

Sharp estimates for Gowers norms on discrete cubes

Supported in part by HRZZ IP-2022-10-5116 (FANAP)

Tuesday, October 8, 2024

Vjekoslav Kovač (University of Zagreb)

joint work with Adrian Beker (U. of Zagreb) and Tonći Crmarić (U. of Split)

Analysis and Geometry on Discrete Spaces, HIM workshop, Bonn

$A \subset \mathbb{Z}^d$ finite set

Additive energy [Tao and Vu (2006)]:

$$E_2(A) := |\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 - a_2 = a_3 - a_4\}|$$

Generalizations by Schoen and Shkredov (2013), Shkredov (2014), de Dios Pont, Greenfeld, Ivanisvili, and Madrid (2021).

Higher energies:

$$\tilde{E}_k(A) := |\{(a_1, a_2, \dots, a_{2k-1}, a_{2k}) \in A^{2k} : a_1 - a_2 = \dots = a_{2k-1} - a_{2k}\}|$$

k -additive energies:

$$E_k(A) := |\{(a_1, \dots, a_{2k}) \in A^{2k} : a_1 + \dots + a_k = a_{k+1} + \dots + a_{2k}\}|$$

Counting k -parallelotopes in A [Shkredov (2014)]:

$$P_k(A) := |\{(a, h_1, \dots, h_k) \in (\mathbb{Z}^d)^{k+1} : a + \epsilon_1 h_1 + \dots + \epsilon_k h_k \in A$$

for every $(\epsilon_1, \dots, \epsilon_k) \in \{0, 1\}^k\}|$

What can be said if additionally

$$A \subseteq \{0, 1\}^d \subset \mathbb{Z}^d?$$

Kane and Tao (2017):

$$E_2(A) \leq |A|^{\log_2 6}.$$

De Dios Pont, Greenfeld, Ivanisvili, and Madrid (2021):

$$\tilde{E}_k(A) \leq |A|^{\log_2(2^k+2)} \quad \text{for } k \geq 2.$$

De Dios Pont, Greenfeld, Ivanisvili, and Madrid (2021), κ. (2022):

$$E_k(A) \leq |A|^{\log_2 \binom{2k}{k}} \quad \text{for } k \geq 2.$$

All these exponents are seen to be sharp by taking $A = \{0, 1\}^d$.

What can be said if

$$A \subseteq \{0, 1, 2, \dots, n-1\}^d \subset \mathbb{Z}^d?$$

Already for $n = 3$ the sharp estimate is

$$E_2(A) \leq |A|^{2.7207109973\dots}$$

and the exponent is just some strange number.

Shao (2024) studied the optimal exponent t_n in

$$A \subseteq \{0, 1, \dots, n-1\}^d \implies E_2(A) \leq |A|^{t_n}$$

and showed

$$3 - (1 + o^{n \rightarrow \infty}(1)) \frac{3 \log_2 3 - 4}{2 \log_2 n} \leq t_n \leq 3 - \frac{c}{\log_2 n}$$

We study the gen. energies P_k . Let $t_{k,n}$ be the optimal exponent in

$$A \subseteq \{0, 1, \dots, n-1\}^d \implies P_k(A) \leq |A|^{t_{k,n}}$$

Three theorems. [Beker, Crmarić, and K. (2024)]:

$$t_{k,2} = \log_2(2k+2)$$

For a fixed $k \geq 2$ and $n \rightarrow \infty$:

$$k+1 - (1 + o_k^{n \rightarrow \infty}(1)) \frac{(k+1) \log_2(k+1) - 2k}{2 \log_2 n} \leq t_{k,n} \leq k+1 - \frac{c}{\log_2 n}$$

For a fixed $n \geq 2$ and $k \rightarrow \infty$:

$$t_{k,n} = \frac{(n-1) \log_2(2k) - \log_2(n-1)!}{H_{n-1}} + o_n^{k \rightarrow \infty}(1),$$

where $H_m := -\sum_{j=0}^m \frac{\binom{m}{j}}{2^m} \log_2 \frac{\binom{m}{j}}{2^m}$ is the entropy of $B(m, 1/2)$.

Numerous sharp inequalities in analysis are known for

$$f: \mathbb{Z}^d \rightarrow \mathbb{C}.$$

(Think of Hausdorff–Young, Young’s convolution ineq., etc.)

What changes if

$$\text{supp } f \subseteq \{0, 1, 2, \dots, n-1\}^d?$$

Can they be refined?

Example.

Sharp Hausdorff-Young on \mathbb{Z} :

$$\|\widehat{f}\|_{L^4(\mathbb{T})} \leq \|f\|_{\ell^{4/3}(\mathbb{Z})}$$

Shao (2024):

$$\text{supp } f \subseteq \{0, 1, \dots, n-1\} \implies \|\widehat{f}\|_{L^4(\mathbb{T})} \leq \|f\|_{\ell^{q_n}(\mathbb{Z})},$$

where

$$q_n = \frac{4}{3 - c/\log_2 n} > \frac{4}{3}.$$

Gowers uniformity norms [Gowers (2001)]:

$$\|f\|_{U^k} := \left(\sum_{a, h_1, \dots, h_k} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} \mathcal{C}^{\epsilon_1 + \dots + \epsilon_k} f(a + \epsilon_1 h_1 + \dots + \epsilon_k h_k) \right)^{1/2^k}$$

where $\mathcal{C}: z \mapsto \bar{z}$.

Note:

$$P_k(A) = \|\mathbb{1}_A\|_{U^k}^{2^k}$$

Sharp estimate:

$$\|f\|_{U^k(\mathbb{Z}^d)} \leq \|f\|_{\ell^{p_k}(\mathbb{Z}^d)}$$

for $p_k = 2^k / (k + 1)$.

Let $p_{k,n}$ be the optimal exponent in

$$\text{supp } f \subseteq \{0, 1, \dots, n-1\}^d \implies \|f\|_{\mathcal{U}^k(\mathbb{Z}^d)} \leq \|f\|_{\ell^{p_{k,n}}(\mathbb{Z}^d)}$$

We will see that

$$p_{k,n} t_{k,n} = 2^k.$$

Proposition. [Beker, Crmarić, and K. (2024)] $k, n \geq 2$, $p, t > 0$, $pt = 2^k$. The following are equivalent.

- (1) $\|f\|_{\mathcal{U}^k} \leq \|f\|_{\ell^p}$ holds for every $f: \mathbb{Z} \rightarrow [0, \infty)$ supported in $\{0, 1, \dots, n-1\}$.
- (2) $\|f\|_{\mathcal{U}^k} \leq \|f\|_{\ell^p}$ holds for every $d \geq 0$ and every $f: \mathbb{Z}^d \rightarrow \mathbb{C}$ supported in $\{0, 1, \dots, n-1\}^d$.
- (3) $P_k(A) \leq |A|^t$ holds for every $d \geq 0$ and every $A \subseteq \{0, 1, \dots, n-1\}^d$.
- (4) There exists $C \in (0, \infty)$ such that $P_k(A) \leq C|A|^t$ holds for every $d \geq 0$ and every $A \subseteq \{0, 1, \dots, n-1\}^d$.

We are essentially imitating the proof by de Dios Pont, Greenfeld, Ivanisvili, and Madrid (2021), who studied E_k and $\|\underbrace{f * f * \dots * f}_{k \text{ times}}\|_{\ell^2}^2$.

The assumption (1) is: for $g: \mathbb{Z} \rightarrow [0, \infty)$, $\text{supp } g \subseteq \{0, 1, \dots, n-1\}$

$$\sum_{b, l_1, \dots, l_k \in \mathbb{Z}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0, 1\}^k} g(b + \epsilon_1 l_1 + \dots + \epsilon_k l_k) \leq \left(\sum_{b=0}^{n-1} g(b)^p \right)^{2^k/p}$$

We prove the claim (2) by the induction on d .

Induction step: for each $b \in \mathbb{Z}$ define

$$f_b: \mathbb{Z}^{d-1} \rightarrow \mathbb{C}, \quad f_b(a) := f(a, b).$$

From the induction hypothesis:

$$\|f_b\|_{\mathbb{U}^k} \leq \|f_b\|_{\ell^p}$$

Write the LHS as the Gowers inner product:

$$\|f\|_{\mathbb{U}^k}^{2^k} = \sum_{b, l_1, \dots, l_k \in \mathbb{Z}} \langle (f_{b + \epsilon_1 l_1 + \dots + \epsilon_k l_k})_{(\epsilon_1, \dots, \epsilon_k) \in \{0, 1\}^k} \rangle_{\mathbb{U}^k}$$

The Gowers–Cauchy–Schwarz inequality yields

$$\begin{aligned} \|f\|_{U^k}^{2^k} &\leq \sum_{b, l_1, \dots, l_k \in \mathbb{Z}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} \|f_{b + \epsilon_1 l_1 + \dots + \epsilon_k l_k}\|_{U^k} \\ &\leq \sum_{b, l_1, \dots, l_k \in \mathbb{Z}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} \|f_{b + \epsilon_1 l_1 + \dots + \epsilon_k l_k}\|_{\ell^p} \end{aligned}$$

It remains to apply

$$\sum_{b, l_1, \dots, l_k \in \mathbb{Z}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} g(b + \epsilon_1 l_1 + \dots + \epsilon_k l_k) \leq \left(\sum_{b=0}^{n-1} g(b)^p \right)^{2^k/p}$$

with

$$g(b) := \|f_b\|_{\ell^p}$$

to conclude

$$\|f\|_{U^k}^{2^k} \leq \left(\sum_{b=0}^{n-1} \|f_b\|_{\ell^p}^p \right)^{2^k/p} = \|f\|_{\ell^p}^{2^k}.$$

The assumption (4) can be restated:

$$A \subseteq \{0, 1, \dots, n-1\}^d \implies \|\mathbb{1}_A\|_{\mathcal{U}^k} \leq D|A|^{t/2^k} = D\|\mathbb{1}_A\|_{\ell^p}$$

Decompose a general $f: \mathbb{Z}^d \rightarrow [0, \infty)$, $\text{supp } f \subseteq \{0, 1, \dots, n-1\}^d$ as

$$f = \sum_{i=0}^N \underbrace{\frac{M}{2^i} \mathbb{1}_{A_i}}_{f_i} + f',$$

where $M = \|f\|_{\ell^\infty}$, $N = \lceil d \log_2 n \rceil$, and $0 \leq f' < 2^{-N}M$. From

$$\|f_i\|_{\mathcal{U}^k} = \frac{M}{2^i} \|\mathbb{1}_{A_i}\|_{\mathcal{U}^k} \leq D \frac{M}{2^i} \|\mathbb{1}_{A_i}\|_{\ell^p} = D \|f_i\|_{\ell^p} \leq D \|f\|_{\ell^p},$$

$$\|f'\|_{\mathcal{U}^k} \leq M(n^d)^{(k+1)/2^k-1} \leq M \leq \|f\|_{\ell^p},$$

we get

$$\|f\|_{\mathcal{U}^k} \leq \sum_{i=0}^N \|f_i\|_{\mathcal{U}^k} + \|f'\|_{\mathcal{U}^k} \leq D(3 + d \log_2 n) \|f\|_{\ell^p}.$$

We remove the constant using the tensor power trick:

$$f(a_1, a_2, \dots, a_d) = g(a_1)g(a_2) \cdots g(a_d)$$

$$\implies \|f\|_{\mathcal{U}^k} = \|g\|_{\mathcal{U}^k}^d, \quad \|f\|_{\ell^p} = \|g\|_{\ell^p}^d$$

$$\implies \|g\|_{\mathcal{U}^k} \leq (D(3 + d \log_2 n))^{1/d} \|g\|_{\ell^p}$$

Letting $d \rightarrow \infty$ we obtain

$$\|g\|_{\mathcal{U}^k} \leq \|g\|_{\ell^p}.$$

One only needs to prove

$$\sum_{b, l_1, \dots, l_k \in \mathbb{Z}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} g(b + \epsilon_1 l_1 + \dots + \epsilon_k l_k) \leq \left(\sum_{b=0}^1 g(b)^{2^k/t} \right)^t$$

for $g: \mathbb{Z} \rightarrow [0, \infty)$, $\text{supp } g \subseteq \{0, 1\}$ and

$$t = \log_2(2k + 2).$$

Denoting

$$x = g(0)^{2^k/t}, \quad y = g(1)^{2^k/t}$$

this simplifies as

$$x, y \in [0, \infty) \implies x^t + y^t + 2kx^{t/2}y^{t/2} \leq (x + y)^t$$

A nice calculus exercise!

The lower bound

$$k + 1 - (1 + o_k^{n \rightarrow \infty}(1)) \frac{(k + 1) \log_2(k + 1) - 2k}{2 \log_2 n} \leq t_{k,n}$$

means

$$\liminf_{n \rightarrow \infty} ((t_{k,n} - k - 1) \log_2 n) \geq -\frac{k + 1}{2} \log_2(k + 1) + k.$$

The Gowers norms on \mathbb{R} :

$$\|f\|_{U^k(\mathbb{R})} := \left(\int_{\mathbb{R}^{k+1}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} e^{i\epsilon_1 + \dots + i\epsilon_k} f(x + \epsilon_1 h_1 + \dots + \epsilon_k h_k) dx dh_1 \dots dh_k \right)^{1/2^k}$$

Eisner and Tao (2012):

$$\|g\|_{U^k(\mathbb{R})} \leq C_k \|g\|_{L^{2^k/(k+1)}(\mathbb{R})}$$

with

$$C_k = \frac{2^{k/2^k}}{(k+1)^{(k+1)/2^{k+1}}}$$

and the equality is attained for Gaussians (among other extremizers).

$$f_{M,n}(m) := \begin{cases} \exp\left(-4M^2\left(\frac{m}{n} - \frac{1}{2}\right)^2\right) & \text{for } m \in \{0, 1, 2, \dots, n-1\}, \\ 0 & \text{otherwise} \end{cases}$$

is plugged into

$$\|f_{M,n}\|_{U^k} \leq \|f_{M,n}\|_{\ell^{p_{k,n}}}.$$

Denoting $g(x) := e^{-x^2}$ we get

$$\lim_{n \rightarrow \infty} \frac{1}{n^{k+1}} \|f_{M,n}\|_{U^k}^{2^k} = \frac{1}{(2M)^{k+1}} \|g \mathbb{1}_{[-M,M]}\|_{U^k(\mathbb{R})}^{2^k},$$

$$\limsup_{n \rightarrow \infty} \frac{1}{n^{t_{k,n}}} \|f_{M,n}\|_{\ell^{p_{k,n}}}^{2^k} \leq \frac{1}{(2M)^{k+1}} \|g \mathbb{1}_{[-M,M]}\|_{L^{2^k/(k+1)}(\mathbb{R})}^{2^k},$$

so take logarithms, subtract, and let $M \rightarrow \infty$:

$$\liminf_{n \rightarrow \infty} \left((t_{k,n} - k - 1) \log_2 n \right) \geq 2^k \log_2 \frac{\|g\|_{U^k(\mathbb{R})}}{\|g\|_{L^{2^k/(k+1)}(\mathbb{R})}} = 2^k \log_2 C_k$$

The upper bound

$$t_{k,n} \leq k + 1 - \frac{c}{\log_2 n}$$

will follow from Shao's result (2024) and

$$t_{k+1,n} \leq t_{k,n} + 1.$$

This is an easy consequence of a recursive formula

$$\|f\|_{\mathcal{U}^{k+1}}^{2^{k+1}} = \sum_{h \in \mathbb{Z}^d} \|\overline{f(\cdot + h)}f(\cdot)\|_{\mathcal{U}^k}^{2^k}$$

and Young's convolution inequality.

Recall that the *Shannon entropy* of

$$X \sim \begin{pmatrix} \cdots & 0 & 1 & 2 & \cdots & n-1 & \cdots \\ \cdots & q_0 & q_1 & q_2 & \cdots & q_{n-1} & \cdots \end{pmatrix}$$

is

$$H(X) := - \sum_j q_j \log_2 q_j.$$

We denoted

$$H_m := H(B(m, 1/2)).$$

For the lower bound

$$\liminf_{k \rightarrow \infty} \left(t_{k,n} - \frac{(n-1) \log_2(2k) - \log_2(n-1)!}{H_{n-1}} \right) \geq 0$$

start with

$$\sum_{a, h_1, \dots, h_k \in \mathbb{Z}} \prod_{(\epsilon_1, \dots, \epsilon_k) \in \{0,1\}^k} f(a + \epsilon_1 h_1 + \dots + \epsilon_k h_k) \leq \left(\sum_{j=0}^{n-1} f(j)^{2^k/t} \right)^t$$

for $t = t_{k,n}$ and only observe the mutually equal terms obtained by taking:

- $a \in \{0, 1, \dots, n-1\}$ arbitrary,
- precisely a of the numbers h_1, \dots, h_k equal -1 ,
- precisely $n-1-a$ of the numbers h_1, \dots, h_k equal 1 ,
- precisely $k-n+1$ of the numbers h_1, \dots, h_k equal 0 .

$$\binom{k}{n-1} 2^{n-1} \prod_{j=0}^{n-1} f(j) \binom{n-1}{j} 2^{k-n+1} \leq \left(\sum_{j=0}^{n-1} f(j) 2^{k/t_{k,n}} \right)^{t_{k,n}}.$$

Now take

$$f(j) := \left(\frac{\binom{n-1}{j}}{2^{n-1}} \right)^{t_{k,n}/2^k}$$

$$\Rightarrow \binom{k}{n-1} 2^{n-1} \prod_{j=0}^{n-1} \left(\frac{\binom{n-1}{j}}{2^{n-1}} \right)^{(n-1)t_{k,n}/2^{n-1}} \leq \left(\sum_{j=0}^{n-1} \frac{\binom{n-1}{j}}{2^{n-1}} \right)^{t_{k,n}} = 1.$$

Taking logarithms,

$$\underbrace{\sum_{j=0}^{n-2} \log_2(k-j)}_{(n-1) \log_2 k + o_n^{k \rightarrow \infty}(1)} - \log_2(n-1)! + (n-1) + \underbrace{\sum_{j=0}^{n-1} \frac{\binom{n-1}{j} t_{k,n}}{2^{n-1}} \log_2 \frac{\binom{n-1}{j}}{2^{n-1}}}_{-H_{n-1} t_{k,n}} \leq 0$$

For the upper bound

$$\limsup_{k \rightarrow \infty} \left(t_{k,n} - \frac{(n-1) \log_2(2k) - \log_2(n-1)!}{H_{n-1}} \right) \leq 0$$

split the same inequality as

$$\sum_{j=0}^{n-1} f(j)^{2^k} + \sum_{l=1}^{n-1} \sum_{(a, h_1, \dots, h_l) \in T_{n,l}} \binom{k}{l} \prod_{(\epsilon_1, \dots, \epsilon_l) \in \{0,1\}^l} f(a + \epsilon_1 h_1 + \dots + \epsilon_l h_l)^{2^{k-l}} \leq \left(\sum_{j=0}^{n-1} f(j)^{2^k/t} \right)^t,$$

$$T_{n,l} := \left\{ (a, h_1, \dots, h_l) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})^l : \right. \\ \left. 0 \leq a + \epsilon_1 h_1 + \dots + \epsilon_l h_l \leq n-1 \right. \\ \left. \text{for every } (\epsilon_1, \dots, \epsilon_l) \in \{0,1\}^l \right\}.$$

Substituting $g(j) = f(j)^{2^k/t}$ we reduce the inequality to

$$\sum_{j=0}^{n-1} g(j)^t + \sum_{l=1}^{n-1} \sum_{(a, h_1, \dots, h_l) \in T_{n,l}} \binom{k}{l} \prod_{(\epsilon_1, \dots, \epsilon_l) \in \{0,1\}^l} g(a + \epsilon_1 h_1 + \dots + \epsilon_l h_l)^{t/2^l} \leq 1$$

for every $g: \{0, 1, \dots, n-1\} \rightarrow [0, \infty)$ such that $\sum_{j=0}^{n-1} g(j) = 1$.

We are going to prove this for any given $0 < \delta < 1$,

$$t = \frac{(n-1) \log_2(2k) - \log_2(n-1)!}{H_{n-1}} + \delta,$$

and sufficiently large k .

The terms $g(j)^t$ are handled separately, by splitting into 2 cases, etc. Every other (more interesting) term is of the form

$$\binom{k}{l} (g(0)^{q_0} g(1)^{q_1} \dots g(n-1)^{q_{n-1}})^t,$$

where $(q_0, q_1, \dots, q_{n-1})$ is the distribution on the set $\{0, 1, \dots, n-1\}$ of

$$h_1 X_1 + \dots + h_l X_l,$$

where X_1, X_2, X_3, \dots are independent symmetric Bernoulli trials.

$$1 = \sum_{j=0}^{n-1} g(j) \geq \sum_{\substack{0 \leq j \leq n-1 \\ q_j \neq 0}} q_j \frac{g(j)}{q_j} \geq \prod_{\substack{0 \leq j \leq n-1 \\ q_j \neq 0}} \left(\frac{g(j)}{q_j} \right)^{q_j} = \frac{\prod_{j=0}^{n-1} g(j)^{q_j}}{\prod_{j=0}^{n-1} q_j^{q_j}}$$

That way we have obtained

$$\prod_{j=0}^{n-1} g(j)^{q_j} \leq 2^{-H(q_0, \dots, q_{n-1})},$$

so

$$\binom{k}{l} (g(0)^{q_0} g(1)^{q_1} \dots g(n-1)^{q_{n-1}})^t \leq \binom{k}{l} 2^{-H(h_1 X_1 + \dots + h_l X_l) t}$$

for $(a, h_1, \dots, h_l) \in T_{n,l}$.

The RHS is at most

$$\begin{cases} 2^{-n+1} \cdot 2^{-H_{n-1} \delta} & \text{for } l = n - 1, \\ O_n^{k \rightarrow \infty} (k^{l - (n-1)H(h_1 X_1 + \dots + h_l X_l) / H_{n-1}}) & \text{for } 1 \leq l \leq n - 2. \end{cases}$$

Summing over $T_{n,n-1}$:

$$\sum_{(a, h_1, \dots, h_{n-1}) \in T_{n,n-1}} \binom{k}{n-1} \prod_{(\epsilon_1, \dots, \epsilon_{n-1}) \in \{0,1\}^{n-1}} g(a + \epsilon_1 h_1 + \dots + \epsilon_{n-1} h_{n-1})^{t/2^{n-1}} \leq \underbrace{2^{-H_{n-1}\delta}}_{< 1}$$

Summing over $T_{n,l}$, $1 \leq l \leq n-2$:

$$\sum_{l=1}^{n-2} \sum_{(a, h_1, \dots, h_l) \in T_{n,l}} \binom{k}{l} \prod_{(\epsilon_1, \dots, \epsilon_l) \in \{0,1\}^l} g(a + \epsilon_1 h_1 + \dots + \epsilon_l h_l)^{t/2^l} = o_n^{k \rightarrow \infty}(1)$$

as soon as

$$l - (n-1) \frac{H(h_1 X_1 + \dots + h_l X_l)}{H_{n-1}} < 0$$

$$\iff \frac{H(h_1 X_1 + \dots + h_l X_l)}{l} > \frac{H_{n-1}}{n-1}$$

Lemma.

For $n \geq 2$, $1 \leq l \leq n-1$, $h_1, \dots, h_l \in \mathbb{Z} \setminus \{0\}$ s.t. $|h_1| + \dots + |h_l| \leq n-1$ we have

$$\frac{H(h_1 X_1 + \dots + h_l X_l)}{l} \geq \frac{H_{n-1}}{n-1},$$

with eq. attained only when $l = n-1$ and $|h_1| = \dots = |h_{n-1}| = 1$.

Sketch of the proof. From the precise bounds by Adell, Lekuona, and Yu (2010),

$$\frac{1}{2} \log_2 \frac{e\pi m}{2} - \frac{1}{4m} < H_m < \frac{1}{2} \log_2 \frac{e\pi m}{2} + \frac{1}{10m},$$

one easily gets

$$l < n-1 \implies \frac{H_l}{l} > \frac{H_{n-1}}{n-1},$$

so one can maximize the LHS with a fixed number of terms l .

Lemma.

For $m \in \mathbb{N}$, $h_1, \dots, h_m \in \mathbb{Z} \setminus \{0\}$ we have

$$H(h_1 X_1 + \dots + h_m X_m) \geq H_m,$$

with equality attained only when $|h_1| = \dots = |h_m|$.

Sketch of the proof. First reduce to the case when $h_1, \dots, h_m > 0$.

$X = h_1 X_1 + \dots + h_m X_m$, $Y \sim B(m, 1/2)$, $X \not\sim Y$

p_X, p_Y their probability mass functions

$p_X^\downarrow, p_Y^\downarrow$ their decreasing rearrangements

Karamata's inequality (1932) applies to the strictly concave function

$$\psi: [0, 1] \rightarrow \mathbb{R}, \quad x \mapsto \begin{cases} -x \log_2 x & \text{for } x > 0, \\ 0 & \text{for } x = 0 \end{cases}$$

and makes it is enough to see that p_Y^\downarrow majorizes p_X^\downarrow and $p_X^\downarrow \neq p_Y^\downarrow$.

Note that

$$\mathcal{A}_z := \left\{ A \subseteq \{1, 2, \dots, m\} : \sum_{j \in A} h_j = z \right\}$$

is an antichain for every $z \in \mathbb{Z}$.

By Erdős' generalization of Sperner's theorem (1945) or by the Yamamoto–Bollobás–Lubell–Meshalkin inequality (1954, ..., 1966) we have

$$\begin{aligned} & |\mathcal{A}_{z_1}| + |\mathcal{A}_{z_2}| + \dots + |\mathcal{A}_{z_N}| \\ & \leq \text{maximal size of } N \text{ disjoint antichains in } \mathcal{P}(\{1, 2, \dots, m\}) \\ & = \underbrace{\binom{m}{\lfloor m/2 \rfloor} + \binom{m}{\lfloor m/2 \rfloor + 1} + \binom{m}{\lfloor m/2 \rfloor - 1} + \binom{m}{\lfloor m/2 \rfloor + 2} + \dots}_N \end{aligned}$$

for $N = 1, 2, \dots$. Dividing by 2^m we get $p_X^\downarrow \preceq p_Y^\downarrow$.

Thank you for your attention!