}}{s_t} = r^2(t) \cdot \big(1+\epsilon(n,t)\big) \geq 1 + \frac{2\Delta}{t} - \frac{3}{t} \geq 1 + \frac{\Delta}{t}$. This completes the proof of the second claim of the lemma.

For $t_1 + \Delta \leq t \leq k-1$, we have

$$r(t) \quad = \quad 1+\frac{4\,(t-t_1)\,(t-t_2)}{t(n-2t)} \quad \leq \quad 1-\frac{4\Delta \cdot (t_2 - t)}{t(n-2t)} \quad \leq \quad 1-\frac{4\Delta \cdot \left(\frac{n}{2} - t\right)}{t(n-2t)} \quad = \quad 1-\frac{2\Delta}{t}$$

Therefore $\frac{s_{t+1}}{s_t} \leq 1 - \frac{2\Delta}{t} + \frac{1}{n-2t} \leq 1 - \frac{\Delta}{t}$, recalling that $\Delta \geq \log(n)$, and $n-2t \geq n-2k \geq 2\frac{n}{\log n}$.

▮

Corollary 4.9:

1.

$$\frac{r(n,k-1)}{r(n,k)} \in \left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot \left(\frac{n-k}{k} \cdot \frac{k-t_1}{n-k-t_1}\right)^2$$

2.

$$\frac{r(n-1,k-1)}{r(n,k)} \in \left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot \frac{n}{n-2t_1} \cdot \left(\frac{k-t_1}{k}\right)^2$$

Proof: We prove only the first claim of the corollary. The proof of the remaining claim is similar.

Note that $|t_1(n,k) - t_1(n,k-1)| \leq 1$. Let $L = O\left(\sqrt{n \log n}\right)$ be the length of the interval around $t_1 = t_1(n,k)$ such that both $r(n,k)$ and $r(n,k-1)$ are attained, up to an $(1-1/n)$-factor by summing the corresponding summands in this interval (by Corollary 4.8). It suffices to show that for any t in the interval $t_1 \pm L$ holds $s_t(n,k-1)/s_t(n,k) \in 1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)$. Indeed we have

$$\begin{aligned}
\frac{s_t(n,k-1)}{s_t(n,k)} &= \left(\frac{n-k}{k} \cdot \frac{k-t}{n-k-t}\right)^2 = \\
&\left(\frac{k-t}{k-t_1} \cdot \frac{n-k-t_1}{n-k-t}\right)^2 \cdot \left(\frac{n-k}{k} \cdot \frac{k-t_1}{n-k-t_1}\right)^2 \in \\
&\left(1 \pm O\left(\frac{L}{k}\right)\right) \cdot \left(1 \pm O\left(\frac{L}{n}\right)\right) \cdot \left(\frac{n-k}{k} \cdot \frac{k-t_1}{n-k-t_1}\right)^2 \subseteq \\
&\left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot \left(\frac{n-k}{k} \cdot \frac{k-t_1}{n-k-t_1}\right)^2
\end{aligned}$$

∎

We are now ready to prove Proposition 4.6. The first claim of the proposition is that $1/9 < \frac{r(n,k-1)}{r(n,k)} < 9$. In fact, it is easy to see that for all $0 \le t \le k-1$ holds $\frac{s_t(n,k-1)}{s_t(n,k)} = \left(\frac{n-k}{k} \cdot \frac{k-t}{n-k-t}\right)^2 \le 1$, so the upper bound trivially holds, even with 9 replaced by 1. We pass to the lower bound. By the first claim of Corollary 4.9 it suffices to show that for some absolute constant $c > 0$ holds $1/3 + c/\log(n) \le \frac{n-k}{k} \cdot \frac{k-t_1}{n-k-t_1}$. We write δ for $c/\log(n)$.

After rearranging, we need to show that $t_1 \le \frac{(2/3-\delta)k(n-k)}{(n-k)-(1/3+\delta)k}$. This would follow from a stronger inequality $t_1 \le \left(1 - \frac{3\delta}{2}\right) \cdot \frac{2k(n-k)}{3n-4k}$. Recall that t_1 is a root of the quadratic $4t^2 - 3nt + 2k(n-k)$. Substituting $3nt_1 - 4t_1^2$ for $2k(n-k)$ it is easy see that this inequality would follow from $\frac{3n-4t_1}{3n-4k} \ge 1 + 3\delta$. Recall that $t_1 \le \frac{11k}{12}$, and that $k \ge \frac{n}{\log(n)}$. Hence $\frac{3n-4t}{3n-4k} \ge 1 + \frac{k}{3(3n-4k)} \ge 1 + \frac{1}{9\log(n)}$, completing the proof (for c small enough). ∎

We pass to the second claim of the proposition. Let $x = r(n-1,k-1)$. Let $y = \frac{k^2(n-k-t_1)^2}{(n-k)^2(k-t_1)^2} \cdot x$. Let $z = \frac{(n-2t_1)k^2}{n(k-t_1)^2} \cdot x$. By Corollary 4.9 we have that $y \in \left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot r(n-1,k)$ and $z \in \left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot r(n,k)$.

Next we claim that $z = F(x,y)$. Since F is 1-homogeneous, it suffices to verify the identity

$$\frac{(n-2t_1)\,k^2}{n\,(k-t_1)^2} = F\left(1, \frac{k^2\,(n-k-t_1)^2}{(n-k)^2\,(k-t_1)^2}\right).$$

Simplifying, it is the same as showing:

$$\frac{n-2t_1}{n} = \frac{8\,(n-k-t_1)^2\,(k-t_1)^2}{6k(n-k)\,(n-k-t_1)\,(k-t_1) - k^2\,(n-k-t_1)^2 - (n-k)^2\,(k-t_1)^2}.$$

This can be verified by applying several times the identity $4t_1^2 - 3nt_1 + 2k(n-k) = 0$. We omit the details.

Now we can conclude the proof. Let $\rho = \max\left\{\frac{r(n-1,k)}{y}, 1\right\}$. Then $\rho \le 1 + O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)$. By the proof of the first claim of the proposition, the point (x, y) lies in the domain $0 < x/9 < y < 9x$ and hence also the point $(\rho \cdot x, \rho \cdot y)$. Both coordinates of this point are larger or equal to those of $\Big(r(n-1, k-1), r(n-1, k)\Big)$, which, by the first claim of the proposition, also lies in this domain. By the 1-homogeneity and monotonicity of F in this domain we have

$$F\Big(r(n-1, k-1), r(n-1, k)\Big) \le F(\rho x, \rho y) = \rho F(x, y) = \rho z \in \left(1 \pm O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right) \cdot r(n, k).$$

∎

4.2 Proof of (8)

We start with some simple observations. First, as above, by making the constant hidden in the asymptotic notation to be large enough, we may assume that the claim holds for $n \le n_0$, for any fixed n_0 of our choice. Next, it suffices to show the claim for $k \ge k_0$, for any fixed k_0 that we choose. This is because for $k < k_0$ the set $S(n, k)$ may be viewed as a subset of $S\big(n + (k_0 - k), k_0\big)$ (see a similar argument in the proof of Proposition 4.1). From now on we assume $n \ge n_0$ and $k \ge k_0$, for sufficiently large n_0 and k_0.

We will work with the function ϕ introduced in the proof of Theorem 1.8. Recall that ϕ is a function on $\left[0, \frac{k}{n}\right]$ defined by $\phi(y) = H(2y) + 4y + 2(1-2y) \cdot H\left(\frac{k/n - y}{1-2y}\right) - 2H\left(\frac{k}{n}\right)$, and that $\psi\left(\frac{k}{n}\right) = \phi\left(\frac{t_1(n,k)}{n}\right)$.

Let t_1 stand for $t_1(n, k)$, and let $t^* = \lceil t_1 \rceil$. We proceed as follows: First, we observe that ϕ is defined on $\frac{t^*}{n}$ and that $2^{n\phi\left(\frac{t^*}{n}\right)} \le O\left(k^{3/2}\right) \cdot r(n, k)$. Then we show that $\phi\left(\frac{t_1}{n}\right)$ and $\phi\left(\frac{t^*}{n}\right)$ differ by at most $O\left(\frac{1}{n}\right)$, which implies $2^{n\psi\left(\frac{k}{n}\right)} = 2^{n\phi\left(\frac{t_1}{n}\right)} \le O\left(2^{n\phi\left(\frac{t^*}{n}\right)}\right)$, and completes the proof.

By Lemma 4.7, $t_1 \le \frac{11k}{12}$, and hence $t^* \le t_1 + 1 \le k$. Therefore ϕ is defined on $\frac{t^*}{n}$. Next, recall that, by Stirling's formula, for all $0 < a < b$ holds $\binom{b}{a} = \Theta\left(\sqrt{\frac{b}{a(b-a)}}\right) \cdot 2^{bH(a/b)}$, and in particular, for $0 < a \le b/2$ holds $\binom{b}{a} = \Theta\left(\sqrt{\frac{1}{a}}\right) \cdot 2^{bH(a/b)}$. Substituting this estimate for the binomial coefficients in the formula for $s_{t^*}(n, k)$ gives

$$r(n, k) \;\ge\; s_{t^*}(n, k) \;=\; \Theta\left(\frac{k}{t^*\,(k - t^*)} \cdot \sqrt{\frac{n}{2t^*\,(n - 2t^*)}}\right) \cdot 2^{n\phi\left(\frac{t^*}{n}\right)} \;\ge\; \Omega\left(k^{-\frac{3}{2}}\right) \cdot 2^{n\phi\left(\frac{t^*}{n}\right)}.$$

Next, we argue that $\left|\phi\left(\frac{t_1}{n}\right) - \phi\left(\frac{t^*}{n}\right)\right| \le O\left(\frac{1}{n}\right)$. Since $t_1 \le t^* < t_1 + 1$, it suffices to show that the absolute value of the derivative of ϕ is bounded by a constant on $\left(\frac{t_1}{n}, \frac{t^*}{n}\right)$. Let $a := \frac{k}{n}$. Then

$$\frac{1}{2}\phi'(y) \quad = \quad \log\left(\frac{1-2y}{2y}\right) + 2 - 2H\left(\frac{a-y}{1-2y}\right) - \frac{1-2a}{1-2y} \cdot \log\left(\frac{1-a-y}{a-y}\right) \qquad (9)$$

Let $\frac{t_1}{n} < y < \frac{t^*}{n}$. Then, by Lemma 4.7 and by our assumptions on k and n, we have that $0 < a \leq \frac{1}{2}$ and $c_1 a \leq y \leq (1-c_2)\,a$, for some absolute constants $0 < c_1, c_2 < 1$. It is easy to see that for a bounded away from zero all the terms on the RHS of (9) are bounded. Hence it only remains to consider the case $a \to 0$. To deal with this case, we can rewrite (9) as follows (omitting the second and the third term on the RHS, since their contribution is bounded by 2):

$$\frac{1}{2}\phi'(y) \quad \approx \quad \log\left(\frac{1-2y}{2y}\right) - \frac{1-2a}{1-2y}\cdot\log\left(\frac{1-a-y}{a-y}\right) \quad =$$

$$\left(\log\left(\frac{1-2y}{2y}\right) - \log\left(\frac{1-a-y}{a-y}\right)\right) + 2\frac{a-y}{1-2y}\cdot\log\left(\frac{1-a-y}{a-y}\right) \quad =$$

$$\log\left(\frac{1-2y}{1-a-y}\right) + \log\left(\frac{a-y}{2y}\right) + 2\frac{a-y}{1-2y}\cdot\log\left(\frac{1-a-y}{a-y}\right).$$

It is easy to see that all the summands in the last expression are bounded by a constant, completing the proof of (8).

∎

4.3 Proof of Corollary 1.11

We start with the first claim. Let $A \subseteq \{0,1\}^n$ be a Hamming ball of radius k. First, we observe that Proposition 4.1 implies the following bound on $\mu(A)$.

$$\mu(A) \quad \leq \quad C\cdot(k+1)^3 2^{5n/\log(n)}\cdot r(n,k). \tag{10}$$

To see this, let f be a function on $\{0,1\}^n$ with $supp\left(\widehat{f}\right) \subseteq A$. Write $f = \sum_{i=0}^k f_i$, with $supp\left(\widehat{f}\right) \subseteq S(n,i)$, for $i = 0, ..., k$. By Proposition 4.1, we have $\mathbb{E}\, f_i^4 \leq C\cdot 2^{5n/\log(n)}\cdot r(n,i)\cdot \mathbb{E}^2\, f_i^2$. In the proof of Proposition 4.6, we have observed that $s_t(n,k-1) \leq s_t(n,k)$, for all $0 \leq t \leq k-1$, which implies $r(n,k-1) \leq r(n,k)$, and hence $r(n,i) \leq r(n,k)$, for all $0 \leq i \leq k$. Consequently, we have $\mathbb{E}\, f_i^4 \leq C\cdot 2^{5n/\log(n)}\cdot r(n,k)\cdot\mathbb{E}^2\, f_i^2$. Observing that the functions $\{f_i\}$ are orthogonal, and using Jensen's inequality, we have:

$$\mathbb{E}\, f^4 \;\leq\; (k+1)^3\cdot\sum_{i=0}^k \mathbb{E}\, f_i^4 \;\leq\; C\cdot(k+1)^3 2^{5n/\log(n)}\cdot r(n,k)\cdot\sum_{i=0}^k \mathbb{E}^2 f_i^2 \;\leq$$

$$C\cdot(k+1)^3 2^{5n/\log(n)}\cdot r(n,k)\cdot\left(\sum_{i=0}^k \mathbb{E}\, f_i^2\right)^2 \;=\; C\cdot(k+1)^3 2^{5n/\log(n)}\cdot r(n,k)\cdot\mathbb{E}^2 f^2,$$

completing the proof of (10).

The inequality $\mu(A) \leq 2^{n\psi\left(\frac{k}{n}\right)}$ can now be derived from (10) by a 'tensorization argument', as in derivation of the first claim of Theorem 1.8 from Proposition 4.1. We omit the details.

We pass to the second claim. It suffices to show that $\psi(x) \leq \min\{2\log_2(3)\cdot x, 1\}$ for all $0 \leq x \leq 1/2$, and moreover $\psi(x) = 2\log_2(3)\cdot x$ only at $x = 0$, and $\psi(x) = 1$ only at $x = 1/2$. The key observation is that ψ is strongly concave.

Lemma 4.10: *For all* $0 < x \leq 0.5$ *holds* $\psi''(x) < 0$.

Proof:

We have that

$$\psi'(x) \quad = \quad 2r' \cdot \log_2\left(\frac{1-2r}{2r}\right) + 4r' \cdot \left(1 - H\left(\frac{x-r}{1-2r}\right)\right) +$$

$$2 \cdot \left(1 - \frac{(1-2x)r'}{1-2r}\right) \cdot \log_2\left(\frac{1-x-r}{x-r}\right) - 2\log_2\left(\frac{1-x}{x}\right),$$

and, after some rearrangement, that

$$\frac{1}{2} \cdot \psi''(x) \quad = \quad r'' \cdot \left(\log_2\left(\frac{1-2r}{2r}\right) + 2 \cdot \left(1 - H\left(\frac{x-r}{1-2r}\right)\right) - \frac{1-2x}{1-2r} \cdot \log_2\left(\frac{1-x-r}{x-r}\right) \right) -$$

$$\frac{(r')^2}{\ln 2 \cdot r(1-2r)} - \frac{\big((1-2r) - (1-2x)r'\big)^2}{\ln 2 \cdot (1-2r)(x-r)(1-x-r)} + \frac{1}{\ln 2 \cdot x(1-x)}$$

We claim that the term which multiplies r'' is zero. To see that, we make some observations about the function r, which will be useful later on as well. First, it is easy to see that it increases from 0 to 0.25 on $[0, 0.5]$. Next, we have $r' = \frac{2-4x}{3-8r}$, and finally the identity $\frac{1}{2}\left(3r - 4r^2\right) = x(1-x)$, which follows e.g., from the fact that $t_1(n,k)$ is a root of the quadratic $4t^2 - 3nt + 2k(n-k) = 0$.

Next, after some simplifying, we have

$$\log_2\left(\frac{1-2r}{2r}\right) + 2 \cdot \left(1 - H\left(\frac{x-r}{1-2r}\right)\right) - \frac{1-2x}{1-2r} \cdot \log_2\left(\frac{1-x-r}{x-r}\right) = \log_2\left(\frac{2(x-r)(1-x-r)}{r(1-2r)}\right).$$

Using the identity $\frac{1}{2} \cdot \left(3r - 4r^2\right) = x(1-x)$, it is easy to see that $2(x-r)(1-x-r) = r(1-2r)$ and hence the RHS vanishes. This simplifies the expression for ψ'' to:

$$\psi''(x) \quad = \quad -\frac{2}{\ln 2} \cdot \left(\frac{(r')^2}{r(1-2r)} + \frac{\big((1-2r) - (1-2x)r'\big)^2}{(1-2r)(x-r)(1-x-r)} - \frac{1}{x(1-x)} \right)$$

Since $r' = \frac{2-4x}{3-8r}$, we have $(r')^2 = \frac{4(1-2x)^2}{(3-8r)^2} = \frac{4(1-2r)(1-4r)}{(3-8r)^2}$. Similarly, $(1-2x)r' = \frac{2(1-2x)^2}{3-8r} = \frac{2(1-2r)(1-4r)}{3-8r}$. Making these substitutions, replacing $(x-r)(1-x-r)$ with $\frac{1}{2}r(1-2r)$ and $x(1-x)$ with $\frac{1}{2}\left(3r - 4r^2\right)$, and simplifying, we get

$$\frac{(r')^2}{r(1-2r)} + \frac{\big((1-2r) - (1-2x)r'\big)^2}{(1-2r)(x-r)(1-x-r)} - \frac{1}{x(1-x)} \quad = \quad \frac{8}{(3-8r)(3-4r)} \quad > \quad 0,$$

completing the proof of the lemma.

▮

We can now complete the proof of the second claim of the corollary. It is easy to see that $\psi'(1/2) = 0$. Since ψ'' is negative, this means that ψ' is positive on $(0, 1/2)$ and hence the unique maximum of ψ is at $1/2$, where it equals 1.

On the other hand, using the fact that $r'(0) = 2/3$, it is easy to see that $\lim_{x\to 0} \psi'(x) = 2\log_2(3)$. Since ψ'' is negative, this means that $\psi' < 2\log_2(3)$ on $(0, 1/2)$ and hence that $\psi(x) < 2\log_2(3)\cdot x$ for all $0 < x \leq 1/2$.

▮

References

[1] A. Bonami, *Etude des coefficients Fourier des fonctions de Lp(G)*, Annales de lInstitut Fourier, 20(2) (1970), 335402.

[2] D. L. Donoho and P. B. Stark, *Uncertainty principles and signal recovery*, SIAM J. Applied Math., 49(1989), 906-931.

[3] W. T. Gowers, *A new proof of Szemeredi's theorem for arithmetic progressions of length four*, GAFA 8 (1998), 529-551.

[4] B. Green and T. Tao, *Freiman's Theorem in Finite Fields via Extremal Set Theory*, Combinatorics, Probability & Computing, Vol. 18(3) (2009), 335-355.

[5] J. Hastad, personal communication.

[6] J. Kahn and R. Meshulam, *Uncertainty inequalities on Hamming cubes*, unpublished (1996).

[7] J. H. van Lint, **Introduction to coding theory**, Springer-Verlag, Berlin, 1999.

[8] P. Nayar and K. Oleszkiewicz, *Khinchine type inequalities with optimal constants via ultra log-concavity*, Positivity, 2012.

[9] R. O'Donnel, **Analysis of Boolean functions**, Cambridge University Press, 2014.

[10] Y. Polyanskiy and A. Samorodnitsky, *Improved log-Sobolev inequalities, hypercontractivity and uncertainty principle on the hypercube*, arXiv:1606.07491, 2016.

[11] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Analysis & PDE, 5(3), 2012, 627-655.

[12] I.D. Shkredov, *An introduction to higher energies and sumsets*, arXiv:1512.00627, 2015.

[13] T. Tao and V. Vu, **Additive Combinatorics**, Cambridge University Press 2006.