

IMPROVED SUM–DIFFERENCE INEQUALITIES IN ABELIAN GROUPS

LOGAN J. KLEINWAKS

ABSTRACT. For all finite subsets X, Y of an abelian group, we prove

$$|X - Y| \leq |X + Y|^{\lambda_\infty}, \quad \lambda_\infty = \frac{9451e - 3286}{5378e + 787} = 1.454277448906\dots,$$

improving the classical exponent $3/2$. We also prove that a universal two-set exponent λ over the integers implies an upper bound $2 - 1/\lambda$ for the Gyarmati–Hennecart–Ruzsa constant, the supremum θ^* of t such that $|A - B| \gg |A + B|^t$ and $|A + B| \ll |A|$ for arbitrarily large $A, B \subset \mathbb{Z}$. Consequently,

$$\theta^* \leq \frac{13524e - 7359}{9451e - 3286} = 1.312373302115\dots,$$

improving their bound $4/3$. The first argument combines a coupling with distinct differences, entropy inequalities for independent sums, a finite certificate using non-Shannon inequalities, and an explicit limiting certificate with weights $\int_0^1 t(1-t)^k e^t dt$. The transfer uses localisation and the Plünnecke–Ruzsa inequality over a sequence of scales. The proofs are formalised in Lean 4.

1. FORMAL VERIFICATION AND USE OF AI

The mathematical results in Theorems 2.1–2.2, Corollary 2.3, and the lemmas and propositions used in their proofs have counterparts in the accompanying Lean 4 formalisation. Appendix A gives the correspondence and explains the representation of finite laws. The reference environment is `leanprover/lean4:v4.28.0`, with Mathlib revision `8f9d9cff6bd728b17a24e163c9402775d9e6a365`. The headline proofs use only `propext`, `Classical.choice` and `Quot.sound`. They use neither unproved auxiliary statements nor `native_decide`. See [9, 8] for Lean and Mathlib.

All mathematical formalisation was performed by Aristotle (Harmonic), which also simplified the formalisation under the author’s instructions. Research and proof derivation were performed using Aristotle, GPT-6 Astra, and GPT-5.6 Sol. The author wrote the research-loop instructions; additional research instructions were generated by GPT-6 Astra and GPT-5.6 Sol. Aristotle wrote the initial manuscript under the author’s instructions. The manuscript was revised by GPT-6 Astra under the author’s instructions and by the author. *The author contributed no deep problem-specific insight, the results were obtained through the author’s work on more general mathematical research loops.* The author is responsible for the final text and the claims made in it.

2. PROOF OUTLINE AND MAIN RESULTS

2.1. Proof outline. There are two independent arguments. The first transfers an inequality $|X - Y| \leq |X + Y|^\lambda$ to the small-sumset setting. For $|A + B| \leq K|A|$, write $s = |A + B|$, $d = |A - B|$ and $M_h = |hB - hB|$. A maximal packing by translates of $hB - hB$ decomposes A

Date: First version: September 28, 2026; Version 1.1: October 6, 2026.

2020 Mathematics Subject Classification. 11B30, 11B75, 94A17.

Key words and phrases. Sumsets, difference sets, Shannon entropy, non-Shannon inequalities, formal verification.

into pieces on which the pair inequality can be combined with a cardinality bound. Controlling the overlap of the corresponding sumsets gives

$$(2.1) \quad dM_h \leq sM_{4h}^{2-1/\lambda} \quad (h \geq 1).$$

Multiplying these estimates over $h = 1, 4, \dots, 4^{J-1}$ and using $M_{4^J} \leq K^{2 \cdot 4^J} |A|$ gives $d \leq C(K, J)s^{2-1/\lambda+1/J}$. Letting $J \rightarrow \infty$ bounds the admissible exponent by $2 - 1/\lambda$. This is Part I, in §3.

The second argument establishes the pair inequality. Choose $\Gamma \subset X \times Y$ with exactly one representative for each difference, and let (X_1, Y_1) be uniform on Γ . Then $X_1 - Y_1$ determines the pair and

$$L := H(X_1, Y_1) = \log |X - Y|.$$

For its marginal laws μ, ν , put $h(i, j) = H(\mu^{*i} * \nu^{*j})$ and $S = \log |X + Y|$. Entropy inequalities for independent sums make h nonnegative, nondecreasing, and concave in each coordinate. The representative property gives the additional links

$$L + h(i, j) \leq h(i+1, j) + h(i, j+1), \quad h(1, 1) \leq S.$$

These inequalities retain only the marginal laws. To exploit the dependence in (X_1, Y_1) , we introduce a second independent copy and apply Shannon inequalities and ten instances of the non-Shannon families of Matúš and Csirmaz–Csirmaz to integer linear forms in the four coordinates. Their exact weighted sum, followed by symmetrisation, gives

$$\begin{aligned} 22882L &\leq 5820S + 8694h(1, 1) \\ &\quad + 11645(h(1, 0) + h(0, 1)) + 685(h(2, 0) + h(0, 2)). \end{aligned}$$

The finite certificate is given in §5; the entropy setup and the two known non-Shannon families are in §4.

The remaining step is an inequality for real arrays satisfying these conditions. We prove it by an inductive certificate whose weights are

$$w_k = \int_0^1 t(1-t)^k e^t dt, \quad w_{k+2} = (k+4)w_{k+1} - (k+1)w_k.$$

This recurrence cancels the interior terms, while $w_k \rightarrow 0$ controls the remainder. Since $w_0 = 1$ and $w_1 = 3 - e$, the limiting coefficients are explicit:

$$(21512e + 3148)L \leq (37804e - 13144)S.$$

This yields $L \leq \lambda_\infty S$ and proves the pair inequality. The array argument is in §6, and the two parts are assembled in §7.

2.2. Main results. For finite subsets of an abelian group, write $A \pm B = \{a \pm b : a \in A, b \in B\}$, and let hB denote the h -fold sumset, with $0B = \{0\}$. We use the following precise formulation of the exponent in Gyarmati, Hennecart, and Ruzsa [3, (5)]. A real number t is *admissible* if $t > 1$ and for every $K > 1$ there is $c = c(K) > 0$ such that for every $n_0 \in \mathbb{N}$ there exist finite $A, B \subset \mathbb{Z}$ with $B \neq \emptyset$, $|A| \geq n_0$ and

$$(2.2) \quad |A + B| \leq K|A|, \quad |A - B| \geq c|A + B|^t.$$

Let θ^* be the supremum of the admissible exponents, with the convention $\sup \emptyset = 0$. This is the Gyarmati–Hennecart–Ruzsa exponent, denoted C_{3a} in the Optimization Constants in Mathematics GitHub repository.

Define the unrestricted integer pair exponent by

$$(2.3) \quad \lambda_* = \inf \{ \lambda \in \mathbb{R} : |X - Y| \leq |X + Y|^\lambda \text{ for all finite } X, Y \subset \mathbb{Z} \}.$$

The set of exponents in (2.3) contains 2, and each of its elements is at least 1. The classical inequality recorded in [3, §1] gives $\lambda_* \leq 3/2$.

Theorem 2.1 (two-set inequality). *For every abelian group G and finite $X, Y \subset G$,*

$$|X - Y| \leq |X + Y|^{\lambda_\infty}, \quad \lambda_\infty = \frac{9451e - 3286}{5378e + 787} = 1.454277448906 \dots$$

Theorem 2.2 (transfer). *If $|X - Y| \leq |X + Y|^\lambda$ for every finite $X, Y \subset \mathbb{Z}$, then $\theta^* \leq 2 - 1/\lambda$. Consequently, $\theta^* \leq 2 - 1/\lambda_*$.*

Corollary 2.3.

$$\theta^* \leq 2 - \frac{1}{\lambda_\infty} = \frac{13524e - 7359}{9451e - 3286} = 1.312373302115 \dots$$

Theorem 2.1 has no multiplicative constant and imposes no torsion or cardinality restriction on G . Replacing Y by $-Y$ also gives $|X + Y| \leq |X - Y|^{\lambda_\infty}$. Theorem 2.2 with $\lambda = 3/2$ recovers $\theta^* \leq 4/3$.

2.3. Prior work and the contribution of the proof. Gyarmati, Hennecart, and Ruzsa [3, Corollary 3] proved $|A - B| \leq K^{2/3}|A + B|^{4/3}$ under $|A + B| \leq K|A|$. Their result gives the previous upper bound $4/3$ for θ^* . The unrestricted two-set problem must be distinguished from the single-set inequality $|X - X| \leq |X + X|^{4/3}$ of Freiman and Pigarev, recalled in [3, §1]. The simplex construction of Hennecart, Robert, and Yudin [4] yields $\lambda_* \geq \log(1 + \sqrt{2})/\log 2$; see also [3, §2].

The transfer uses Ruzsa's maximal-packing argument [11] and the Plünnecke–Ruzsa inequality, for which we use the form in [10, Theorem 1.2]. The entropy approach belongs to the theory developed by Ruzsa [12], Tao [13], and Madiman, Marcus, and Tetali [5, 6]. In particular, the submodularity inequality for independent sums is due to Madiman [5]; its discrete abelian-group form also appears in [6, Corollary 2.6].

The non-Shannon inequalities used here are existing inequalities of Matúš [7] and Csirmaz–Csirmaz [1]. Both are reproduced explicitly in [1, Theorem 22 and (31)]. Their proofs use the conditional-copy construction originating in Zhang–Yeung [14] and developed systematically by Dougherty, Freiling, and Zeger [2]. The contributions here are the multiscale transfer, the specific two-copy entropy certificate, and its combination with the limiting array certificate. No new general information inequality is asserted.

3. PART I: THE TRANSFER

All sets in this section are finite subsets of an abelian group, except where the group is explicitly specialised to $\mathbb{Z}$.

Lemma 3.1 (reduction to $K = 2$). *Let $C > 0$ and $r \in \mathbb{R}$. Suppose that $|A - B| \leq C|A + B|^r$ for all nonempty $A, B \subset \mathbb{Z}$ with $|A + B| \leq 2|A|$. Then every admissible θ satisfies $\theta \leq r$.*

Proof. Apply (2.2) with $K = 2$. It gives $c > 0$ and pairs with $|A + B| \geq |A| \geq n_0$ and $c|A + B|^\theta \leq |A - B| \leq C|A + B|^r$. If $\theta > r$, this fails once $|A + B|^{\theta-r} > C/c$. $\square$

Taking $K = 2$ suffices to bound the admissible exponents. The estimates below retain K until this final application.

Lemma 3.2 (packing). *Let D be finite and nonempty. There is $T \subset A$ such that the translates $t + D$ ($t \in T$) are pairwise disjoint and every $a \in A$ satisfies $a - t \in D - D$ for some $t \in T$.*

Proof. Take $T \subset A$ of maximal cardinality with disjoint translates. If $a \in A \setminus T$ had $a - t \notin D - D$ for all $t \in T$, then $a + D$ would be disjoint from every $t + D$, contradicting maximality; elements of T are covered by $t = a$. $\square$

Lemma 3.3 (localisation). *Let D be finite and nonempty and $\lambda \geq 1$. Suppose that $|X - B| \leq |X + B|^\lambda$ for every $X \subset A$ contained in a translate of $D - D$. Then*

$$|A - B| |D| \leq |D - D - B|^{1-1/\lambda} |A + B| |D - D + D - B|.$$

Proof. Let T be as in Lemma 3.2 and assign each $a \in A$ to one $t \in T$ with $a - t \in D - D$; let A_t be the set of elements assigned to t . Then $A - B = \bigcup_t (A_t - B)$. Since $A_t - B \subset t + (D - D - B)$ we have $|A_t - B| \leq U := |D - D - B|$, and by hypothesis $|A_t - B| \leq |A_t + B|^\lambda$. For $x > 0$, $x \leq U$ and $x \leq v^\lambda$ imply $x = x^{1-1/\lambda} x^{1/\lambda} \leq U^{1-1/\lambda} v$; the same bound is immediate for $x = 0$, so

$$|A - B| \leq \sum_{t \in T} |A_t - B| \leq U^{1-1/\lambda} \sum_{t \in T} |A_t + B|.$$

Let $w \in A + B$, and let T_w be the set of t with $w \in A_t + B$. If $w = a + b$ with $a \in A_t$ and $a - t = y - z$ ($y, z \in D$), then $t + D = w + (z - y + D - b) \subset w + (D - D + D - B)$. The translates $t + D$, $t \in T_w$, are disjoint, so $|T_w| |D| \leq |D - D + D - B|$. Summing over $w \in A + B$ gives $|D| \sum_t |A_t + B| \leq |A + B| |D - D + D - B|$. $\square$

Lemma 3.4 (one scale). *Let $B \neq \emptyset$ and $\lambda \geq 1$, and suppose that $|X - B| \leq |X + B|^\lambda$ for every $X \subset A$. Write $M_h = |hB - hB|$. Then for every $h \geq 1$,*

$$|A - B| M_h \leq M_{4h}^{2-1/\lambda} |A + B|.$$

Proof. Apply Lemma 3.3 with $D = hB - hB$. Then $D - D - B = 2hB - (2h + 1)B$ and $D - D + D - B = 3hB - (3h + 1)B$. Since $B \neq \emptyset$, $|mB - nB|$ is nondecreasing in m and n , so both sets have at most M_{4h} elements. $\square$

Proposition 3.5 (multi-scale inequality). *Let A, B be nonempty with $|A + B| \leq K|A|$, let $\lambda \geq 1$, and suppose that $|X - B| \leq |X + B|^\lambda$ for every $X \subset A$. Then for every $J \in \mathbb{N}$*

$$|A - B|^J \leq |A + B|^J (K^{2 \cdot 4^J} |A|)^{1+J(1-1/\lambda)}.$$

Proof. Put $d = |A - B|$, $s = |A + B|$ and $m_j = M_{4^j}$. We show by induction on j that $d^j m_0 \leq s^j m_j^{1+j(1-1/\lambda)}$. The case $j = 0$ is equality. For the step, Lemma 3.4 with $h = 4^j$ gives $d m_j \leq m_{j+1}^{2-1/\lambda} s$, and $m_j \leq m_{j+1}$ gives $m_j^{j(1-1/\lambda)} \leq m_{j+1}^{j(1-1/\lambda)}$; multiplying,

$$d^{j+1} m_0 \leq s^j (d m_j) m_j^{j(1-1/\lambda)} \leq s^{j+1} m_{j+1}^{1+(j+1)(1-1/\lambda)}.$$

Finally $m_0 = |B - B| \geq 1$, and the Plünnecke–Ruzsa inequality $|mB - nB| \leq (|A + B|/|A|)^{m+n} |A|$ [10, Theorem 1.2] gives $m_J \leq K^{2 \cdot 4^J} |A|$. $\square$

Proof of Theorem 2.2. Suppose $|X - Y| \leq |X + Y|^\lambda$ for all finite $X, Y \subset \mathbb{Z}$. Then $\lambda \geq 1$ (take $X = \{0\}$, $Y = \{0, 1\}$). Let $J \geq 1$ and let $A, B \subset \mathbb{Z}$ be nonempty with $|A + B| \leq 2|A|$. Proposition 3.5 with $K = 2$, together with $|A| \leq |A + B| = s$, gives after taking J -th roots

$$|A - B| \leq s (2^{2 \cdot 4^J} s)^{(1+J(1-1/\lambda))/J} = C_J s^{2-1/\lambda+1/J}.$$

By Lemma 3.1 every admissible θ satisfies $\theta \leq 2 - 1/\lambda + 1/J$ for all $J \geq 1$, hence $\theta \leq 2 - 1/\lambda$, and $\theta^* \leq 2 - 1/\lambda$ (this is also true when there is no admissible exponent, since $2 - 1/\lambda \geq 1 > 0$).

For the second statement, apply the first to $\lambda = 2$ to get $\theta^* \leq 3/2$. If $\theta^* > 2 - 1/\lambda_*$, then $\lambda_* < 1/(2 - \theta^*)$, so some λ in the set (2.3) satisfies $\lambda < 1/(2 - \theta^*)$, that is $2 - 1/\lambda < \theta^*$, contradicting the first statement. $\square$

Remark 3.6. At a single scale the ratio M_{4h}/M_h implicit in (2.1) need not be bounded in terms of K . Over the scales 4^j the product of these ratios telescopes to at most $K^{2 \cdot 4^J} |A|$, and the J -th root turns this loss into a constant times $s^{1/J}$.

4. ENTROPY: THE COUPLING, THE GRID, AND NON-SHANNON INEQUALITIES

4.1. Notation. All random variables are finitely supported and defined on a common finite probability space; H denotes Shannon entropy with natural logarithms, and $H(U_1, \dots, U_r)$ the joint entropy. For finitely supported probability measures α, β on an abelian group G , $\alpha * \beta$ is the law of $U + V$ with $U \sim \alpha$, $V \sim \beta$ independent, and $H(\alpha)$ is the entropy of α . We use the following facts.

(E1) If U takes values in a finite set S , then $H(U) \leq \log |S|$.

(E2) $H(U) = H(V)$ if U and V are functions of each other; $H(f(U)) \leq H(U)$; $H(U, V) = H(U) + H(V)$ if U, V are independent.

(E3) Submodularity: $H(U, W) + H(V, W) \geq H(U, V, W) + H(W)$.

(E4) For independent U, V : $H(U) \leq H(U + V)$.

(E5) (Madiman [5]) For independent U, V, W : $H(U + V + W) + H(V) \leq H(U + V) + H(V + W)$.

(E4) follows from $H(U) + H(V) = H(U + V, V) \leq H(U + V) + H(V)$. For (E5), apply (E3) to the joint variables $(U, V + W)$ and $(U + V, W)$, both of which determine $U + V + W$ and which together determine (U, V, W) : this gives $H(U, V, W) + H(U + V + W) \leq H(U, V + W) + H(U + V, W)$, and independence turns it into (E5).

4.2. The coupling and the grid.

Lemma 4.1 (coupling). *For finite $X, Y \subset G$ there is $\Gamma \subset X \times Y$ with $|\Gamma| = |X - Y|$ such that distinct elements of Γ have distinct differences $x - y$.*

Proof. Choose one representative pair for each $z \in X - Y$. □

Fix such a Γ , assume $X, Y \neq \emptyset$, and let (X_1, Y_1) be uniform on Γ . Let μ, ν be the laws of X_1 and Y_1 , and put

$$L = \log |\Gamma| = \log |X - Y|, \quad S = \log |X + Y|, \quad h(i, j) = H(\mu^{*i} * \nu^{*j}) \quad (i, j \in \mathbb{N}).$$

Lemma 4.2 (coupled Ruzsa triangle inequality). *For every finitely supported law ω on G , $L + H(\omega) \leq H(\mu * \omega) + H(\nu * \omega)$. In particular*

$$L + h(i, j) \leq h(i + 1, j) + h(i, j + 1) \quad (i, j \in \mathbb{N}).$$

Proof. Let $W \sim \omega$ be independent of (X_1, Y_1) . Since $(X_1 + W) - (Y_1 + W) = X_1 - Y_1$ determines (X_1, Y_1) , the map $(X_1, Y_1, W) \mapsto (X_1 + W, Y_1 + W)$ is injective on the support. Hence $L + H(W) = H(X_1, Y_1, W) = H(X_1 + W, Y_1 + W) \leq H(X_1 + W) + H(Y_1 + W)$. Take $\omega = \mu^{*i} * \nu^{*j}$. □

This is the entropy analogue of Ruzsa's inequality $|X - Y||W| \leq |X + W||Y + W|$ for the specific coupling Γ .

Lemma 4.3 (grid concavity). *For all $i, j \in \mathbb{N}$:*

$$\begin{aligned} h(i + 2, j) + h(i, j) &\leq 2h(i + 1, j), & h(i, j + 2) + h(i, j) &\leq 2h(i, j + 1), \\ h(i, j) &\leq h(i + 1, j), & h(i, j) &\leq h(i, j + 1), & h(i, j) &\geq 0, & h(1, 1) &\leq S. \end{aligned}$$

Proof. Concavity is (E5) with U, W two independent copies of μ (respectively ν) and $V \sim \mu^{*i} * \nu^{*j}$: $H(\alpha * \alpha * \beta) + H(\beta) \leq 2H(\alpha * \beta)$. Monotonicity is (E4). Finally $\mu^{*1} * \nu^{*1}$ is supported on $X + Y$, so $h(1, 1) \leq S$ by (E1). □

Only unit steps of (E5) are needed: Lemma 4.3 is the only information about h used, besides Lemma 4.2 and Corollary 5.3.

4.3. Two copies and linear forms. Let (X_2, Y_2) be an independent copy of (X_1, Y_1) , and write $\mathbf{V} = (X_1, Y_1, X_2, Y_2)$. For $c \in \mathbb{Z}^4$ write $c \cdot \mathbf{V} = c_1 X_1 + c_2 Y_1 + c_3 X_2 + c_4 Y_2$, and for a finite list F of vectors in $\mathbb{Z}^4$ put $\mathbf{H}[F] = H((c \cdot \mathbf{V})_{c \in F})$. We denote the forms by their values (so $\mathbf{H}[X_1 + Y_2, Y_1 - Y_2]$ is the joint entropy of these two forms), and a parenthesised list of forms is regarded as one joint variable. The following rules hold.

- (R1) ($\mathbb{Z}$ -span.) If every form of F' is an integer combination of forms of F and conversely, then $\mathbf{H}[F] = \mathbf{H}[F']$.
- (R2) (Coupling.) If $X_k - Y_k$ is an integer combination of forms of F ($k = 1$ or 2), then $\mathbf{H}[F] = \mathbf{H}[F, X_k, Y_k]$, since $x - y$ determines (x, y) on Γ .
- (R3) (Exchange.) $\mathbf{H}[F]$ is unchanged if (X_1, Y_1) and (X_2, Y_2) are exchanged in all forms.
- (R4) (Independence.) If the forms of F_1 involve only X_1, Y_1 and those of F_2 only X_2, Y_2 , then $\mathbf{H}[F_1, F_2] = \mathbf{H}[F_1] + \mathbf{H}[F_2]$.
- (R5) $\mathbf{H}[X_k, Y_k] = L$ for $k = 1, 2$, and $\mathbf{H}[\emptyset] = 0$.
- (R6) (Bridge.) A single form with coefficients in $\{0, 1\}$, involving at most one variable from each copy, has entropy $h(i, j)$, where i (resp. j) is the number of X 's (resp. Y 's): e.g. $\mathbf{H}[X_1] = h(1, 0)$, $\mathbf{H}[X_1 + X_2] = h(2, 0)$, $\mathbf{H}[X_1 + Y_2] = \mathbf{H}[Y_1 + X_2] = h(1, 1)$, $\mathbf{H}[Y_1 + Y_2] = h(0, 2)$.
- (R7) (Support.) $\mathbf{H}[X_1 + Y_1] \leq S$, since $X_1 + Y_1 \in X + Y$.

Rules (R1)–(R2) are applications of (E2), (R3) holds because the two copies are independent and identically distributed, and (R4) is the independence of the copies. The identifications used to rewrite lists of forms are certified by (R1)–(R3); independence and the identifications with L and h use (R4)–(R6). Integer coefficients are essential: division by an integer would not be valid in an arbitrary abelian group. The formalisation searches for integer witnesses to mutual determination and verifies each witness (Appendix A); it does not assume completeness of that search. The inequality (R7) is the only inequality that relates the dependent sum $X_1 + Y_1$ to $|X + Y|$; the grid only sees sums of independent variables.

4.4. Non-Shannon inequalities. For jointly distributed a, b, c write $(a, b \| c) = H(a, c) + H(b, c) - H(a, b, c) - H(c)$ and $(a, b) = (a, b \| \emptyset)$, and let

$$[abcd] = -(a, b) + (a, b \| c) + (a, b \| d) + (c, d)$$

be the Ingleton expression, with the convention of [1, §2]. For five jointly distributed variables a, b, c, d, z and $k \in \mathbb{N}$ put

$$\mathbf{M}_k[abcd] = (b, z \| a) + k([abcd] + (a, z \| b) + (a, b \| z)) + \binom{k}{2}((a, c \| b) + (a, b \| c)),$$

$$\mathbf{C}_k[abcd] = (a, b \| z) + k([abcd] + (a, z \| b) + (b, z \| a)) + \binom{k}{2}((a, c \| b) + (b, c \| a)),$$

and let $\mathbf{M}_k[acbd]$, $\mathbf{C}_k[acbd]$ be the same expressions with $[abcd]$ replaced by $[acbd]$ (and no other change).

Theorem 4.4 (Matúš [7]; see [1, Theorem 22]). $\mathbf{M}_k[abcd] \geq 0$ and $\mathbf{M}_k[acbd] \geq 0$ for all $k \in \mathbb{N}$.

Theorem 4.5 (Csirmaz–Csirmaz [1, (31)]). $\mathbf{C}_k[abcd] \geq 0$ and $\mathbf{C}_k[acbd] \geq 0$ for all $k \in \mathbb{N}$.

For $k = 1$ and $z = d$, $\mathbf{M}_1[abcd]$ is a permutation of the Zhang–Yeung inequality [14] (see Remark 5.2). Both theorems are re-proved in the formalisation, by induction on k from one common lemma.

Lemma 4.6 (copy lemma [14, 2]). *For a, b, c, d, z there are a', b', c', d', z' on a finite probability space such that (a', b', c', d') has the law of (a, b, c, d) , (a', b', z') has the law of (a, b, z) , and $((c', d'), z' \| (a', b')) = 0$.*

Proof. Retain the marginal law of (a, b, c, d) and, conditionally on (a, b) , sample z' independently of (c, d) with the conditional law of z given (a, b) . Equivalently, on pairs of original sample points with the same (a, b) -value, use the weight $p(\omega)p(\omega')/p_{a,b}(a, b)$. Fibres of zero mass contribute zero. This preserves the two stated marginals and gives the required conditional independence. $\square$

The formal proof of M_{k+1} applies the case k , with the other Ingleton variant, to (a', c', b', d', z') and adds finitely many Shannon inequalities and the conditional independence [1, proof of Theorem 22]. For C_{k+1} it applies the case k to the joint variables $((a', z'), (b', z'), (c', z'), (d', z'), (c', z'))$, following the second proof of Theorem 16 and the subsequent remark in [1].

5. THE TWO-COPY INEQUALITY

Proposition 5.1 (two-copy inequality). *In the setting of §4,*

$$194497 L \leq 49470 S + 73899 h(1, 1) + 99532 h(1, 0) + 98433 h(0, 1) + 4986 h(2, 0) + 6659 h(0, 2).$$

Proof. The inequality is the sum, with the positive integer weights listed, of the 27 Shannon inequalities and the support inequality of Table 1 and of the ten non-Shannon inequalities of Table 2, after every entropy has been rewritten with (R1)–(R6). Each Shannon row is an instance of (E3), written as a conditional mutual information of joint variables; each row of Table 2 is an instance of Theorem 4.4 or 4.5 in which each of a, b, c, d, z is a single form or a pair of forms, so that each of the joint entropies of the five-variable expression is an $\mathbf{H}[F]$. After rewriting, 49 distinct joint entropies $\mathbf{H}[F]$ occur besides L, S and the $h(i, j)$. Their coefficients cancel, apart from those that (R4)–(R6) turn into multiples of L and of $h(1, 0), h(0, 1), h(2, 0), h(0, 2), h(1, 1)$. The sum is exactly the stated inequality. $\square$

The cancellation is an exact calculation over the integers. The formal proof supplies each row separately and ends with their explicit weighted sum. Tables 1 and 2 give all the inequality rows; the remaining operations are the entropy identities (R1)–(R6). Thus the certificate can be checked without reproducing the search that found its coefficients.

Remark 5.2 (structure of the certificate). In six of the ten rows z coincides with d (cut144) or with c (cut145, cut147, cut148, cut150, cut153), so these are four-variable inequalities. Writing $M_s^{(4)}(a, b, c, d) = (b, c \parallel a) + s[abcd] + \binom{s+1}{2}((a, c \parallel b) + (a, b \parallel c))$ for Matúš's four-variable family [7], whose case $s = 1$ is the Zhang–Yeung inequality [14], a direct expansion gives $M_1[abcd]|_{z=d} = M_1^{(4)}(a, b, d, c)$, $C_s[acbd]|_{z=c} = M_s^{(4)}(c, a, b, d)$ for $s = 2, 3$, and $M_3[abcd]|_{z=c} = M_3^{(4)}(a, b, c, d)$. Each of the four arguments of cut144 determines $X_1 + Y_1$. Only cut146, cut149, cut151 and cut152 involve five distinct variables. The coefficients were obtained by a finite linear-programming search. Their validity here is established by the displayed certificate and does not depend on optimality of that search.

Corollary 5.3 (symmetric two-copy inequality).

$$22882 L \leq 5820 S + 8694 h(1, 1) + 11645 (h(1, 0) + h(0, 1)) + 685 (h(2, 0) + h(0, 2)).$$

Proof. The set $\Gamma' = \{(-y, -x) : (x, y) \in \Gamma\} \subset (-Y) \times (-X)$ again has distinct differences, $|\Gamma'| = |\Gamma|$ and $|(-Y) + (-X)| = |X + Y|$. Its marginals are the reflections of ν and μ , and reflection preserves entropy, so the array attached to Γ' is $h'(i, j) = h(j, i)$. Proposition 5.1 for Γ' is Proposition 5.1 for Γ with $h(i, j)$ replaced by $h(j, i)$. Adding the two inequalities and dividing by 17 gives the claim. $\square$

TABLE 1. Shannon rows and the support row of Proposition 5.1. Each entry $I(A; C \mid B) = H(A, B) + H(B, C) - H(A, B, C) - H(B) \geq 0$ is an instance of (E3); an empty condition means $B = \emptyset$. Row names are those of the formal proof.

row	inequality	weight
s116	$I(Y_2; Y_1 + X_2)$	21105
s117	$I(Y_2; X_1 - X_2)$	9814
s118	$I(Y_2; X_1)$	17442
s119	$I(Y_2; X_1 + X_2)$	4986
s120	$I(Y_2; X_1 + Y_1)$	26370
s121	$I((X_2, Y_2); X_1 - Y_1 - X_2)$	16965
s122	$I((X_2, Y_2); X_1 - Y_1 + Y_2)$	12564
s123	$I((X_2, Y_2); X_1)$	11708
s124	$I((X_2, Y_2); (X_1, Y_1, Y_2) \mid Y_2)$	1304
s125	$I((X_2, Y_2); (X_1 + Y_1, X_2) \mid X_2)$	4896
s126	$I(X_2; Y_1 - Y_2)$	7764
s127	$I(X_2; Y_1 + Y_2)$	6659
s128	$I(X_2; X_1 + Y_2)$	16839
s129	$I(X_2; X_1 + Y_1)$	23100
s130	$I(Y_1 - Y_2; (X_1, X_2))$	2376
s131	$I(Y_1 + X_2; X_1 + X_2 + Y_2)$	18522
s132	$I(Y_1 + X_2; X_1 + Y_1 + Y_2)$	26001
s133	$I(X_1 - X_2; (Y_1, Y_2))$	4016
s134	$I((Y_1, Y_2); (X_1 + X_2 + Y_2, Y_1 - Y_2) \mid Y_1 - Y_2)$	3564
s135	$I((Y_1 + X_2, Y_2); (X_1 + X_2, Y_1 + X_2 - Y_2) \mid Y_1 + X_2 - Y_2)$	2277
s136	$I((Y_1 + X_2, Y_2); (X_1, Y_1 + X_2 + Y_2) \mid Y_1 + X_2 + Y_2)$	2520
s137	$I((X_1, Y_1, Y_2); (X_1, Y_1 + Y_2, X_2) \mid (X_1, Y_1 + Y_2))$	748
s138	$I((X_1 + Y_1 + X_2, Y_2); (X_1, Y_1 + X_2) \mid X_1 + Y_1 + X_2)$	2376
s139	$I((X_1, X_2); (X_1 - X_2, Y_1 + X_2 + Y_2) \mid X_1 - X_2)$	6024
s140	$I((X_1 + Y_2, X_2); (X_1 - X_2 + Y_2, Y_1 + Y_2) \mid X_1 - X_2 + Y_2)$	4149
s141	$I((Y_1 - Y_2, X_2 + Y_2); (X_1 + Y_2, Y_1 - Y_2) \mid Y_1 - Y_2)$	6576
s142	$I((X_1 + Y_2, X_2 + Y_2); (X_1 - X_2, Y_1 + X_2) \mid X_1 - X_2)$	7806
r143	$S - H(X_1 + Y_1) \geq 0 \quad (\text{R7})$	49470

6. THE GRID LEMMA

Proposition 6.1 (grid lemma). *Let $h : \mathbb{N}^2 \rightarrow \mathbb{R}$ and $L, S \in \mathbb{R}$ satisfy, for all $i, j \in \mathbb{N}$,*

- (G1) $h(i + 2, j) + h(i, j) \leq 2h(i + 1, j)$ and $h(i, j + 2) + h(i, j) \leq 2h(i, j + 1)$;
- (G2) $h(i, j) \leq h(i + 1, j)$, $h(i, j) \leq h(i, j + 1)$, and $h(i, j) \geq 0$;
- (G3) $L + h(i, j) \leq h(i + 1, j) + h(i, j + 1)$;
- (G4) $h(1, 1) \leq S$;
- (G5) $22882L \leq 5820S + 8694h(1, 1) + 11645(h(1, 0) + h(0, 1)) + 685(h(2, 0) + h(0, 2))$.

Then $(21512e + 3148)L \leq (37804e - 13144)S$.

The proof occupies the rest of this section.

6.1. Symmetrisation. The array $g(i, j) = \frac{1}{2}(h(i, j) + h(j, i))$ is symmetric and satisfies (G1)–(G4). Concavity of g in i uses concavity of h in both variables, and the link of g at $(0, j)$ is the average of the links of h at $(0, j)$ and $(j, 0)$. Condition (G5) becomes

$$(6.1) \quad 22882L \leq 5820S + 8694g(1, 1) + 23290g(0, 1) + 1370g(0, 2).$$

TABLE 2. The ten non-Shannon rows of Proposition 5.1: instances of Theorem 4.4 (M_k) and Theorem 4.5 (C_k), with the arguments (a, b, c, d, z) .

row	instance	weight
cut144	$M_1[abcd]: a = (X_1 + Y_2, Y_1 - Y_2), b = (X_1 - X_2, Y_1 + X_2),$ $c = (X_1 - X_2 + Y_2, Y_1 + X_2 - Y_2), d = z = (X_1, Y_1)$	4794
cut145	$C_2[acbd]: a = (X_1, Y_1 - Y_2), b = (X_1 + Y_2, Y_1 - Y_2),$ $c = z = (X_1 + X_2 + Y_2, Y_1 - Y_2), d = X_1 + Y_1 + X_2 - Y_2$	1188
cut146	$M_3[abcd]: a = X_2, b = X_1 + Y_1 + X_2, c = Y_1 + X_2, d = X_1 + X_2,$ $z = Y_1 + X_2 - Y_2$	1146
cut147	$C_2[acbd]: a = (X_1 - X_2, Y_1), b = (X_1 - X_2, Y_1 + X_2),$ $c = z = (X_1 - X_2, Y_1 + X_2 + Y_2), d = X_1 + Y_1 - X_2 + Y_2$	2008
cut148	$C_3[acbd]: a = X_1 + Y_1 + X_2, b = Y_1 + X_2 - Y_2, c = z = X_2, d = X_1 + X_2$	516
cut149	$M_3[abcd]: a = Y_1, b = Y_1 + X_2 + Y_2, c = Y_1 + X_2, d = Y_1 + Y_2,$ $z = X_1 - Y_1 - X_2$	1506
cut150	$M_3[abcd]: a = Y_2, b = X_1 + Y_1 + Y_2, c = z = X_1 - X_2 + Y_2, d = Y_1 + Y_2$	963
cut151	$M_3[acbd]: a = X_1, b = X_1 - Y_1 + Y_2, c = (X_1 + X_2 + Y_2, Y_1),$ $d = X_1 + X_2, z = X_1 + X_2 + Y_2$	396
cut152	$M_3[acbd]: a = Y_1, b = X_1 - Y_1 - X_2, c = (X_1, Y_1 + X_2 + Y_2), d = Y_1 + Y_2,$ $z = Y_1 + X_2 + Y_2$	420
cut153	$M_3[abcd]: a = Y_1 + X_2, b = X_1 - Y_1 + Y_2, c = z = Y_1, d = Y_1 + X_2 - Y_2$	153

From now on we use only: g is symmetric; $i \mapsto g(i, j)$ is concave and nondecreasing for each j ; $g \geq 0$; the links $\ell_j := g(1, j) + g(0, j + 1) - g(0, j) - L \geq 0$; $g(1, 1) \leq S$; and (6.1).

6.2. The weights. For $m, k \in \mathbb{N}$ let $B(m, k) = \int_0^1 t^m (1 - t)^k e^t dt \geq 0$ and $w_k = B(1, k)$.

Lemma 6.2. $w_0 = 1$, $w_1 = 3 - e$, and for all $k \in \mathbb{N}$:

- (i) $w_{k+2} = (k + 4)w_{k+1} - (k + 1)w_k$;
- (ii) $0 \leq w_{k+1} \leq w_k$ and $2w_{k+1} \leq w_k + w_{k+2}$;
- (iii) $w_k \leq 1/(k + 1)$;
- (iv) $(k + 1)w_{k+1} \leq (k + 3)w_{k+2}$.

Proof. Integration by parts gives $B(0, k + 1) = (k + 1)B(0, k) - 1$, $B(0, 0) = e - 1$, $B(1, 0) = 1$, and $B(m, k) = B(m, k + 1) + B(m + 1, k)$ gives $w_k = 1 - kB(0, k)$. These imply $w_1 = 3 - e$ and (i). Next $w_k - w_{k+1} = B(2, k) \geq 0$ and $w_k - 2w_{k+1} + w_{k+2} = B(3, k) \geq 0$. From $B(0, k + 1) \geq 0$ we get $(k + 1)B(0, k) \geq 1$, hence (iii). Finally (iv) is the convexity in (ii) at $k + 1$ combined with (i). $\square$

The integral representation supplies both the recurrence needed for cancellation and the decay needed to pass to the limit. In particular, $w_1 = 3 - e$ accounts for the occurrence of e in the final exponent.

6.3. Row inequalities. For $f : \mathbb{N} \rightarrow \mathbb{R}$ let $\tau_m(f) = mf(1) - (m - 1)f(0) - f(m)$, the defect at m of the chord through $(0, f(0))$ and $(1, f(1))$.

Lemma 6.3. Let f be concave, i.e. $f(k + 2) + f(k) \leq 2f(k + 1)$. Then for all $m \in \mathbb{N}$: $\tau_m(f) \geq 0$, $(m + 1)\tau_{m+1}(f) \leq m\tau_{m+2}(f)$, and

$$w_{m+1}\tau_{m+2}(f) \leq w_{m+2}\tau_{m+4}(f).$$

Proof. With $\delta_k = f(k + 1) - f(k)$ nonincreasing, $\tau_{m+1} = \sum_{k=1}^m (\delta_0 - \delta_k)$ is a sum of m nonnegative, nondecreasing terms. Hence $\tau_{m+1} \geq 0$, and averages over longer initial segments are larger. For

$m \geq 1$ this gives $\tau_{m+1}/m \leq \tau_{m+2}/(m+1)$; the case $m = 0$ follows from $\tau_1 = 0$. Applying this twice gives $(m+3)\tau_{m+2} \leq (m+1)\tau_{m+4}$. Multiplying by Lemma 6.2(iv), $(m+1)w_{m+1} \leq (m+3)w_{m+2}$, gives the last claim. $\square$

6.4. The certificate. Put

$$\kappa = \frac{e-1}{24660}, \quad N = 1 + 21512\kappa, \quad \Lambda = e + 13144\kappa,$$

so that $24660N = 21512e + 3148$ and $24660\Lambda = 37804e - 13144$.

Lemma 6.4. *For every $m \in \mathbb{N}$,*

$$(6.2) \quad (N - w_{m+2})L \leq \Lambda S + (w_{m+1} - w_{m+2})g(0, m+3) - w_{m+1}g(m+2, m+3).$$

Proof. Write $\tau_m^{(j)} = \tau_m(g(\cdot, j))$. For $m = 0$ (where $w_1 = 3 - e$ and $w_2 = 11 - 4e$) the difference of the two sides of (6.2) equals

$$(e - 2 - 1370\kappa)\ell_1 + (3e - 8)\ell_2 + w_0\tau_2^{(1)} + w_1\tau_3^{(2)} + (e + 7324\kappa)(S - g(1, 1)) \\ + \kappa(5820S + 8694g(1, 1) + 23290g(0, 1) + 1370g(0, 2) - 22882L),$$

using $g(2, 1) = g(1, 2)$ and $g(3, 2) = g(2, 3)$ in $\tau_2^{(1)} = 2g(1, 1) - g(0, 1) - g(2, 1)$ and $\tau_3^{(2)} = 3g(1, 2) - 2g(0, 2) - g(3, 2)$. All coefficients are positive: for example, $2.7 < e < 2.8$ gives $0 < \kappa < 10^{-4}$ and $e - 2 - 1370\kappa > 0$, and each bracket is nonnegative by the links, Lemma 6.3, $g(1, 1) \leq S$ and (6.1).

For the step from m to $m+1$, add to (6.2) the link $\ell_{m+3} \geq 0$ with weight $w_{m+2} - w_{m+3} \geq 0$ and the row inequality $w_{m+2}\tau_{m+4}^{(m+3)} - w_{m+1}\tau_{m+2}^{(m+3)} \geq 0$ of Lemma 6.3. By the recurrence $w_{m+3} = (m+5)w_{m+2} - (m+2)w_{m+1}$ and the symmetry $g(m+4, m+3) = g(m+3, m+4)$, the terms in $g(1, m+3)$ and $g(0, m+3)$ cancel and the result is (6.2) for $m+1$. $\square$

The choice of κ is forced: it is the unique value for which the coefficient of $g(0, 1)$ in the base combination vanishes. The row inequalities with weights w_{j-2}, w_{j-1} and the links with weights $w_{j-1} - w_j$, $j \geq 3$, form the dual certificate; for every finite truncation the remainder is the last two terms of (6.2).

Proof of Proposition 6.1. By monotonicity $g(m+2, m+3) \geq g(0, m+3) \geq 0$, and $w_{m+1} \geq w_{m+2} \geq 0$, so the last two terms of (6.2) add up to at most $-w_{m+2}g(0, m+3) \leq 0$. Hence $(N - w_{m+2})L \leq \Lambda S$ for all m . If $L \leq 0$ the claim follows from $\Lambda S \geq \Lambda g(1, 1) \geq 0$. If $L > 0$, let $m \rightarrow \infty$ and use $w_{m+2} \leq 1/(m+3)$: this gives $NL \leq \Lambda S$, and multiplying by 24660 gives the claim. $\square$

7. PROOFS OF THEOREM 2.1 AND COROLLARY 2.3

Proof of Theorem 2.1. If X or Y is empty, both sides vanish. Otherwise take Γ as in Lemma 4.1 and h, L, S as in §4. Lemma 4.3 gives (G1), (G2) and (G4), Lemma 4.2 gives (G3), and Corollary 5.3 gives (G5). By Proposition 6.1,

$$(21512e + 3148) \log |X - Y| \leq (37804e - 13144) \log |X + Y|,$$

that is $|X - Y| \leq |X + Y|^{\lambda_\infty}$, since $(37804e - 13144)/(21512e + 3148) = (9451e - 3286)/(5378e + 787)$. $\square$

Proof of Corollary 2.3. By Theorem 2.1 with $G = \mathbb{Z}$, λ_∞ belongs to the set in (2.3), so $\lambda_* \leq \lambda_\infty$. By Theorem 2.2, $\theta^* \leq 2 - 1/\lambda_* \leq 2 - 1/\lambda_\infty$, and $2 - 1/\lambda_\infty = (13524e - 7359)/(9451e - 3286)$. $\square$

APPENDIX A. THE FORMAL PROOF

The accompanying repository consists of the twenty proof modules listed below, the manuscript, and build and publication metadata. Its mathematical namespace is `SumsDifferences`; subsidiary namespaces include `MultiScale`, `ConverseAmplification`, `CoupledEntropy`, `CoupledForms`, `NonShannon`, `GridClosedForm`, and `ClosedForm`. Module names in the table omit their common prefix `SumDifference` and the extension `.lean`.

The reference toolchain is `leanprover/lean4:v4.28.0`, and the Mathlib commit is

`8f9d9cff6bd728b17a24e163c9402775d9e6a365`.

The additive-combinatorial input taken from Mathlib is the Plünnecke–Ruzsa inequality `pluennecke_ruzsa_inequality_nsmul_sub_nsmul_add`. The finite entropy theory is developed in `FinEntropy`, `JointEntropy`, `CondEntropy`, `EntropyEquality`, `EntropyCompute`, and `ProductLaw`. Group-valued laws are represented by elements of the group algebra $\mathbb{R}[G]$ with nonnegative coefficients of total mass one; multiplication is convolution. Thus `ent` and `pushEntropy` denote the ordinary Shannon entropies used in the paper.

The theorem `pair_ceiling_entropic` is polymorphic in a type G equipped with `AddCommGroup` G . Its auxiliary `DecidableEq` G instance supplies equality decisions for finite sets and imposes no mathematical restriction, since classical logic provides such an instance for every G . Cardinalities are coerced to $\mathbb{R}$, and exponentiation is real exponentiation. Empty sets are included. The definition `Admissible` has exactly the quantifiers in (2.2); `theta` is its real supremum, with `sSup` $\emptyset = 0$. No lower-bound construction is required to prove the upper bound on this supremum.

paper	Lean declaration	module
(2.2), θ^*	<code>Admissible, theta</code>	<code>ThetaDefs</code>
(2.3)	<code>pairCeilingExponents, lamSup</code>	<code>ThetaMultiScaleCore</code>
Lemma 3.1	<code>admissible_le_of_rpow_bound</code>	<code>ThetaLocalization</code>
Lemma 3.2	<code>exists_translate_packing</code>	<code>ThetaLocalization</code>
Lemma 3.3	<code>card_sub_mul_card_le_localized_const</code>	<code>ThetaLocalization</code>
Lemma 3.4	<code>card_sub_mul_le_scale</code>	<code>ThetaMultiScaleCore</code>
Proposition 3.5	<code>card_sub_pow_mul_le_telescope, card_sub_pow_le_multiscale</code>	<code>ThetaMultiScaleCore</code>
Theorem 2.2	<code>one_le_of_pair_ceiling, admissible_le_of_pairCeiling_multiscale_J, admissible_le_of_pairCeiling_multiscale, theta_le_of_pair_ceiling, theta_le_two_sub_inv_lamSup</code>	<code>ThetaMultiScaleCore</code>
(E4), (E5), (E1)	<code>ent_le_ent_mul, ent_madiman, ent_mul_le_log_card</code>	<code>EntropySumsetCalculus</code>
Lemma 4.1	<code>exists_coupling</code>	<code>CoupledEntropyCore</code>
Lemma 4.2	<code>coupled_link, link</code>	<code>EntropySumsetCalculus, CoupledEntropyCore</code>
Lemma 4.3	<code>ent_concave_step, grid_concave</code>	<code>CoupledEntropyCore</code>
$\mathbf{H}[F]$, (R1)–(R7)	<code>HL, Det.gen, HL_eq_of_det, HL_swap, HL_indep, HL_pair1/2, HL_X1, ..., HL_X1Y1_le</code>	<code>LinearFormsEntropy</code>
identities via (R1)–(R3)	<code>HL_eq_norm</code>	<code>LinearFormsNormalForm</code>
Lemma 4.6	<code>copy_step</code>	<code>MatusInequality, CopyLemma</code>
Theorem 4.4	<code>matus_ineq</code>	<code>MatusInequality</code>
Theorem 4.5	<code>companion_ineq</code>	<code>CompanionInequality</code>

paper	Lean declaration	module
pairs of forms as variables	HS_eq_HL2	LinearFormsPairs
Proposition 5.1	CoupledForms.two_copy_ineq	ThetaTwoCopyLemma
Corollary 5.3	CoupledForms.two_copy_ineq_sym	ThetaClosedFormBound
Lemma 6.2	GridClosedForm.Z_zero, Z_one, Z_rec, Z_succ_le, Z_convex, Z_le, Z_weight	ThetaGridClosedForm
Lemma 6.3	tau_nonneg, tau_ratio, tau_two, psi_nonneg	ThetaGridClosedForm
Lemma 6.4	inv_base, inv_step, inv_all	ThetaGridClosedForm
Proposition 6.1	grid_closed_sym, grid_closed_form	ThetaGridClosedForm
Theorem 2.1	ClosedForm.log_card_le_of_coupling_closed, pair_ceiling_entropic	ThetaClosedFormBound
Corollary 2.3	lamSup_le_closed_form, theta_le_closed_form	ThetaClosedFormBound

Differences of presentation. Lemmas 3.3–3.4 and Proposition 3.5 are formalised with an additional constant $C > 0$ in the hypothesis $|X - B| \leq C|X + B|^\lambda$; the paper uses $C = 1$, as does the formal proof of Theorem 2.2. The pair exponent is formalised directly by the infimum (2.3); no alternative characterisation of it is used.

The certificate of Proposition 5.1. Each of the 76 rows (Tables 1 and 2, the identities (R4)–(R6), 24 further identifications by (R1)–(R3) and $\mathbf{H}[\emptyset] = 0$) is a separate lemma, and the proposition is closed by `linear_combination` with the integer weights of the tables. The identifications of lists of forms use `HL_eq_norm`; independence and the identifications with L and h are proved separately. For the former, a computable test finds integer witnesses for the mutual determination of two lists of forms (allowing (R2) and (R3)), the kernel re-checks these witnesses with `decide`, and the lemma `Det.gen` turns them into an equality of entropies. The search procedure is not trusted; only the re-check enters the proof. The published Lean source contains the complete certificate; no external data file or search program is a proof input.

Axioms. The commands

```
#print axioms SumsDifferences.theta_le_closed_form
#print axioms SumsDifferences.pair_ceiling_entropic
```

report `propext`, `Classical.choice` and `Quot.sound` only.

REFERENCES

- [1] E. P. Csirmaz and L. Csirmaz, *Information inequalities for five random variables*, *Computation* **14** (2026), no. 2, article 42. Extended version: arXiv:2512.23316v2. References to numbered results are to this version. <https://doi.org/10.3390/computation14020042>.
- [2] R. Dougherty, C. Freiling, and K. Zeger, *Non-Shannon information inequalities in four random variables*, 2011. arXiv:1104.3602.
- [3] K. Gyarmati, F. Hennecart, and I. Z. Ruzsa, *Sums and differences of finite sets*, *Funct. Approx. Comment. Math.* **37** (2007), 175–186. Author manuscript. <https://doi.org/10.7169/facm/1229618749>.
- [4] F. Hennecart, G. Robert, and A. Yudin, *On the number of sums and differences*, *Astérisque* **258** (1999), 173–178. https://www.numdam.org/item/AST_1999__258__173_0/.
- [5] M. Madiman, *On the entropy of sums*, *Proc. IEEE Information Theory Workshop, Porto, 2008*, 303–307. Author manuscript. <https://doi.org/10.1109/ITW.2008.4578674>.
- [6] M. Madiman, A. W. Marcus, and P. Tetali, *Entropy and set cardinality inequalities for partition-determined functions*, *Random Structures Algorithms* **40** (2012), 399–424. arXiv:0901.0055.
- [7] F. Matúš, *Infinitely many information inequalities*, *Proc. IEEE International Symposium on Information Theory, Nice, 2007*, 41–44. <https://doi.org/10.1109/ISIT.2007.4557201>. The five-variable family used here, with a proof, is reproduced in [1, Theorem 22].

- [8] The mathlib Community, *The Lean mathematical library*, Proc. 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, 2020, 367–381. arXiv:1910.09336. The Mathlib 4 revision used here is 8f9d9cff6bd728b17a24e163c9402775d9e6a365.
- [9] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, Automated Deduction—CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer, 2021, 625–635. <https://lean-lang.org/papers/lean4.pdf>.
- [10] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica **32** (2012), 721–733. arXiv:1101.3507v3.
- [11] I. Z. Ruzsa, *An analog of Freiman’s theorem in groups*, Astérisque **258** (1999), 323–326. https://www.numdam.org/item/AST_1999__258__323_0/.
- [12] I. Z. Ruzsa, *Sumsets and entropy*, Random Structures Algorithms **34** (2009), 1–10. <https://doi.org/10.1002/rsa.20248>.
- [13] T. Tao, *Sumset and inverse sumset theory for Shannon entropy*, Combin. Probab. Comput. **19** (2010), 603–639. Revised preprint, titled *Sumset and inverse sumset theorems for Shannon entropy*: arXiv:0906.4387v5.
- [14] Z. Zhang and R. W. Yeung, *On characterization of entropy function via information inequalities*, IEEE Trans. Inform. Theory **44** (1998), 1440–1452. <https://www.cs.cornell.edu/courses/cs783/2007fa/papers/ZYnShannon.pdf>.